Republic of Iraq
Ministry of Higher Education
and Scientific Research
University of Babylon
College of Engineering

Design of health care monitoring system using secure wireless body area network based on Internet of things

A Thesis
Submitted to the Department of Electrical Engineering / College of Engineering / University of Babylon in Partial Fulfillment of the Requirements for the Degree of Master in Science in Electrical Engineering / Communications.

BY
DHUHA AJIL JASSIM
(B.Sc.2022)

Supervised by
Prof. Dr Saad Saffah Hassoon

2023A.D. 1444 A.H.

بِسْمِ اللَّهِ الرَّحْمَٰنِ الرَّحِيمِ

﴿يَرْفَعِ اللَّهُ الَّذِينَ آمَنـــــــُوا مِنكُمْ
وَالَّذِينَ أُوتُـــــوا الْعِلْمَ دَرَجَاتٍ﴾

صدق الله العظيم

سورة المجادلة : 11

Supervisors Certification

I certify that this thesis titled **“ Design of health care monitoring system using secure wirless body area network based on Internet of things”** and submitted by the student (**Dhuha Ajil Jassim)** was prepared under my supervision at the Department of Electrical Engineering / College of Engineering / University of Babylon as a part of requirements for a Master degree of Science in Electrical Engineering/Communications.

Supervisors

Signature:

Name*: Prof. Dr Saad Saffah Hresh*

Date: / / 2023

I certify that this thesis metioned above has been completed in architecture engineering in the college of engineering / University of Babylon .

Signature:

Head of Depatment :

Date: / / 2023

Acknowledgements

Thanks be to God for the insight that inspired me, and praise be to Him for the blessings He has bestowed upon me, and to Him is the credit for achieving what I aspire to in this research. Praise be to God, who by His praise opens every book and by His remembrance every speech is issued, and by His praise the people of blessings enjoy the abode of reward.

*It gives me great pleasure to extend my thanks and gratitude to (****Prof. Dr. Saad Saffah Hasson****), who provided me with the information I needed in my research*

And for the great efforts, he made for me since he proposed the subject of the research and his continuous supervision, and for his advice that helped me a lot in overcoming the difficulties I faced, calling from God success and brilliance in the scientific career.

I would like to extend my thanks and gratitude to the Deanship of the College of Engineering and the Presidency of the Electrical Engineering Department for the facilities and administrative procedures they provided me, which effectively contributed to the completion of the requirements of this research.

.

Researcher

Dedication

With God's help and grace, this research was completed and I dedicate it.

-To the awaited Imam (may God hasten his honorable reappearance) I dedicate first and to the souls of the martyrs, without whom it would not be here.

My parents...may God have mercy on them

My brothers and sisters the arm and the forearm.., I dedicate to you with love and dignity

My dear husband. the one who was the best support in my scientific and research career, and spared no effort in helping me, and he is credited with achieving this achievement through his support and encouragement for my education..

My respected professors, supervisor and faculty members who did not skimp on giving you valuable information and any idea.

My colleagues and comrades who did not skimp on helping me.

Abstract

Recent years have seen a rise in the elderly population (those aged 65 and older) in several countries, as the global population of senior citizens has grown. The ability to undertake remote monitoring of the body's status and the surrounding environment has grown in importance to examine the health status of older individuals who have limited financial resources and access to contemporary medical services. Therefore, it is vital to monitor all movements and bodily activities conducted in daily life. A wireless body area network (WBAN)constitutes one such surveillance system. A WBAN consists of sensors that are either placed around the body or are small enough to be inserted within the body.

Incorporating and embedding WBAN sensors into the Internet of Things (IoT) has been a topic of considerable attention among scholarly and industrial communities due to the revolutionary effect it has had on human existence. The rapid development of IoT technology has altered human existence by introducing, among other innovations, smart gadgets, smart healthcare, smart industry, smart cities, and smart grids.

The rapid development of IoT technology has altered human existence by introducing, among other innovations, smart gadgets, smart healthcare, smart industry, smart cities, and smart grids.

