Internet of Things IoT-Assisted Secure Monitoring Framework for Cardiovascular Implants

Hashim Elshafie[1]

[1]Department of Computer Engineering, College of Computer Science, King Khalid University, Abha 61421,
Kingdom of Saudi Arabia KSA.

Abstract
This paper explores the integration of IoT and Cloud computing to create secure, low-cost, real-time health monitoring systems, emphasizing their importance in remote care—especially post-COVID-19. It advocates for digital alternatives to traditional diagnostic tools and highlights the need for home-based solutions in low-resource settings. The study also points out that while progress exists, the combined use of IoT and Cloud for medical emergencies in developing countries is still underdeveloped, calling for innovative mobile health applications to overcome infrastructure and cost challenges

Keywords:
Internet of things (IoT), Secure Monitoring and Cardiovascular Implants

1. Introduction

Inpatient duration prediction is essential for further efficient care and resource management. This predictive capability can enhance patient outcomes by allowing healthcare providers to allocate resources more effectively and ensure timely interventions . By leveraging real-time data analytics, healthcare professionals can identify patterns in patient behavior, leading to proactive measures that mitigate risks associated with cardiac conditions. This capability is crucial for monitoring patients with implanted cardiac devices, as it allows for timely interventions and personalized treatment plans. By leveraging advanced data analytics and connectivity, healthcare providers can access real-time information, ensuring that any irregularities in heart function are addressed immediately [1][2][3]. This capability not only enhances patient care but also contributes to better clinical outcomes through timely interventions. This research proposes a hybrid monitoring system for encompassing inpatient stay predictions using deep learning Natural Language Processing and varied machine learning methods for different types of patient records to meet these demands and obtain importable insights for hospital purposes [4][5][6]. Self-monitoring vascular devices are likely to have broad medical relevance due to the widespread use of stents across the body. For instance, stents are commonly deployed in regions such as the heart, brain, renal (kidney) and carotid arteries, as well as the ureters and esophagus, among others. Similarly, synthetic grafts—used to replace native blood vessels—are widely applied in clinical settings, particularly for peripheral access in procedures like blood exchange during hemodialysis, as illustrated in Figure 1.

Figure 1. An example of a self-monitoring vascular stent developed by Vesselsens, capable of two-way communication to enable predictive medical interventions for restenosis.

The proposed solution is further extended and examined in experimentation. Patients were released from the hospital for a particular duration, detailed information concerning the patient's current look felt for the hospital, such as medical records, biometrics, and other associated data, is usually retrieved in the hospital administration network. To anticipate the patient's length of stay, these patient-related data will be accumulated and systematically analyzed. In this manner, the accumulated insights may help hospital staff to manage patient admission more effectively, thereby helping to improve overall care quality. While many existing studies concern predicting inpatient stay outside the hospital environment, this information

Manuscript received June 5, 2025
Manuscript revised June 20, 2025
https://doi.org/10.22937/IJCSNS.2025.25.6.23

needed no hospital-based real-time monitoring solution [7][8] [9][10][11].

Following successful ex-vivo and animal model studies, the VLAP™ device (Figure 2) has entered its first clinical trial involving human participants. A recent case report demonstrated that the device effectively prevented hospital admission through telehealth monitoring of a patient in self-isolation due to COVID-19. Additionally, Synchron—a company established in 2012—has developed a stent-based technology aimed at diagnosing and treating neurological disorders such as paralysis, epilepsy, and depression. Their product, the Stentrode™, is implanted non-invasively within blood vessels and is capable of detecting brain signals across various frequency ranges.

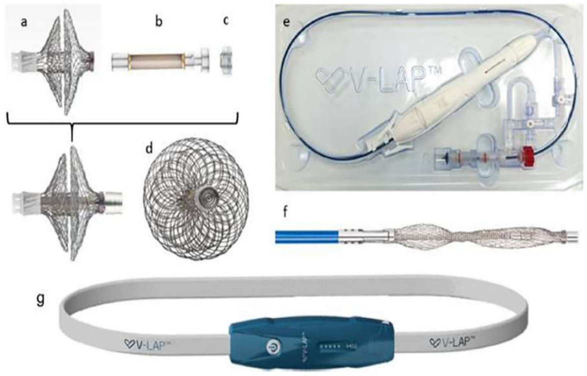


Figure 2. Depiction of the V-LAP™ device developed by Vectorious [83], including the implant components (a and d), the electronic circuit and pressure sensor cup (b and c), the delivery mechanism (e), the nitinol anchoring structure (f), and the external wearable belt (g).

Therefore, it appears essential to adopt a revised strategy for managing patients with heart failure (HF). Traditionally, medical intervention was initiated during the more advanced stages of decompensation phases C or D; see Figure 3. However, emerging evidence suggests that earlier clinical action—during the initial stages (phases A or B)—may be more effective, particularly when guided by physiological indicators that begin to shift well before symptoms appear. These early changes can often be detected as early as 10 to 20 days prior to symptom onset. The device is non-invasively implanted into the vascular system and is capable of detecting neural activity across a broad frequency spectrum.

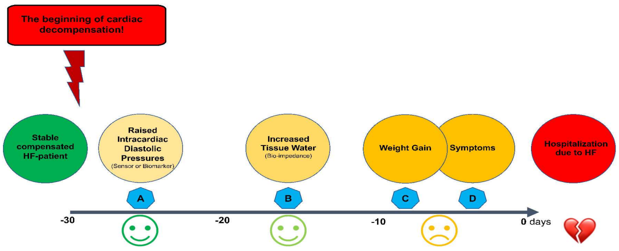

The beginning of cardiac decompensation!
Stable compensated HF-patient
Raised Intracardiac Diastolic Pressures
(Sensor or Biomarker)
Increased Tissue Water
(Bio-impedance)
Weight Gain
Symptoms
Hospitalization due to HF
A
B
C
D
-30
-20
-10
0 days

Figure 3. Stages of worsening heart failure (HF). At present, clinical intervention typically begins at stage C. However, it would be more effective to respond earlier, during stages A or B. Remote monitoring presents opportunities to enable such early detection and intervention.

1.1. Definition and Concepts of Internet of Things

The IoT(IoT) is considered to be an infrastructure in which objects, data, services, and applications can communicate and work with each other to make intelligent and autonomous decisions. This interconnected network of devices enables real-time data collection and analysis, which is particularly beneficial in the healthcare sector. By integrating IoT technology with cardiac devices, healthcare providers can monitor patient conditions continuously, leading to enhanced patient care and timely interventions [12][13][14]. This integration not only allows for real-time data collection but also facilitates advanced analytics and personalized treatment plans. These features are crucial for enhancing patient safety and ensuring timely medical interventions. In the context of cardiac devices, these features leverage real-time data collection and analysis to monitor patients' heart health continuously. By utilizing IoT technology, healthcare providers can receive immediate alerts regarding any irregularities, allowing for prompt intervention and personalized care.

This real-time monitoring capability enhances the overall safety and efficiency of cardiac care, ultimately leading to improved patient outcomes. The integration of IoT technology into cardiac devices provides real-time data transmission, which enables healthcare providers to monitor patients remotely and respond to potential complications swiftly. The advent of IoT has witnessed countless applications in areas as health, agriculture, environment, and daily life. The current COVID-19 pandemic raises concerns about the deployment of care resources, quarantine areas, etc. In developing countries, quarantine areas in which COVID-19 cases are isolated (wards) are quickly running out. Hospitals lack medical supplies and space for isolation in emergency cases [15][16].

The advancement of IoT-driven technologies for monitoring and preventing congenital heart disease (CHD) represents a crucial and rapidly evolving area in healthcare. These innovations hold the promise of significantly enhancing care for CHD patients and may even contribute to preventing the condition altogether. IoT-enabled systems support continuous cardiovascular monitoring by linking medical devices to the internet, enabling the collection of health and environmental data through a centralized platform. This real-time information can be used to monitor trends and detect abnormalities early, facilitating timely diagnosis and intervention. Recent progress in IoT applications for CHD has led to more precise detection and diagnostic capabilities. For example, wireless ECG devices can now be installed in patients' homes, transmitting live data to healthcare providers for immediate analysis and response—offering a life-saving advantage over conventional diagnostic approaches. The system's architecture is illustrated in Figure 4 below.