This work aims to design and prove a monitoring system for a patient using Rivest–Shamir–Adleman algorithm (RSA) and transmuting the information over a wireless medium from the patient to the doctor's computer. The proposed system consists of three parts, firstly, three sensors have been considered, which are heart rate, temperature, and sound. Secondly, the security system processes the data and encrypted using the RSA algorithm which can be sent over the internet to the remote doctor.

Finally, the data is stored and processed, de-encrypted in the cloud, and then resolved to be displayed on the doctor's PC. In the doctor's computer, data are displayed using a new proposed platform which includes patient age, patient gender, heart rate, temperature, and cough sound.

In addition, the system performance was analyzed using simulation tools by Matlab. In the simulation Bit error rate (BER) is considered a performance to show the effect of using the RSA algorithm on the performance.

The proposed system shows that data can be transmitted over a wireless medium and the internet with a high performance of reliability and security compared to the recent work, then developed a new user interface to display patient data efficiently

List of Contents

List of Contents

List of Contents

Chapter Four: Result and Discussion

Chapter Five :Conclusion and Future Works

List of Tables

List of Figures

List of Figures

List of Abbreviations

Abbreviation	Definition
6LoWPAN	IPv6 over Low-Power Wireless Personal Area Networks
AEAD	authenticated encryption with associative data
API	application programming interface
ARQ	Automatic repeat request
AS	adaptive switching
AVISPA	automated validation of Internet security-sensitive protocols and applications.
AWGN	Additive white Gaussian noise
BCS	Body Care System
BER	bit error rate
BSN	Body sensor network
CoAP	Constrained Application Protocol
COS	Commercial off the Shelf
CVD	Cardiovascular Disease
DES	Data Encryption Standard
DF	decryption failure
DIP	dual in-line package
DTM	Direct transmission mode
ECG	Electrocardiography
HR	Heart Rate
HRM	heart rate monitor
HRS	heart rate sensor
HSN	Hybrid Sensing Network
HTTP	Hypertext Transfer Protocol

List of Abbreviations

Abbreviation	Definition
IaaS	Infrastructure as a Service
IoMT	Internet of medical Things
IoT	Internet of Things
IoT-SIM	IoT-based Semantic Interoperability
MN	master node
MySQL	It is a relational database management system based on SQL
NSA	The National Security Agency
OS	Operating System
PaaS	Online Platform Service
PGP	Pretty Good Privacy
PPG	Photo plethysmography
RAPCHI	Robust authentication protocol for IoMT-based cloud-healthcare infrastructure
RDF	Resource Description Framework
REST	Representational state transfer
RFID	Radio-frequency Identification
ROM	Random oracle model
RSA algorithm	(Rivest–Shamir–Adleman) algorithm
RTDs	Resistance Temperature Detectors
SaaS	Software Service
SCOS	cough sound sensor
SHS	Smart Hospital System
SK	Session key
SM	smart mobile

List of Abbreviations

Abbreviation	Definition
SNR	Signal-to-noise ratio
SPARQL	Protocol and RDF Query Language
SPO2	The concentration of oxygen in the blood
SQL	It is a computer language for working with sets of facts and the relationships between them.
SW-SSS	Slepian -Wolf-coding-based secret sharing
TCMN	Two cognitive master nodes
TS	body temperature sensor
UHF	Ultra high frequency
VLSI	Very large-scale integration
VM	virtual machine
WBAN	wireless body area network
WHO	World Health Organization
WMSNs	Wireless medical sensor networks
WSN	wireless sensor network

Chapter One

General Introduction

CHAPTER ONE
GENERAL INTRODUCTION

1.1 Back ground

A sensor network, commonly referred to as a wireless sensor network (WSN), is a multihop self-organizing network system made up of several reasonably priced mini-sensor nodes that are wirelessly dispersed around the detecting area. The goal of a WSN is to gather, analyze, and send data to an observer from sensing objects inside the network's coverage region [1-4]. Smart healthcare is only one of the many businesses that have adopted the WSN, which is a crucial element of the Internet of things. A universal medical system that can quickly verify patient emergencies through the remote monitoring function and enhance patient care quality may be built using wireless medical sensor networks (WMSNs) [5].

Medical sensors are physically affixed on patients in a WSN-based healthcare system, and the collected data are subsequently sent securely to authorized parties. However, the wireless medical sensor network's sensors have limited storage and computing capabilities, thus collecting too much data may compromise the network's ability to analyze data in real-time [6].

Typically, sensor nodes are low-resource devices with networking, computation, and storage capabilities. Additionally, sensor nodes are often dispersed in an area with a low population. Academics are very concerned about the security of wireless sensor networks, especially in WMSN where sensitive patient-specific private data makes security, privacy, and medical data problems more important. Before the whole process may be used and run effectively, many challenges must be overcome. The main challenges that need to be addressed and managed with care include preserving the integrity of the medical data gathered from sensor nodes, ensuring that only authorized users have safe access to this data, and preventing the exploitation of data conveyed over public channels. Data transferred between parties must be guaranteed to be private and accurate [7].

Body sensor network (BSN) The most current technological advancements in WBAN systems may be used for the early diagnosis and prevention of diseases that may emerge later in people's lives. Wireless body area networks (WBAN) are one kind of WSN. The implementation of sensor nodes on WBAN for continuous health monitoring makes this feasible [8]. In WBAN, on the body or in clothes, sensors may be worn [9-10]. It is possible to measure aspects of the human body with these sensors. The measured data may be collected and transferred to the main server where the medical applications reside.

The Internet of Things (IoT) is a network of electronic, computational devices, and digital that are all interconnected and capable of moving data over a defined network without the aid of humans at any level [9].

BSN and IoT technology has been intertwined with healthcare for a while. However, the public acceptance of small wearable biosensors and the rapid expansion of the Internet of Things has opened up new horizons for personalized e-health and services. With wearable devices and smart healthcare services as examples, a smart service in healthcare may collect many types of data used in a sensor layer or physical or wearable electronic devices equipped with sensors. All data can be sent to the cloud or to the server that hosts it over the wireless network at the network layer. True healthcare services are provided by the service layer, which also manages patient data on their heartbeat, blood pressure, and blood sugar levels.

A system's security is one of its most vital components. People have diverse perspectives on security, and as a result, it is defined in several ways. In general, security is a notion comparable to system-wide safety. Currently, the majority of communication in sensor network applications (such as the body sensors network, or BSN) in healthcare is wireless. This may provide a variety of security risks to these systems. These are the security concerns that might cause significant difficulties for wireless sensor systems [10].

1.2 Literature review

Increasing rates of population aging have posed several difficulties for healthcare providers. For example, A new issue that requires a long-term commitment of medical and human resources is stroke rehabilitation for the elderly [11]. A relatively recent specialty, medical rehabilitation was developed in the middle of the 20th century. It has been considered a brand-new field of therapy that focuses on recuperating or rebuilding impairments to lessen or cure bodily or mental dysfunctions. It has been identified as an excellent method for enhancing the bodily functioning of several patients sorts. However, there are a few hurdles to the expansion of medical rehabilitation's spectrum of applications. Initially, the majority of rehabilitation treatments require extensive, long-term therapy. To give patients easier access to rehabilitation services, more assistive facilities are needed. The aging population in today's society is growing at a quicker rate than the availability of resources for rehabilitation, making them more limited.

Using the Internet of Things (IoT) to improve healthcare systems is a viable solution to the aforementioned problems. In recent years, the use of Internet-based technology for rehabilitation services has increased in popularity [12] due to the development of fresh concepts such as the Smarter Planet and the Smart City.

In [13] a secure healthcare system built on the IoTs makes use of the BSN architecture. By creating two communication channels for assuring transmission secrecy and providing entities in open IoT-based communication networks, system efficiency, and transmission resilience may be achieved concurrently.

In [14] Innovative, (IoT)-aware, intelligent architecture that allows autonomous, real-time monitoring and tracking of patients, personnel, and biological devices across hospitals and nursing institutions. A Smart Hospital

System (SHS) is suggested in line with the IoT vision. It employs RFID, WSN, and Smart Mobiles (SM), among other complementary technologies. These communicate using a CoAP/6LoWPAN/REST-based network architecture. The SHS contains a node-based ultra-low-power hybrid sensing network (HSN) that is based on 6LoWPAN to collect real-time physiological data from patients as well as ambient factors. The capability of UHF RFID is also included.