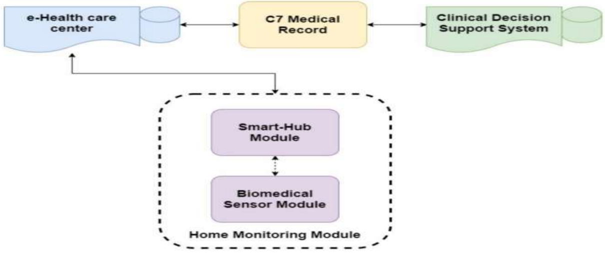


Figure 4 : Construction diagram

This defines a conceptual IoT-based early-warning architecture specifically designed for the remote monitoring of COVID-19 patients both in hospital wards and at home. It facilitates the implementation of various IoT devices strategically deployed in quarantine areas as well as directly within the patient's residence. On-body wearable sensors are advanced instruments that can be comfortably worn on the body, which focus on collecting and relaying crucial physiological data that they gather from or near the skin. The diversity of on-body wearable sensors available for health monitoring is extensive. These innovative instruments can accurately measure a plethora of different physiological parameters, such as blood pressure, heart rate, and oxygen saturation levels, among others. Additionally, various monitoring systems, including advanced ECG devices, have the capability to display monitoring results in real-time, providing immediate insights into the patient's health status [17][2][18]. However, it is important to note that measurements conducted by a qualified physician or a medical center may not always present a comprehensive portrayal of the individual's overall medical state. This lack of comprehensiveness can be attributed to the various conditions under which these measurements are taken. Furthermore, to obtain accurate results, it is essential for individuals to be in a relaxed state and typically, they should refrain from activities that could falsely elevate or diminish the readings being taken. If not properly controlled, this could lead to an ineffective description of the person's true medical condition. On the other hand, the remote monitoring of physiological parameters can be carried out at any time and from any location, enabling continuous health oversight from the comfort of home. The classification of on-body wearable sensors can be divided into two distinct types; the first being on-body contact sensors that maintain close contact with the skin, and the second being peripheral non-contact sensors that can monitor vital signs without the need for direct skin contact. These wearable sensors are notable for being self-powered, compact instruments that transduce signals efficiently, and they may serve as either personal devices for individual health management or as part of professional medical solutions aimed at broader patient care [4][19].

IoT-based solutions offer a cost-effective means for continuous, real-time monitoring of patients with congenital heart diseases (CHDs). The functional block diagram is illustrated in the figure 5 below.

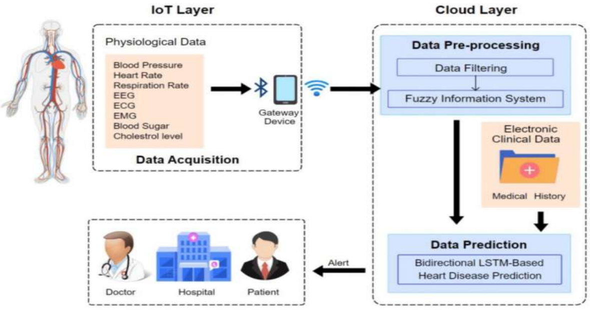


Figure 5: Functional block diagram

The IoT-based system is composed of multiple elements, including sensors, actuators, and interconnected devices that together create a cohesive network. In the context of monitoring and preventing Congenital Heart Disease, these sensors and actuators play a crucial role in tracking vital signs such as heart rate, blood pressure, oxygen saturation, and respiratory rate. The collected data is transmitted over the network to a remote server, where it is stored and analyzed using AI algorithms to detect any irregularities. Connected devices like smartwatches, smartphones, and medical alert systems are then used to notify patients or healthcare providers when abnormal vital signs are detected, enabling prompt medical response. The workflow of this system is illustrated in Figure 6.

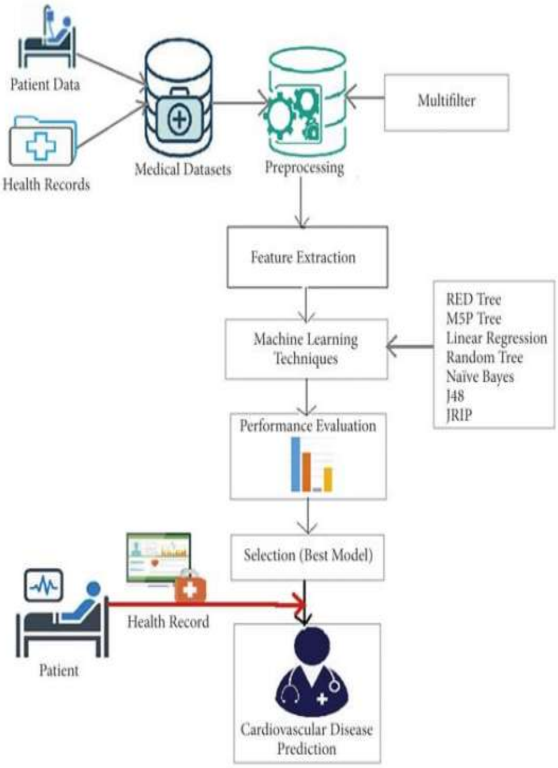


Figure 6: Operational flow diagram

1.2. Applications in Healthcare

In the current evolution of the Internet of Things, there has been a remarkable and increasing number of physical devices that have the capability to obtain, process, and transfer data over the vast expanse of the internet. The internet plays a crucial and transformative role in facilitating the collection and integration of data from multiple locations in real-time while delivering significant opportunities for a more intelligent and responsive healthcare system. Considering that a substantial portion of a person's daily life takes place within various healthcare scenarios, certain forms and types of healthcare services are legitimately required. [12][20].

From an IoT perspective, as the majority of devices being deployed at any given time will likely be other people’s private, modern technology, there is a great and pressing interest in establishing and exploring effective methods to validate the authenticity and reliability of the network relations that are listed and utilized. Additionally, there is a growing interest in healthcare checkup devices that are designed to be compatible with and capable of transmitting critical data to cloud web services, where this information can be analyzed, and any unusual cases can be flagged and observed by a qualified person equipped with the necessary expertise and technology to research further into these anomalies [21][22][23].

Reinforcement learning (RL) plays a vital role in remote health monitoring, particularly in situations that demand continuous or critical observation. Figure 5 outlines a typical IoT-based healthcare setup. Initially, sensors (acting as agents) are trained within a specific environment. In medical contexts, both environmental factors and a patient’s health indicators assist in making informed decisions. Basic patient attributes such as age, weight, and height serve as foundational inputs, while more critical indicators—like heart rate, blood pressure, and glucose levels—function as key decision-making variables. These critical variables can differ depending on the specific healthcare scenario.

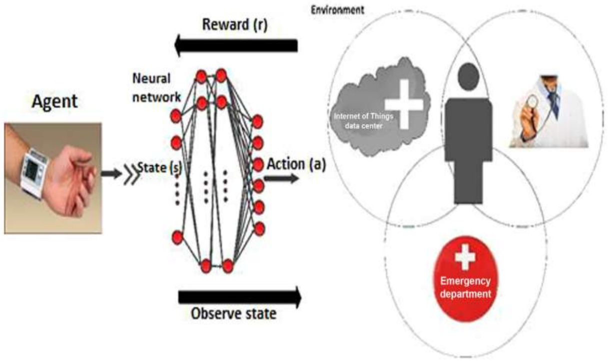


Figure 7. A visual illustration of the communication architecture used in IoT-enabled healthcare systems.

The potential outcomes can be realized in a variety of innovative ways, which may include unlocking access to a sophisticated remote analysis program or instigating an immediate action based on the readings from the wearable measurement device. In addition to the fundamental readings, it should be noted that the data generated can also potentially be exploited to compromise the correct functioning of the system [24][25].. It is equally crucial that robust methods to ensure data privacy are implemented alongside reliability measures. In recent years, cloud storage solutions have rapidly gained approval due to their economies of scale and the significantly reduced demand for maintaining the underlying infrastructure and expertise. Nonetheless, numerous consumer fears, including concerns over security and data privacy, often deter them from fully embracing the advantages of cloud storage solutions. The challenge lies in addressing these fears while demonstrating the benefits that come with adopting such advanced technology [26][27][28].

Finally, the patient informs the healthcare expert about their condition, who then suggests a suitable medical intervention tailored to the patient's needs. Following this, the patient’s treatment is executed locally, ensuring accessibility and convenience. The operation of the eHealth monitoring system is then repeated meticulously until the patient is fully cured. The key benefits of such a health management system incorporate significantly lowered overall operational costs for medical care, substantial decreases in the number of times a patient must be admitted to the hospital, and importantly, it provides a significant peace of mind when it is no longer required for individuals to remain in the hospital beyond the prior signs of recovery that they exhibit. This aspect enhances their quality of life considerably [29][30][31].

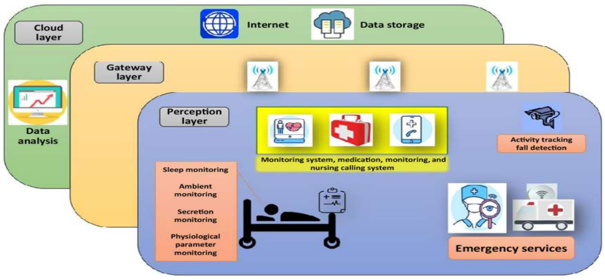


Figure 8: A smart healthcare and nursing system for hospitals utilizing Internet of Things technology and an integrated nurse call feature.