In [15] For a cognitive cooperative communication system, two cognitive master nodes (TCMN) are suggested. These nodes may speed up the retransmission process and prevent collisions. First, an extensive investigation of a scheme's network architecture is conducted. Second, the suggested protocol's connection and outage probabilities are represented mathematically and generated. Third, Throughput, energy use, and end-to-end latency are all examined and studied. The simulation and numerical findings show that the TCMN can use the Direct Transmission Mode (DTM) and previously finished work to run its system under normal operating conditions.

In [16] Utilizing the information provided by the random forest model, a technique is shown that is efficient enough to predict outcomes and accurate enough to track patients' sleep using Commercially Accessible Sensors (COS). With the use of this technological innovation, snoring patterns, as well as the patient's body movement, heartbeat, and SPO2 level (the amount of oxygen in the blood required for optimum biological function) may be evaluated. The computer system receives real-time data transfer. The recommended technique makes it easy and affordable to evaluate patients' sleep habits, improving patient treatment. This study demonstrates how to apply a smart, resource-efficient Internet of Things-based sleep quality monitoring system on a variety of participants.

In [17] This study proposes a wearable fabric platform based on open hardware and software that wirelessly collects data about users' movements and heart rates and uploads it to cloud infrastructure open for monitoring and analysis. People who wish to track their health and fitness without intrusive equipment should wear this platform. The approach that is being suggested has the potential to enable senior citizens and other individuals who need continual medical attention to live freely.

In [18] This research examines the process of developing a framework for mobile cloud telemedicine as well as an evaluation of the possible performance of such a framework. The huge processing capacity of the cloud is combined with the local, real-time monitoring capabilities of Android mobile devices to accomplish this goal.

In [19] To facilitate semantic interoperability across various IoT devices in the healthcare sector, we proposed an IoT-SIM or IoT-based Semantic Interoperability Model. Doctors interact with a range of IoT devices to check the current health status of their patients. Information that has been semantically tagged is meaningfully communicated between the doctor and the patient. A straightforward method for semantic annotation of data using heterogeneous IoT devices is presented to provide annotations for the data. A semantic web framework called Resource Description Framework (RDF) is used to link objects using triples to give them semantic meaning. Data from patients with RDF annotations have been made semantically interoperable. From an RDF graph, records are extracted using a SPARQL query. Tools like Tableau, Gruff-6.2.0, and Mysql were used to simulate the system.

In [20] To stop these kinds of assaults, a useful architecture called Privacy-Protector—patient privacy-protected data collection—is given in this study. For the protection of patient data, Privacy-Protector incorporates the concepts of secret sharing and share mending (in the event of data loss or compromise). The Slepian-Wolf-based secret sharing (SW-SS) has been used in privacy-protection for the first time. The design employed a distributed database made up of several cloud servers, which guarantees that patient data privacy may be safeguarded so long as one of the servers is secure. Present a patient access control system as well, wherein many cloud servers work together in a common framework to give healthcare professionals patient data without disclosing the details of the data. The Privacy-Protector framework is safe and privacy-protected against a variety of assaults, according to the privacy performance study.

In [21] We advocate shifting the focus of healthcare from clinics to patients and streamlining communication between all parties, including the healthcare facility, the patient, and the services provided. IoT with a main focus on patients The electronic Health ecosystem requires a multi-layer design that incorporates devices, fog computing, and managing complex data for clouds in terms of diversity, speed, and data latency. This is required for the healthy functioning of the ecosystem. Several case studies of services and applications are developed on those tiers after this fog-driven IoT architecture. This area comprises, among other things, assisted living technology, medicine electronic, implants and early warning systems, mobile health, smart cities, and population monitoring. This article will discuss the challenges that Internet of Things (IoT) electronic health confronts in the management of data, scalability, legality, interoperability, device-network-human-interfaces, security, and privacy.

In [22] The Adaptive Switching (AS) algorithm is a one-of-a-kind adaptive access approach. The algorithm for adaptive switching (AS) is a unique adaptive access approach. This methodology is based on the adaptive selection of either the well-known Go-Back-N or Selective Repeat algorithms. Using the resulting MATLAB simulation, the throughput performance of the suggested approach is evaluated and compared to that of the Go-Back-N and Selective Repeat ARQ strategies currently in use. It has been determined at what speed the network should transition from the Selective Repeat to Go-Back-N technique or from the Selective Repeat to Go-Back-N approach to achieve the desired level of throughput performance.

In [23] For telecare medical information systems, a brand-new resource-efficient AKE approach called REAS-TMIS is recommended. It makes use of a hash function and Authenticated Encryption with Associative Data (AEAD). For encrypted communication among IoT devices with limited resources, AEAD schemes were developed expressly for this purpose. REAS-TMIS is resource-effective due to these AEAD characteristics. Additionally, REAS-TMIS does away with the computationally costly processes of elliptic curve point multiplication and chaotic map. In addition, after verifying the user's validity, REAS-TMIS provides Session Key (SK) setup capabilities for usage in future encrypted communications between MS and users. The well-known random oracle concept is used to confirm SK's security.

In [24] For CHI using the Internet of Medical Things (IoMT) during a pandemic, a safe and compact authentication technique (RAPCHI) based on cryptographic primitives is described. The proposed framework is more secure than current frameworks and resistant to a variety of security risks. The Random oracle Model (ROM) and two different techniques are used to validate the formal security analysis of RAPCHI in the study. Further, the study uses the simulation programming language AVISPA to demonstrate that RAPCHI is resistant to man-in-the-middle and reply attacks. In addition, the study finds that RAPCHI is comparatively light in terms of computation and communication when compared to equivalent frameworks. These results suggest that the proposed paradigm is viable for usage in real-world circumstances.

1.3 Problem Statement

Where security is a serious challenge wherever large-scale networks are installed. IoT-based healthcare solutions work with data about people. Even if it was obtained from harmless wearable sensors, major privacy issues might still affect this data. Two of the most pressing concerns in IoT-based healthcare applications are data security and patient privacy. This is because wireless connections and devices constitute the vast majority of connected devices.

In this research project, an Internet of Things (IoT) in a healthcare system that is hosted in the cloud is created, and its theoretical and practical vulnerabilities are investigated. Data may be communicated through wireless media and received by an authorized doctor, as has been shown. The doctor can show the patient's status and other meta data securely.

1.4 Thesis Objectives

This thesis is comprised of two parts, a theoretical part, and an experimental part, where the theoretical part is explained as:

- Design and suggested new WSN system-based IoT healthcare.
- Working with the RSA algorithm as a reliable solution for the IoT-cloud healthcare system.

The experimental parts :

- To detect coughs, measure temperatures, and record heartbeats, three sensors are utilized: voice, body temperature, and heartbeat sensors.
- Data is transferred via the wireless channel from the sensors to the computer, where it is encrypted using the RSA algorithm.
- The data is uploaded to the cloud after encryption.
- Data is also authenticated with a user name and password at end user devices, hospital or doctor devices.
- At the doctor device's end, all the data collected by the sensors is shown.

1.5 Thesis Aim

1. Implementation of the Internet of Things in the cloud-hosted healthcare system.
2. Receive patient data using sensors, encrypt it with the secondary computer, and transmit it to the cloud.
3. The data is received and decoded only by the attending physician, who performs the necessary actions for each case

1.6 Thesis outlines

This thesis comprised of the fifth chapters, and summarized as follow :

Chapter 1: a description of the cloud and the Internet of Things in the healthcare sector.

Chapter 2: a literature review on The IoT health care systems that are now available.

Chapter 3: the suggested system from the perspectives of both theory and experiment.

Chapter 4: the results and discussion

Chapter 5: conclusion and future works

Chapter Two

Theoretical

CHAPTER TWO

Theoretical Introduction to Body Area Monitoring System

2.1 Introduction to Body Care System (BCS)

In every civilization, the elderly require greater health services and care facilitation. Thus, the evolution of science has made it easier to monitor the aged, as well as the general population. According to the World Health Organization (WHO) study, cardiovascular illnesses accounted for 30% of global deaths. Without regard to time, the vital indications of health control and detection were the most intriguing topic. In hospitals, at home, and even when patients are being transported and vital signs are being transmitted to the medical database, the wireless body area network (WBAN) monitors human physiological markers. The majority of energy is expended during the data transfer process on communication. Therefore, the enhancement of data transport is of the biggest importance [25].