On the other hand, it is essential to note that while there are numerous advantages, there can be a challenging adoption of this kind of advanced technology as it introduces various technical concerns that must be addressed adequately. Regarding the general performance of such systems, the trade-off from reduced operation costs might result in a longer time-lag in revealing and healing potential health conditions when compared with traditional local or specialist analysis methods. Furthermore, within the healthcare field, there is an increasing requirement for trust in the reliability of the therapy administered, making the patient's choice essential to be pleased with the diagnosis received, which can sometimes be a complicated process [32].

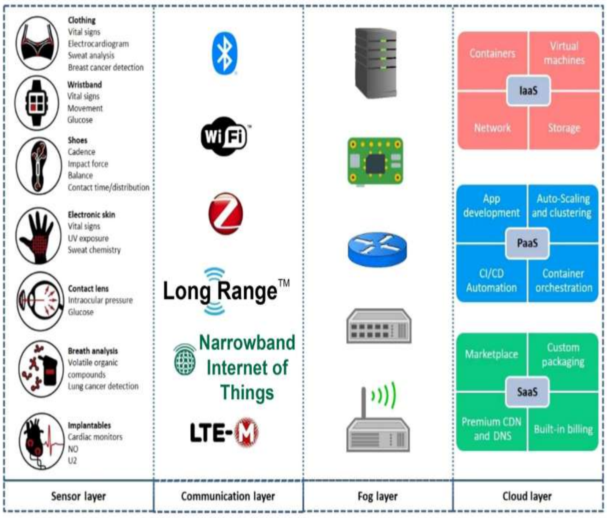


Figure 9: The significance of cloud computing in enabling IoT-driven smart healthcare systems.

2. Cardiac Devices and Remote Monitoring

Not only did these tenebrous clouds hinder physical movement, they also effectively halted vital global communication and meaningful interaction, effectively isolating individuals and entire communities from one another. Amidst the euphonious and relentless roar of the howling wind, there emerged an unexpectedly soothing sound that resonated throughout the land, this was the rigoursodic multifunction, a transformative auditory experience that jolted the people of the earth towards the direction of its friendly and encouraging acts. Remarkably, this deeply impactful sound originated from a remarkable wireless device that facilitated connections between individuals across vast distances, characterized by what we know today as the IoT(IoT) [33][34][35].

The article examined a range of IoT applications in smart healthcare, with particular emphasis on basic symptom monitoring. It also provided an in-depth discussion of current IoT technologies used in healthcare, addressing key areas such as networking, data processing, and sensor hardware. The primary objective of this review is to shed light on core challenges related to IoT device capabilities, system architectures, communication protocols, and healthcare-specific applications (as illustrated in Figure 10). These IoT devices integrate all essential components required for both hardware and software platforms.

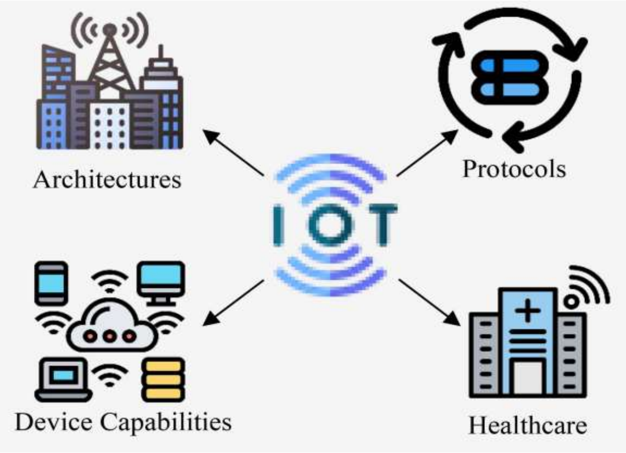


Figure 10 : Visual representation of IoT device functions, system architectures, communication protocols, and their applications in smart healthcare.

2.1. Types of Cardiac Devices

Cardiac implantable electronic devices (CIEDs) serve as a cornerstone in the comprehensive treatment regimen for a variety of heart conditions and electrical disturbances that may arise in patients. These devices encompass several types that play crucial roles in managing cardiovascular health, including bradycardia pacemakers and implantable defibrillators. The defibrillators, which can be implanted either intravenously or subcutaneously, are specifically designed to be activated in cases of fatal tachyarrhythmias, providing critical interventions that can save lives. Furthermore, when these devices are administered via a patent foramen ovale, an external electromagnet has the potential to deactivate them or, conversely, may cause inappropriate and competitive pacing, leading to complications. Lastly, cardiac resynchronization therapy biventricular devices come into play in clinical scenarios involving refractory heart failure, particularly in patients exhibiting prolonged QRS intervals and low ejection fractions. These advanced devices work to enhance the coordinated contraction of the ventricles, significantly improving overall cardiac function and patient outcomes in this challenging disease state [36][37].

There is a rapidly growing and increasing scientific interest that is closely related to the application of the IoT(IoT) specifically to various medical disciplines. This advancement enables the remote monitoring of crucial physiological parameters and supports the timely detection of any physio pathological disturbances that may arise. Diabetes, which is notorious for its severe and often debilitating complications, serves as a significant example of particular interest in the realm of remote monitoring associated with the parameters related to this chronic condition. Smartphones, which are now commonplace and widely utilized, are equipped with multiple and diverse sensors. These advanced sensors empower users to effectively control and monitor numerous health parameters in real time. Further research works have validated the impressive accuracy of these recordings for the identification of atrial fibrillation, achieving a remarkable sensitivity of up to 99.6%, although this comes with a specificity of 80.9%, which is noteworthy. Additionally, various nutritional consultations, cardiac procedures that are performed, along with detailed information about the implants, are meticulously stored within electronic health records. These innovative devices have undergone further validation and development to facilitate the seamless interchange of information among multiple brand devices, enhancing the overall interoperability of health data in the medical field [38][39].

The lithium battery can function for as long as 12 years, depending on usage frequency. When replacement becomes necessary, the battery is removed via a minor surgical incision, and a new one is connected to the existing leads, as illustrated in Figure 11.

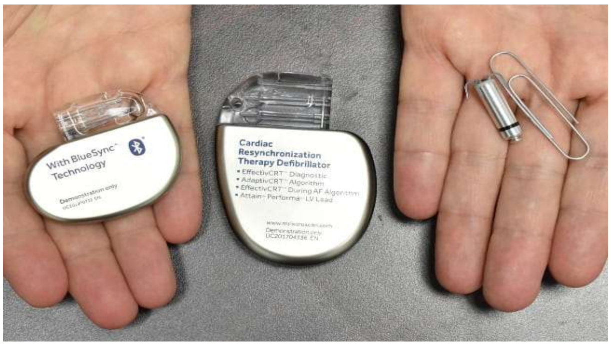


Figure 11: The lithium battery for pacemaker when replacement

2.2. Importance of Remote Monitoring

Remote control of cardiac devices significantly enhances both the monitoring and treatment of patients who have implanted device technologies in their bodies. This innovative technique is made possible through advancements in biotelemetry paired with the Internet of Medical Things (IoMT), which facilitates a seamless flow of information. Enhanced communication pathways between patients and their healthcare providers can lead to improved medical outcomes, fostering a proactive approach to patient care [40][41].

2.3 Pacemakers Devices

Cardiac Implantable Electronic Devices (CIEDs) such as pacemakers, implantable cardioverter-defibrillators (ICDs), and cardiac resynchronization therapy defibrillators (CRT-Ds)—have significantly transformed the care of patients with recurrent and potentially fatal heart rhythm disorders. These technologies provide constant heart rhythm surveillance, allowing medical professionals to identify abnormalities in real time. The remote monitoring function is vital for early interventions, minimizing the need for hospital visits, and enhancing patient health outcomes. Through continuous observation of both vital signs and device functionality, clinicians can make better-informed decisions and tailor treatment strategies accordingly [42][43].

The latest guidelines and expert consensus recommendations for CIEDs advocate remote monitoring for all CIED patients. In line with these recommendations, interest in remote monitoring is rapidly growing and its penetration in an influential and influential country is increasing year by year [44][45].

However, this long-distance connectivity poses some unique hazards. Personal health data are commonly transmitted using a cellular network, the data can be malformed by a hacker, and their working can be used to infiltrate hospital workstations or networks. In a recent occurrence, malfunctions in the pacemaker programming of a patient in the first known cyber assault resulted in the patient's death upon receiving an electrical shock [46].