Wireless body sensor networks are comprised of several types of biological sensors. This network's sensors are installed on various body areas and may be implanted or covered. Each of these sensors must meet specified standards to detect and record indications. A sensor network is typically capable of recognizing sensors with faults brought on by the failure or loss of energy sources by using fault-tolerant design strategies at each level of data processing or data transmission by a sensor. For example, in collaborative data collection systems, an energy-efficient sensor may send insufficient data or no data to the center at different times. So, this sensor will make the final decision in the middle more difficult. These networks can identify false sensors by employing a variety of methods, such as giving each sensor a reputation or identifying outlier data and data mining in the center's output. The majority of the aforementioned approaches also rely on the fact that the number of sensors in the network is insufficient, the number of environmental measurements is unrestricted, and the network latency is ineffective. Due to the limited number of sensors in WBSN networks, it is typically difficult to identify defects using the aforementioned techniques [26].

In general, a sensor from the WBSN network consumes energy during one of the three phases of its operation:

1. When measuring the environment.
2. When information is being processed or stored.
3. A data center or other sensors are being connected.

Hardware problems, as well as the electrical and physical architecture of the relevant sensor, must be observed during the analysis of the first two scenarios. The majority of a WBSN network's sensor's energy is extracted and sent when interfacing with the environment, on the other hand. To this end, the current study concentrated more on a review of contemporary methods of transmission and communication in the transmission of one sensor of the WBSN network while telemedicine monitored patient vital signs in the field of medical care systems. Due to its importance in the field of human health and the difficulties of its implementation, this research examined and implemented wireless sensor networks that were installed on the body [27].

In body sensor networks, sensors are put on the bodies of patients to monitor their vital signs and detect movement. Examples of these sensors are motion sensors and ECG sensors. A variety of biosensors make up the body sensor network. A wireless body sensor network not only tracks patients' vital signs but also gives them real-time feedback so they may track the course of their illness and take the necessary preventative measures. A wireless body sensor network is a component that is put on the patient's body as a case sensor network. RFID tags and electrocardiogram sensors can be thought of as parts of the body sensor network. Wireless sensor networks and body sensor networks share several difficulties and potentials. Body sensor networks give doctors the ability to continuously check patients' health in physiologically normal circumstances without interfering with their daily activities. All body sensor networks employ cheap, many, tiny nodes with communication and computation capabilities as well as the information they gather to diagnose illnesses and recommend treatment. The unique possibility that these networks provide to transfer medical treatment from the hospital setting to the patient's home environment is what makes the usage of body sensor networks in medical contexts significant [28].

The increase of wireless network penetration becomes logically more, simpler, and less expensive as hardware and software technologies progress. But because of this issue, operational sensors within these networks require more battery power and have a shorter usable life [29].

2.2 IoT in Healthcare Systems;

The Internet of Things (IoT) has received much investigation and is now a proven technology standard. Currently, sensors are employed in practically all goods, from ordinary items to industrial monitoring systems. It has been noticed that the use of sensor-based Internet of Things (IoT) technology in intensive healthcare systems is quickly rising. The Internet of Things facilitates a simpler, more intelligent, and more productive lifestyle. The data processing platform of the prototype model is a smartphone; this was done so that user-friendly voice recognition capabilities and alarm features could be provided [30].