Overcoming this issue would require cooperation from multiple stakeholders including manufacturers, safety experts, medical workers, regulatory bodies, and patients to create and manage sound safety processes, although current safety standards for Implantable Devices for Chronic Life (IDCL) are still non-mandatory. Efforts are needed to help shape regulatory law on cybersecurity. It is likewise important to improve public understanding and trust in CIED safety. Although the majority of cyber breaches are related to suppliers, it is impossible to fully discard the actions of third parties by workers or the environment. In the expectation of more complex devices, it will be difficult to ensure protection throughout the security timeline [47][48].

3. Security Challenges in Online Monitoring

To comply with regulatory requirements, manufacturers of medical devices have established their own specialized systems through which patients can transmit their cardiac activity data that is collected by external monitoring devices. Based on the data retrieved through these systems, each device manufacturer can tailor the parameters of their devices, diagnose potential cardiac arrhythmias, and make necessary adjustments to the therapy being administered by the implant in response to the data analysis. However, a significant inconvenience faced by patients is that they are often required to carry one specific monitoring device for each device manufacturer, which can be cumbersome and inefficient [49][15].

The data settings are typically established by default, and the prevailing clinical practices can directly impact patient outcomes. Moreover, there are several notable security vulnerabilities that exist within these monitoring systems. For instance, the device appears to lack the implementation of transport layer security (TLS) protocols, which raises

significant concerns regarding the confidentiality of patient information. Even though it is asserted that the system is in compliance with HIPAA regulations, which are designed to protect patient data on the server side and amidst health services, it nonetheless fails to ensure secure data transmission both to the patient and from the patient back to the server. This lack of security poses the risk of malicious attackers being able to manipulate and/or insert false cardiac data, which could potentially lead to inadequate or improper therapy being administered by the device, thereby compromising the well-being of patients who are relying on this critical technology for their health [32]. Figure 12 illustrates a schematic of a remote follow-up system. In this setup, data from the cardiac implantable electronic device (CIED) is transmitted to a monitor or transceiver, which patients typically place in common areas such as their bedroom or living room. This transceiver connects to a central server via Wi-Fi or GSM networks, and the collected data can be securely accessed by hospital systems. Only authorized clinical staff—such as physicians, nurses, or technicians associated with the specific clinic can view data from their own patients. Data transmission from the patient to the clinic can occur through various methods: On-demand, initiated by the patient due to symptoms or prompted by a clinic's request.
Event-triggered, which happens automatically in response to device issues or clinical events like arrhythmias. Scheduled, where transmissions occur at predefined times and dates.

The configuration of the remote monitoring system depends on both the patient's medical history and the clinic's operational preferences and capabilities. To fully utilize the benefits of remote monitoring, the internal organization and workflow of the clinic play a critical role. As discussed later, the timing and manner in which the transmitted data is reviewed can significantly influence patient safety, operational costs, and overall satisfaction.

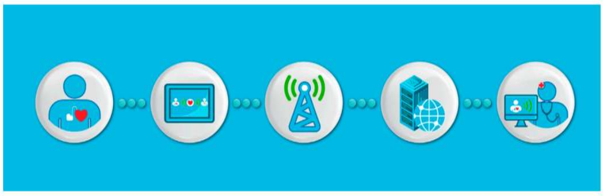


Figure 12 : Diagram illustrating the system setup, which includes the patient with a CIED, a transmitter, a server, and the hospital's computer and medical staff.

4. Secure Communication Protocols

To enhance security further, an additional EC counter is integrated within the device, and its count is incremented every time a successful Egram Intrusion beat is detected. This counter serves as a crucial check to compare how many times the external command has effectively initiated a shock, thus playing a vital role in maintaining patient safety [50][51] [52].

A patient with a specific cardiac condition and medical history uses an implantable cardioverter-defibrillator (ICD) to manage their health. Figure 13 illustrates the communication flow between the implanted ICD and a controller located within a healthcare facility. The patient employs a FDA-approved portable monitoring device for personal assessment of the ICD's performance. Data collected is transmitted via the Internet to cloud-based servers, where it becomes accessible to healthcare professionals for detailed evaluation. Clinicians use a remote controller to supervise, configure, and operate the ICD. This controller includes an interface that allows the practitioner to wirelessly transmit various input parameters directly to the device.

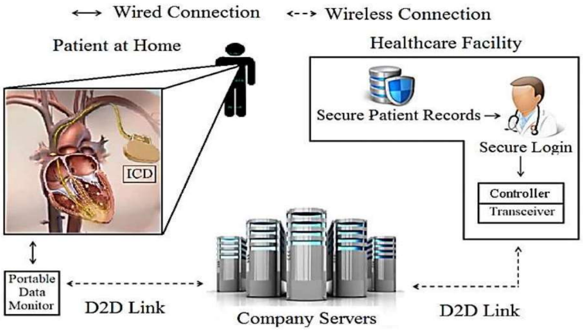


Figure 13. ICD-controller communication model

4.1. Overview of Communication Protocols

For example, an Electrocardiogram (ECG) device affixed to a patient continuously captures the heart's electrical signals. This critical health information is subsequently sent to healthcare professionals for analysis and interpretation to guide medical decisions. Following a thorough technical examination of this data, healthcare professionals provide appropriate medical advice and recommendations. Furthermore, specific guidelines are established to secure all patient health monitoring data, ensuring that it remains confidential while still being accessible to authorized expert personnel. In summary, this paper elaborates on the innovative concept of real-time heart monitoring through the lens of IoT, underscoring the importance of attendance notification within hospitals via secure communication channels. The result is a sophisticated ECG patient heart monitoring system designed not only for automatic classification of heart activity but also for efficient attendance notifications, thus enhancing patient care and healthcare delivery overall. [53][54].

4.2. Secure Protocols for Healthcare IoT

Biosensors are crucial components in these systems, as they continuously generate vital biometric data that is sent to a responsible microcontroller. Following this initial transfer, the collected data is then transmitted to the cloud, where it is securely stored and meticulously processed. For instance, in the realm of cardiac care, these systems are instrumental in detecting and effectively treating arrhythmia by activating an actuator such as a defibrillator when irregularities are detected. The convenience and functionality of these systems enable them to be implemented in home settings, providing valuable health monitoring; however, this also makes them susceptible to various forms of unwanted data tampering and cyber threats [54].

The proposed health monitoring system is developed to continuously observe vital signs from patients or elderly people, securely store the collected data, and transmit it to a public cloud database. It provides a real-time monitoring interface that authorized healthcare professionals or caregivers can access at any time and from any location. The system employs a three-tier architecture comprising the patient layer, the cloud layer, and the doctor layer. This three-layer architecture is depicted in Figure 14.

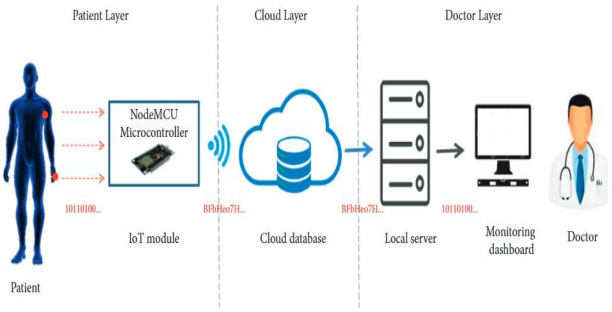


Figure 14: Architecture of the proposed model

5. Authentication and Access Control

A significant aspect of this system is its reliance on the concatenation of these inter-lock bits, which are subsequently fed into the SHA-3 256 function to produce a secure 256-bit value. This contributes to the overall integrity of the device and its communications. Furthermore, this secured system serves as a critical platform for Internet-of-Medical-Things (IoMT) network access and auditing, particularly in the context of medical treatment for patients. It enables the medical devices utilized by patients to effectively manage their health conditions while being thoroughly documented within the healthcare system.

5.1. Importance of Authentication

Using a wireless network to send and receive information can be dangerous. Many people can have access to a wireless network from outside a home and can use that network to gain access to a computer without the owner's knowledge. Verifying the patient’s identity is an essential security measure in remote health monitoring systems. It is crucial that the system confirms the data originates from the correct individual before any medical or financial actions are taken based on that information. A wide range of authentication methods have been developed using passwords, smart cards, biometrics, digital signatures, and other forms of ID. These methods are often not well suited to remote health care; for example, patients may be reluctant to input passwords, may be unable to use a smart card reader, or may be willing to give a potentially harmful third party their password [52][55][56].

5.2. Access Control Mechanisms

Within this communication framework, we must generate new communication request resources each time a fresh message is dispatched. This counter will serve as a critical verification tool, allowing for the tracking and comparison of how many times the external command has successfully triggered the necessary intervention, such as administering a shock, and thereby ensuring the utmost safety of the patient. Ultimately, a thorough solution verification process has been undertaken, involving a series of tests focused on confirming the entire process's functionality regarding the accuracy and correctness of the access control system employed [57][52].

The User-Managed Access (UMA) schema, as shown in Figure 15, involves three main phases: first, the Resource Owner (RO) registers a Resource Server (RS) with the Authorization Server (AS) using a Protection API Token (PAT) and sets access control policies for the RS's scopes through its management interface; second, a Requesting Party (RP), via a client application, requests access to a resource on the RS by obtaining authorization data and a Requesting Party Token (RPT) from the AS's Authorization API, authenticated with an Authorization API Token (AAT); finally, with the valid RPT and authorization data, the RP's client is granted access to the requested resource on the RS.

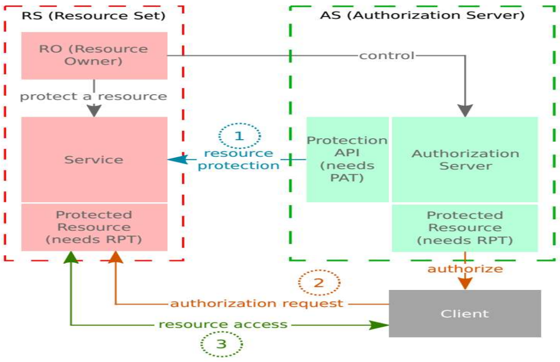


Figure 15. The primary stages and components involved in User-Managed Access (UMA) include the Protection API Token (PAT) and the Requesting Party Token (RPT).

6. Data Encryption and Decryption

Sensitive data is incredibly important and crucial to uphold. The consequences of obtaining unauthorized access to such data could lead to a myriad of serious cybersecurity issues. One such advancement in technology includes cellular medical devices, which facilitate the remote monitoring of an individual's health condition. These devices could be extremely advantageous in providing timely and vital health information. Wireless networks are generally employed in the transfer of data between these sophisticated medical devices, and the information exchanged often contains highly confidential data pertaining to patients. Given the nature of this data, it is critical that upon reception, we consider the possibility that it could have been tampered with, leading to unauthorized access or breaches of security. Any receiving device that has gained unauthorized entry could potentially acquire sensitive information that enables it to access web pages and databases.

To enhance security measures, measured memory locks are utilized to generate texts that are specifically designed for encoding. Due to the potentially excessive number of locks involved, a Text Locks Generation Algorithm is implemented to streamline the process. The unique principle of Syng folly is employed within the text creation technique, where the wording typically contains two sections of consecutive spaces, adding another layer of complexity to the encryption process. Moreover, a reasonable and thorough evaluation of the algorithm will subsequently be provided with the aim of thoroughly assessing each sensitivity level to the acceptable fake key, ensuring the robustness of the encryption methods in place [58][59].

The general concept of the Implantable Medical Device (IMD) solution, illustrated in Figure 16, provides a foundation for understanding the core elements described throughout the manuscript.

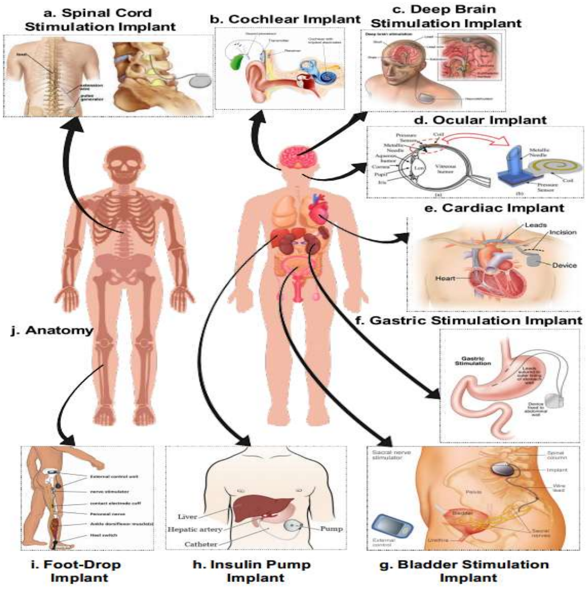


Figure 16 : Implantable Medical Devices

6.1. Symmetric and Asymmetric Encryption

This paper has been meticulously designed with the central objective of identifying several lightweight post-quantum security asymmetric cryptographic protocols that are specifically suited for smart city IoT networks.

Another notable vulnerability in this specific use-case pertains to a smart meter home area network (HAN), which is intermittently pinged by a single packet originating from a malevolent and disposable endpoint. The intent behind this malicious activity is to eavesdrop on the communications and attempt to decrypt the packets exchanged within the network. The index of the secure secret key stream, referred to as Tsetlin, is incorporated to obscure abstracts of various randomly selected packets, which may have been substituted or served as surrogates during the transmission. This occurs at the moment when smart inverters are engaged in exchanging their operation and management control packets (O&M) in accordance with the smart meter [60][61][62].

6.3. Key Management

Online monitoring of various implantable medical devices by utilizing the IoTcan create a highly promising healthcare infrastructure designed specifically for patients. This innovative approach is particularly vital for the ongoing development in the monitoring of wearable and pacemaker devices, as it has far-reaching implications for the future healthcare market. The unique aspect of this system is its accessibility; anyone can easily utilize the device. This includes not only patients with chronic diseases but also healthy individuals and elderly persons, thanks to its user-friendly design. The infrastructure that this technology fosters may serve as the cornerstone for a novel healthcare paradigm, which facilitates the possibility for patients to receive timely and effective real-time treatment while remaining in the comfort of their own homes [63][1].

The proposed system comes equipped with several additional features that extend beyond what traditional monitoring systems for cardiac devices typically offer. In fact, it is versatile enough that it can also be applied to a vest, shirt, or even a chair, thereby allowing a wide variety of devices to be used in conjunction. This integration of technology promotes a seamless monitoring experience. Moreover, a smartphone connected to the Internet can easily access real-time information about the patient's condition and has the capability to instantly notify the nearest medical staff in the event of an emergency. Medical personnel can monitor the activities of patients living with chronic diseases in real time, regardless of the distance separating them, thus enhancing the quality of care provided. Additionally, patients benefit from receiving tailored advice and support from medical staff as part of this interactive care process, enabling a more engaged and responsive healthcare experience [63][64][65].

7. Anomaly Detection and Intrusion Prevention

Recently, remote cardiac devices have increasingly demonstrated vulnerabilities to various external attacks, primarily due to their inherently limited resources and the presence of inadequate security mechanisms designed to protect sensitive data. With the surge in the adoption and usage of such sophisticated medical devices in healthcare settings, an additional, significant security concern has inevitably arisen. This situation highlights the urgent need for medical facilities to devise and implement innovative tools and methodologies that prioritize patient safety and data integrity. These new instruments must be capable of securely and continuously monitoring the health data transmitted by these devices, thereby effectively mitigating risks to consumers and ensuring consistent, dependable, and secure treatment for patients of all demographics [66][67][68][69].

7.1. Behavioral Analysis

For instance, patients can undergo interrogation of their implanted devices using an external monitoring unit while comfortably seated in their own homes, promoting convenience and reducing travel stress. Additionally, this remote functionality empowers medical professionals to proactively track and treat their patients and can mitigate the need for frequent in-clinic visits, which is often inconvenient for individuals managing chronic conditions. The potential for early detection of critical health events that might otherwise go unnoticed is perhaps one of the most compelling advantages of this technology, leading to significantly improved outcomes and enhancements in the overall health and well-being of the patient population [70].

7.2. Intrusion Detection Systems

To design systems that can effectively and rapidly perform robust detection of various cyber-attacks targeting the IoT application layer, a top-down approach is adopted. This method begins from the network layer and progresses upwards to reach the application layer, addressing potential threats at every level. Cyber-attacks can be classified in two broad categories, which take into account their ability to propagate along the network medium: (1) Attacks that actively involve the network medium, such as Denial-of-Service attacks, stand out as the predominant source of cyber-attacks within IoT networks. These types of attacks have an innate advantage due to their ability to easily propagate between connected devices and hubs, thereby creating significant security risks. (2) On the other hand, there are attacks that are confined to and propagate from a specific device, such as Root to Local and User to Root attacks, which have been the focus of previous work. Nevertheless, it remains exceptionally challenging to guarantee or even anticipate that no attack occurring at the network layer will advance further up through the subsequent network layers, thereby increasing overall vulnerability to cyber threats. Compounding this problem is the fact that the IoT network environment is entirely open and accessible to anyone with malicious intent [71][72] [73][74].