IoT-based technologies make it simple to monitor several fatal illnesses. Cardiovascular illnesses, or CVDs, are very prevalent and account for the vast majority of deaths worldwide. As a direct result of the revolution in information and technology, there is now a growing need for health monitoring solutions that are accessible by smartphone. It is conceivable to collect and transmit real-time health data to both patients and healthcare practitioners using these technologies. Everybody needs to be allowed to assess their health, and in times of crisis, they should be urged to seek quick medical treatment. Long-term medical costs for the country may be reduced by the adoption of these monitoring systems. Given the widespread availability of mobile internet connections, it is fairly straightforward to combine a mobile internet connection with an open-source Android health care system [31]. Electrocardiography, often known as an ECG, has become a common diagnostic test that everyone may have. This development has been placed in the last several decades. Electrocardiograms can correctly assess heart function due to their ability to detect the small voltage difference created by cardiac muscle. With the help of a smart gadget, medical professionals and patients may continually monitor heart rates, gather vital information, and take appropriate action to avoid grave harm. Some of the most crucial physical characteristics of the human body, such as heart rate and body temperature, play a significant role in establishing a patient's state of health [32].

Our health monitoring system's integration of IoT has given us a substantial competitive advantage in the creation of modern medical treatments. Smaller sensors as a result of VLSI technical breakthroughs have eased the development of wearable solutions. The devices are growing more effective and powerful as a result of constant internet connectivity. Internet of Things-based medical monitoring gadgets keeps a close eye on a patient around-the-clock, every day of the week [32], [33].

The gadgets analyze statistical data to produce the required signals at any important point. Patients may be monitored remotely and emergency actions can be performed since IoT-based gadgets are always linked to the internet. Therefore, Detection and emergency response services can be provided by IoT-based devices. IoT-based health monitoring systems are very different from traditional health monitoring systems. It can be difficult to integrate IoT into health monitoring systems [34].

Here are a few of the difficulties: Most IoT initiatives have not yet been put into practice satisfactorily. IoT creates enormous amounts of data that need to be managed properly using specialist big data and data warehouse technologies. IoT systems face significant security challenges. If security mechanisms are flawed or antiquated, hackers might readily get critical personal information from users. Infrastructural systems that are outdated and do not adhere to current security procedures might cause issues [35].

2.3 Encryption

In cryptography, encoding data is the process of encryption. By using this method, the data is converted from its original plaintext representation into a different version called ciphertext. The ability to convert ciphertext to plaintext and access the original data should only be available to persons with the appropriate authorization. Even though encryption doesn't prohibit interference by itself, it does make it more difficult for a possible interceptor to interpret the data [36].

Due to technological restrictions, a pseudo-random encryption key produced by an algorithm is often employed in encryption techniques. Without the key, it is feasible to decryption the message, but doing so requires a lot of computer power and expertise for a well-designed encryption system. Communication may be quickly decryption by an authorized recipient using the key that the sender sends to recipients but not to unauthorized users. On the other hand, this key is inaccessible to unauthorized users [37].

Numerous different kinds of encryption have been used successfully in cryptography throughout its development. Many types of encryption, especially simpler ones, were originally used by the military. Since that time, new methods have been created, and they are presently being used in many settings throughout the whole modern landscape of computer technology. Modern encryption systems use both the public-key and symmetric-key ideas [38].

Encryption is a method used in cryptography to maintain secrecy. Sensitive information, like passwords and private communications, may be accessible to prospective interceptors since data may be viewed online. Keys are used in the encryption and decryption of communications. Symmetric keys and public keys (also known as asymmetric-key) are the two primary types of keys used in cryptography. Simple modular arithmetic is frequently used in the development of complicated encryption algorithms [38].

The encryption key is made public in public-key encryption systems so that anybody may use it to encrypt communications. The decryption key, however, which permits communications to be read, is only known to the person that is receiving them. Before public-key encryption was introduced in 1973, every encryption technique employed symmetric keys (also called private-key). The subsequent publication of Diffie and Hellman's work was in a journal with a sizable audience, and the benefits of their method were detailed in-depth. The Diffie-Hellman key exchange is the name given to this technique [39].

RSA is a popular public-key cryptosystem. It was developed in 1978 and is being utilized today for uses involving digital signatures. The RSA algorithm chooses two prime integers based on number theory, which aids in producing both the encryption and decryption keys. Phil Zimmermann created Pretty Good Privacy (PGP) in 1991, a public-key encryption program that is freely accessible and comes with the source code. Symantec acquired PGP in 2010 and updates it frequently [40].