8. Regulatory Compliance and Standards

Cardiovascular diseases represent the leading cause of mortality across the globe, affecting millions of individuals each year. The emergence of cutting-edge technologies known collectively as the IoT(IoT) and the Internet of Medical Things (IoMT) has ushered in a new era in healthcare delivery and management. Among the most promising applications of IoMT devices, particularly in the field of cardiology, is the development of innovative technologies dedicated to secure ECG (electrocardiogram) monitoring. These advanced systems not only enhance the way we monitor heart health but also facilitate a robust connection to healthcare providers, ensuring rapid responses to any potential cardiac issues [75][76] .

8.1. HIPAA Compliance

Despite these advancements, the data collected is often vulnerable to both design flaws and security issues inherent in cyber technology. As a result, it is paramount to develop a safe and implementable program for any successful remote monitoring product that aims to effectively safeguard user information. Commercial mobile products also play a crucial role in deterring potential eavesdroppers, while patients have the opportunity to view certain data through their closely monitored devices. Numerous companies are currently offering a variety of cardiac devices, such as defibrillators, pacemakers, loop monitoring systems, and Implantable Loop Recorders (ILR), designed specifically for remote monitoring of patients [77][78] [79]. Figure 17 illustrates the concept of the Internet of Medical Things (IoMT) from a patient-centered perspective, integrating various technologies such as Artificial Intelligence (AI), Blockchain (BC), Cloud Computing (CC), 5G connectivity, and Big Data analytics. IoMT has emerged as a transformative approach, offering a wide array of functionalities and enhancing communication systems to near-optimal levels. It enables the seamless interconnection of numerous devices, establishing a unified platform that supports multiple users. Given its rapid growth and technological evolution, it is essential to thoroughly examine its potential applications across diverse domains.

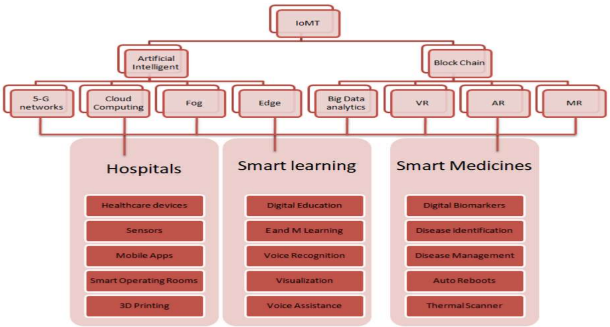
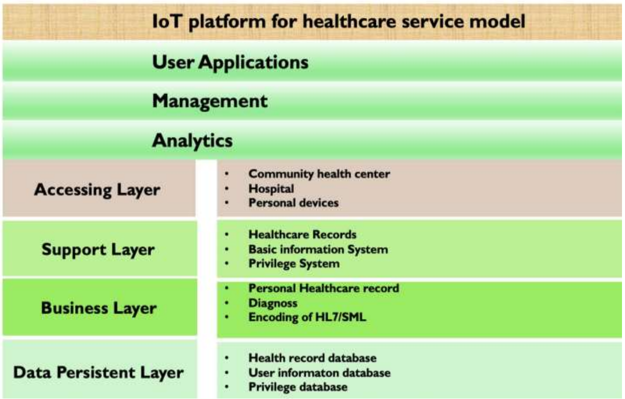


Figure 17: Overview of IoMT in the context of patient data

Network remote maintenance reviews and collaborations with healthcare experts are underway to ensure that the system is optimized for the efficient use of these products. Users are encouraged to visit the device console and configure its broadband antenna according to one of six designated tasks on hub clients. The attachment of vital information on the device itself, including battery levels, incidents, and rehabilitation data, becomes crucial in this context. Once the data is processed, the broadband connection is established and the information is transmitted over the same server. Continuous storage of patient data is facilitated via this network, often directed to platforms such as Dropbox; nevertheless, safety remains an ongoing concern during this data transfer process. As healthcare technology evolves, it is critical to emphasize secure and responsible handling of sensitive personal health information [46].

8.2. ISO Standards for Healthcare IoT

In an IoT framework, the healthcare network platform functions as a service-oriented system centered around managing and utilizing residents' health information, as illustrated in figure 18.



IoT platform for healthcare service model

User Applications

Management

Analytics

Accessing Layer	• Community health center • Hospital • Personal devices
Support Layer	• Healthcare Records • Basic information System • Privilege System
Business Layer	• Personal Healthcare record • Diagnoss • Encoding of HL7/SML
Data Persistent Layer	• Health record database • User informaton database • Privilege database

Figure 18 : IoT functional framework of the platform model for the health information service model.

Subsequently, in alignment with the constraints that have been proposed for the thoughtful design of healthcare IoT systems and applications, it is strongly suggested that additional constraints be integrated into the pertinent ISO standards to enhance specificity. This enhancement may involve the introduction of a proposal that is based on various mechanisms, algorithms, protocols, enactments, or other means, all of which are explicitly targeted at healthcare applications in order to ensure better compliance and effectiveness. The constraints that are proposed for the enhancement of healthcare IoT standards can indeed be employed as metrics for the evaluation of the healthcare IoT standards across the board. Furthermore, as a significant contribution to this field, a detailed document template has been meticulously developed for the uploading of healthcare IoT solutions accompanied by the proposed metrics, thereby streamlining the process of documentation and compliance in this vital area of healthcare technology [54].

9. Case Studies and Best Practices

Online heart rate monitoring has become increasingly essential in a multitude of cases, especially in the context of health and fitness management. The normal heart rate value for adults at rest typically ranges between 60 and 100 beats per minute, serving as a vital indicator of an individual's cardiac health. An innovative system for remote heart rate monitoring has been proposed, which has, to date, successfully performed on a variety of smart devices. This system is centered around the concept of utilizing IoT (Internet of Things) wearable devices that can be employed conveniently and are available at a reasonable price point. The most popular application of such gadgets is undoubtedly the smartwatches that are designed to meticulously track the user's physical activities and health metrics [80][52].

10. Future Trends and Technologies

Currently, countries all over the globe are either enforcing severe dropdowns or implementing partial lockdown measures for the public in response to the COVID-19 pandemic outbreak. There are various reports being disseminated, indicating that the COVID-19 crisis will require a certain amount of time to be managed effectively, particularly until a vaccine for comprehensive treatment is developed. Until that time, as a usual case during such crises, maintaining the security of citizens' lives and ensuring the quality of health treatment provided to them must be given top priority. The use of the IoT(IoT) emerges as a significant impetus for change and could play an increasingly vital role—enabling a preventative healthcare system that operates at lower costs and with greater efficiency by continuously monitoring human well-being through a wide array of relatively inexpensive and easy-to-use wearable devices that are interconnected via the internet [82][83].

11. Conclusion

The system architecture is a basic foundation to be used in the future as a reliable means for new health monitoring communication systems to save the life of patients. Although some early preparation steps have been taken by a number of healthcare companies, the IoT(IoT) and Cloud technology are poised to experience an explosive growth in the upcoming years, marked by the rising prevalence of wearable devices, emerging IoT Apps and platforms for monitoring health, remote diagnosis, healthcare applications and patient care. Moreover, it is noticeable that the COVID-19 pandemic has thrown a light on the urgent necessity for a home-based monitoring system that is capable of allowing healthcare professionals to monitor more patients online. It is the contention that these new developments would result in a new wave of low-cost, secure and real-time vital signs monitoring health systems, and there is a demand to develop such systems rather than use the costly stethoscope, sphygmomanometer or otoscope for amino acid, cholesterol or blood oxygen measurements.

Acknowledgment:

"The authors extend their appreciation to the Deanship of Research and Graduate Studies at King Khalid University for funding this work through Large Research Project under grant number RGP2/447/46"

References

[1] A. Molloy, K. Beaumont, and A. Alyami, "Challenges to the development of the next generation of self-reporting cardiovascular implantable medical devices," IEEE Reviews in ..., 2021. ieee.org

[2] G. Prieto-Avalos, N. A. Cruz-Ramos, and G. Alor-Hernandez, "Wearable devices for physical monitoring of heart: a review," Biosensors, 2022. mdpi.com

[3] T. Bekfani, M. Fudim, J. G. F. Cleland, "A current and future outlook on upcoming technologies in remote monitoring of patients with heart failure," in *Journal of Heart*, 2021. wiley.com

[4] M. Waleed, T. Kamal, T. W. Um, A. Hafeez et al., "Unlocking Insights in IoT-Based Patient Monitoring: Methods for Encompassing Large-Data Challenges," 2023. ncbi.nlm.nih.gov

[5] A. Rahman, M. Karmakar, and P. Debnath, "Predictive analytics for healthcare: Improving patient outcomes in the US through Machine Learning," Revista de Inteligencia, 2023. researchgate.net

[6] A. Olalekan Kehinde, "Leveraging Machine Learning for Predictive Models in Healthcare to Enhance Patient Outcome Management," Int Res J Mod Eng Technol Sci, 2025. researchgate.net

[7] Hashim Elshafie, Ibrahim Al-Qahtani, Abdulilah A;-Ahmari “Energy Efficient Design for Body Sensor Network Applications” the book published by LAB LAMBERT Academic Publishing, is a trademark of Dodo Books Indian Ocean Ltd. And OmniScriptum S.R.L. publishing group. 120 High Road, east Finachley, London, N2 9ED King Str. Armeneasca 28/1. Office 1, Chisinau MD-2012, Republic of Moldova, Europe, ISBN: 978-620-6-84323- 8, Published on /11/2023,

[8] A. J. Zeleke, P. Palumbo, P. Tubertini, and R. Miglio, "Machine learning-based prediction of hospital prolonged length of stay admission at emergency department: a Gradient Boosting algorithm analysis," Frontiers in Artificial, 2023. frontiersin.org

[9] TPT Armand, MAI Mozumder, S Ali, and AO Amaechi, "Developing a low-cost IoT-based remote cardiovascular patient monitoring system in Cameroon," Healthcare, 2023. mdpi.com

[10] M. Umer, T. Aljrees, H. Karamti, A. Ishaq, and S. Alsubai, "Heart failure patients monitoring using IoT-based remote monitoring system," Scientific Reports, 2023. nature.com

[11] A. A. Nancy, D. Ravindran, and P. M. D. Raj Vincent, "Iot-cloud-based smart healthcare monitoring system for heart disease prediction via deep learning," Electronics, 2022. mdpi.com

[12] M. Javaid and I. H. Khan, "IoT(IoT) enabled healthcare helps to take the challenges of COVID-19 Pandemic," Journal of oral biology and craniofacial research, 2021. nih.gov

[13] W. Li, Y. Chai, F. Khan, S. R. U. Jan, and S. Verma, "A comprehensive survey on machine learning-based big data analytics for IoT-enabled smart healthcare system," Mobile Networks and Applications, 2021. springer.com

[14] K. C. Rath, A. Khang, and D. Roy, "The role of IoT(IoT) technology in Industry 4.0 economy," in … and applications in the industry 4.0 …, 2024. [HTML]

[15] L. Tan, K. Yu, A. K. Bashir, X. Cheng, and F. Ming, "Toward real-time and efficient cardiovascular monitoring for COVID-19 patients by 5G-enabled wearable medical devices: a deep learning approach," Neural Computing and ..., 2023. springer.com

[16] J. Mistry and A. Ganesh, "An Analysis of IoT-Based Solutions for Congenital Heart Disease Monitoring and Prevention," Journal of Xidian University, 2023. researchgate.net

[17] N. Gomes, M. Pato, A. R. Lourenco, and N. Datia, "A survey on wearable sensors for mental health monitoring," Sensors, 2023. mdpi.com

[18] R. Jegan and W. S. Nimi, "On the development of low power wearable devices for assessment of physiological vital parameters: a systematic review," Journal of Public Health, 2024. springer.com

[19] S. Ksibi, F. Jaidi, and A. Bouhoula, "A Comprehensive Study of Security and Cyber-Security Risk Management within e-Health Systems: Synthesis, Analysis and a Novel Quantified Approach," 2022. ncbi.nlm.nih.gov

[20] A. Elhadad, F. Alanazi, and A. I. Taloba, "Fog computing service in the healthcare monitoring system for managing the real-time notification," Journal of Healthcare, 2022. wiley.com

[21] Dr. Hashim Elshafie, “Emerging Threats in Internet-of-Things (IoT) Hardware Security” , the book published by LAB LAMBERT Academic Publishing, is a trademark of Dodo Books Indian Ocean Ltd. And OmniScriptum S.R.L. publishing group. 120 High Road, east Finachley, London, N2 9ED King Str. Armeneasca 28/1. Office 1, Chisinau MD-2012, Republic of Moldova, Europe, ISBN: 978-620-8-42482-4, Published on 22/01/2025,

[22] N. Singh, M. Raza, V. V. Paranthaman, M. Awais, and M. Khalid, "IoTand cloud computing," Digital Health, Elsevier, 2021. nih.gov

[23] 10. Hashim Elshafie, Mosab Hamdan, Sayeed Salih, Refan Mohamed Almohamedh, Ala Eldin Abdallah Awouda, Abdelwahed Motwakel, “Emerging Threats in Internet-of-Things (IoT) Hardware Security” IJCSNS International Journal of Computer Science and Network Security, VOL.25 No.4, 4 pp. 27-52April 2025.

[24] Shamimul Qamar,Ashraf M. Abdelrehman, Hashim E. A. Elshafie, Khalid Mohiuddin ”Sensor Based IoT Industrial Healthcare Systems”, International Journal of Scientific Engineering and Science, ISSN (Online): 2456-7361, Impact factor (SJIF): 8.233 , Volume 2, Issue 11, pp. 29-34, 2018

[25] A. Djenna, S. Harous, and D. E. Saidouni, "IoTmeet internet of threats: New concern cyber security issues of critical cyber infrastructure," Applied Sciences, 2021. mdpi.com

[26] M. K. Hasan, T. M. Ghazal, R. A. Saeed, "A review on security threats, vulnerabilities, and counter measures of 5G enabled Internet-of-Medical-Things," IET, 2022. wiley.com

[27] V. Vyasa and Z. Xu, "Maintenance in automotive and aerospace applications–An overview," International Journal of Advances in, 2024. sciencetransactions.com

[28] Z. Wenhua, F. Qamar, T. A. Abdali, R. Hassan, and S. T. A. Jafri, "Blockchain technology: security issues, healthcare applications, challenges and future trends," Electronics, 2023. mdpi.com

[29] J. Leng, X. Yan, and Z. Lin, "Design of an IoTSystem for Smart Hospitals," 2022. [PDF]

[30] S. B. Junaid, A. A. Imam, A. O. Balogun, L. C. De Silva, "Recent advancements in emerging technologies for healthcare management systems: a survey," Healthcare, 2022. mdpi.com

[31] G. F. Huseien and K. W. Shah, "A review on 5G technology for smart energy management and smart buildings in Singapore," Energy and AI, 2022. sciencedirect.com

[32] A. Sawand, S. Djahel, Z. Zhang, and F. Nait-Abdesselam, "Toward energy-efficient and trustworthy eHealth monitoring system," 2015. [PDF]

[33] M. M. Islam, S. Nooruddin, F. Karray, "Internet of things: Device capabilities, architectures, protocols, and smart applications in healthcare domain," IEEE Internet of Things, 2022. [PDF]

[34] M. Lombardi, F. Pascale, and D. Santaniello, "Internet of things: A general overview between architectures, protocols and applications," Information, 2021. mdpi.com

[35] K. Kędzierski, J. Radziejewska, A. Sławuta, M. Wawrzyńska et al., "Telemedicine in Cardiology: Modern Technologies to Improve Cardiovascular Patients’ Outcomes—A Narrative Review," 2022. ncbi.nlm.nih.gov

[36] K. Damman, E. Schwammenthal, "Integration of implantable device therapy in patients with heart failure. A clinical consensus statement from the Heart Failure Association (HFA) and European Heart," *Journal of Heart*, 2024. wiley.com

[37] D. Suhag, "Biomaterials for Cardiovascular Applications," in *Biomaterials for Medical Applications, Volume 2*, 2024, Springer. [HTML]

[38] A. Chaudhary, "IoT(IOT): Research challenges and future applications," Journal of Emerging Trends in Science, 2022. igmpublication.com

[39] P. Ratta, A. Kaur, S. Sharma, and M. Shabaz, "Application of blockchain and IoTin healthcare and medical sector: applications, challenges, and future perspectives," Journal of Food, 2021. wiley.com

[40] N. Pierucci, D. Laviola, and M. V. Mariani, "Remote monitoring and heart failure," European Heart, 2025. oup.com

[41] J. A. Sapp, A. M. Gillis, A. AbdelWahab, and I. Nault, "Remote-only monitoring for patients with cardiac implantable electronic devices: a before-and-after pilot study," Open Access Journal, 2021. cmajopen.ca

[42] N. Varma, F. Braunschweig, H. Burri, and G. Hindricks, "Remote monitoring of cardiac implantable electronic devices and disease management," *Europace*, 2023. oup.com

[43] A. AbdelWahab, I. Nault, S. R. Raj, and E. Lockwood, "Remote monitoring of cardiovascular implantable electronic devices in Canada: survey of patients and device health care professionals," CJC Open, 2021. sciencedirect.com

[44] X. Lu, Y. Yang, and W. Gong, "Challenges of ambient WiFi backscatter systems in healthcare applications," Computer Networks, 2024. [HTML]

[45] M. Osama, A. A. Ateya, M. S. Sayed, M. Hammad, and P. Pławiak, "Internet of medical things and healthcare 4.0: Trends, requirements, challenges, and research directions," Sensors, 2023. mdpi.com

[46] A. Kapoor, A. Vora, and R. Yadav, "Cardiac devices and cyber attacks: How far are they real? How to overcome?," 2020. ncbi.nlm.nih.gov

[47] M. Ienca, G. Valle, and S. Raspopovic, "Clinical trials for implantable neural prostheses: understanding the ethical and technical requirements," The Lancet Digital Health, 2025. thelancet.com

[48] L. Shi, D. Xuan, and M. Jakovljevic, "A review on the evolving environment of medical device real-world evidence

regulation on market access in the USA," Cost Effectiveness and Resource Allocation, 2024. springer.com

[49] M. U. Tariq, "Advanced wearable medical devices and their role in transformative remote health monitoring," in *Transformative approaches to patient literacy and …*, 2024. researchgate.net

[50] C. Segarra, E. Muntané, M. Lemay, V. Schiavoni et al., "Secure Stream Processing for Medical Data," 2019. [PDF]

[51] I. Makhdoom, M. Abolhasan, J. Lipman, R. P. Liu et al., "Anatomy of Threats to the Internet of Things," 2019. [PDF]

[52] I. Jaffar, M. Usman, and A. Jolfaei, "Security hardening of implantable cardioverter defibrillators," 2019. [PDF]

[53] T. Sadad, M. Safran, I. Khan, S. Alfarhood et al., "Efficient Classification of ECG Images Using a Lightweight CNN with Attention Module and IoT," 2023. ncbi.nlm.nih.gov

[54] A. I. Siam, M. Amin Almaiah, A. Al-Zahrani, A. Abou Elazm et al., "Secure Health Monitoring Communication Systems Based on IoT and Cloud Computing for Medical Emergency Applications," 2021. ncbi.nlm.nih.gov

[55] S. A. El-Moneim Kabel, G. M. El-Banby, L. A. Abou Elazm, W. El-Shafai et al., "Securing Internet-of-Medical-Things networks using cancellable ECG recognition," 2024. ncbi.nlm.nih.gov

[56] J. Sriram, M. Shin, T. Choudhury, and D. Kotz, "Activity-aware ECG-based Patient Authentication for Remote Health Monitoring," 2009. [PDF]

[57] L. Cruz-Piris, D. Rivera, I. Marsa-Maestre, E. de la Hoz et al., "Access Control Mechanism for IoT Environments Based on Modelling Communication Procedures as Resources," 2018. ncbi.nlm.nih.gov

[58] E. Constable, J. Gospodaric, and A. Pimenov, "Encoding terahertz holographic bits with a computer-generated 3D-printed phase plate," Scientific Reports, 2024. nature.com

[59] Z. Meng, H. Yan, M. Liu, W. Qin, and G. M. Genin, "Encoding and storage of information in mechanical metamaterials," Advanced, 2023. wiley.com

[60] I. Rigoev and A. Sikora, "Security aspects of smart meter infrastructures," in *Smart Meters: Artificial Intelligence to Support …*, Springer, 2023. [HTML]

[61] D. Kohout, T. Lieskovan, and P. Mlynek, "Smart metering cybersecurity—requirements, methodology, and testing," Sensors, 2023. mdpi.com

[62] M. Rana, Q. Mamun, and R. Islam, "Current Lightweight Cryptography Protocols in Smart City IoT Networks: A Survey," 2020. [PDF]

[63] G. Gaobotse, E. Mbunge, J. Batani, and B. Muchemwa, "Non-invasive smart implants in healthcare: Redefining healthcare services delivery through sensors and emerging digital health technologies," Sensors International, 2022. sciencedirect.com

[64] M. Paul, L. Maglaras, M. A. Ferrag, and I. Almomani, "Digitization of healthcare sector: A study on privacy and security concerns," ICT express, 2023. sciencedirect.com

[65] W. S. Admass, Y. Y. Munaye, and A. A. Diro, "Cyber security: State of the art, challenges and future directions," Cyber Security and Applications, 2024. sciencedirect.com

[66] E. Kwarteng and M. Cebe, "A survey on security issues in modern Implantable Devices: Solutions and future issues," Smart Health, 2022. [PDF]

[67] S. Das, G. P. Siroky, S. Lee, D. Mehta et al., "Cybersecurity: The need for data and patient safety with cardiac implantable electronic devices," Heart rhythm, 2021. nih.gov

[68] L. Wasserman and Y. Wasserman, "Hospital cybersecurity risks and gaps: Review (for the non-cyber professional)," Frontiers in digital health, 2022. frontiersin.org

[69] AU Patel, CL Williams, and SN Hart, "Cybersecurity and information assurance for the clinical laboratory," The Journal of ..., 2023. oup.com

[70] D. Wood, N. Apthorpe, and N. Feamster, "Cleartext Data Transmissions in Consumer IoT Medical Devices," 2018. [PDF]

[71] Ö Aslan, S. S. Aktuğ, M. Ozkan-Okay, A. A. Yilmaz et al., "A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions," Electronics, 2023. mdpi.com

[72] C. S. Yadav, J. Singh, A. Yadav, H. S. Pattanayak, and R. Kumar, "Malware analysis in IoT & android systems with defensive mechanism," Electronics, 2022. mdpi.com

[73] H. Albustanji, "COVID-19 Pandemic Impact on Cyber Threats," Faculty of Organisation Studies in Novo mesto, 2024. researchgate.net

[74] A. Bobbio, L. Campanile, M. Gribaudo, and M. Iacono, "A cyber warfare perspective on risks related to health IoT devices and contact tracing," Neural Computing and …, Springer, 2023. springer.com

[75] Y. Li, G. Cao, W. Jing, J. Liu, and M. Liu, "Global trends and regional differences in incidence and mortality of cardiovascular disease, 1990− 2019: findings from 2019 global burden of disease study," European Journal of ..., 2023. unboundmedicine.com

[76] M. Di Cesare, P. Perel, S. Taylor, and C. Kabudula, "The heart of the world," *Heart*, 2024. nih.gov

[77] D. M. Mathkor, N. Mathkor, Z. Bassfar, and F. Bantun, "Multirole of the internet of medical things (IoMT) in biomedical systems for managing smart healthcare systems: An overview of current and future innovative …," *Journal of infection and …*, Elsevier, 2024. sciencedirect.com

[78] A. M. Ferrick, S. R. Raj, T. Deneke, P. Kojodjojo, et al., "2023 HRS/EHRA/APHRS/LAHRS expert consensus statement on practical management of the remote device clinic," Europace, 2023. oup.com

[79] M. N. Bhuiyan, M. M. Rahman, and M. M. Billah, "IoT(IoT): A review of its enabling technologies in healthcare applications, standards protocols, security, and market opportunities," IEEE Internet of Things, 2021. [HTML]

[80] S. Iranpak, A. Shahbahrami, and H. Shakeri, "Remote patient monitoring and classifying using the IoTplatform combined

with cloud computing," Journal of Big Data, 2021. springer.com

[81] A. Heidari, N. Jafari Navimipour, and M. Unal, "Machine learning applications in internet-of-drones: Systematic review, recent deployments, and open issues," ACM Computing, 2023. [HTML]

[82] F. Subhan, A. Mirza, M. B. M. Su'ud, M. M. Alam, and S. Nisar, "AI-enabled wearable medical IoTin healthcare system: A survey," *Applied Sciences*, 2023. mdpi.com

[83] P.D. Singh, G. Dhiman, and R. Sharma, "IoTfor sustaining a smart and secure healthcare system," in Computing: Informatics and Systems, Elsevier, 2022. [HTML].

Hashim Elshafie is an expert in telecommunications engineering. He earned his Bachelor’s degree in Electronics Engineering with a focus on Telecommunications from Sudan University of Science and Technology SUST. He then pursued advanced studies at Universiti Teknologi Malaysia UTM, where he completed both his Master’s and PhD in Electrical Engineering with a specialization in Telecommunications. From 2013 to 2015, he served as a senior researcher at the MIMOS Center of Excellence in Telecommunications Engineering MIMOS-UTM in addition he was a member of the Telematic Research Group TRG in UTM. Moreover, he gained industrial experience at Malaysian Institute of Microelectronic Systems (MIMOS Berhad), a National Applied R&D Centre in Malaysia, from 2011 to 2013. His research focus in Telecommunication and Networking Engineering, Satellite and Radar Communications, Antenna Engineering and Electromagnetics waves, Wireless Sensor Networks, IoT(IoT), 5G/6G Cellular Systems, Artificial Intelligence (AI), Spectrum Sharing with Cognitive Radio techniques, and TV White Space Management Schemes. Since January 2016, Dr. Elshafie has been an Assistant Professor in the Department of Computer Engineering at King Khalid University KKU in the Kingdom of Saudi Arabia.