In the twenty-first century, encryption is used to safeguard digital data and information systems. Over time, as processing power has grown, encryption technology has also progressed and become safer. However, this technological development has also brought to light a possible drawback of current encryption techniques [41].

The size of the encryption key determines how strong the encryption mechanism is For example, Data Encryption Standard (DES), the first encryption algorithm, used a 56-bit key with 2^56 possible combinations. A 56-

bit key is no longer safe given today's computer capability since it may be broken via a brute force assault [42].

Large volumes of data may be processed concurrently thanks to quantum computing, which makes use of quantum physics' features. Quantum computing has the potential to function hundreds of times more quickly than current supercomputers. The encryption technology of today faces a challenge from this computational power. For example, extremely large prime numbers are multiplied to produce a semiprime number that serves as the public key for RSA encryption. This semiprime number has to be factored in to decode this key without its private key, which can take so much time on contemporary computers.

The computation of this key would need a special computer for weeks or months. However, this semiprime integer can be factored by quantum computing using quantum algorithms in the same amount of time as conventional computing. All data currently secured by public-key encryption would thereafter be exposed to quantum computing assaults. In addition, several types of encryption, including elliptic curve cryptography and symmetric key encryption, are susceptible to the threats presented by quantum computers [43].

Although quantum computing as it stands now is still quite restricted, it may one day pose a challenge to the security of encryption. Large volumes of code cannot be handled by quantum computing, which is presently not commercially viable because quantum computers are only computational devices. Furthermore, the development of quantum computing will also allow for the support of encryption. The National Security Agency (NSA) is currently developing standards for post-quantum encryption. As a countermeasure to the threat presented by quantum computing, quantum encryption has the great potential [44].

2.4 RSA Encryption

One of the primary methods to safeguard information security is the use of cryptographic techniques. Its primary function is to protect sensitive data, but it also handles other system security tasks including authentication, digital signatures, and secret storage. Using this technology, both encrypted and decrypted data may be protected against tampering, forgery, and counterfeiting. When an encryption key is compromised, anybody with access to the system may decode the data, rendering the technology useless. The encryption key is the most crucial part of the whole operation. To that end, careful consideration must be given to the selection of key data, the distribution of the private key, and the storage of both sets of data transmission keys throughout the encryption and decryption processes. The author of this piece, who is well-versed in the RSA public key algorithm, offers advice on how to build a complete and useful RSA encrypt/decrypt solution. Additionally, a thorough explanation of the encryption method and code implementation is provided [45].

The RSA algorithm has been used as a possible authentication method in the ISAKMP / Oakley authentication framework. A critical element of the system is the key exchange algorithm, Diffie-Hellman. First, the participants engage in conversation and use the Diffie-Hellman method to produce shared keys for the session. The next steps of the key agreement protocol will make use of these previously established shared keys [46] [47].

In addition to protecting the information's confidentiality, the encryption and decryption system may also guarantee the data's integrity and authenticity, which would be useful in avoiding forgeries and knockoffs. The total security of the encryption and decryption process relies on the rigor of the mathematics, the internal organization of the algorithm, and the secrecy of the key.

Information security is a major problem in many fields; this article presents a thorough examination of how cryptography, encryption, decryption, RSA public key, and other related technologies have been put to use in these and other fields.

It uses the example of RSA file encryption to show how important RSA mathematical approaches are in the IT sector while also highlighting its limitations. This kind of public-key encryption is known as RSA. It covers topics of how to apply RSA information security issues to one's everyday life. It also covers the principles of data encryption and decryption as well as an explanation of how RSA is utilized. In response to the increasing use of RSA encryption, a new program intended to enhance the RSA algorithm was finally made available to the public [48].

2.5 RSA implementation

The four phases of the RSA algorithm are key generation, distribution, encryption, and decryption. If three very large positive numbers are found, e, d, and n, So that the regular exponent (m) is true for all integers, then RSA is used to observe one of its basic principles. Equasion (1) is used to observe

$(m^e)^d \equiv m \ (mod\ n)$………………………………………..........(1) (with $0 \leq m < n$)

It might be quite challenging to find (d) even when one knows (e, n, or even m), in this case, the triple bar (≡) stands for modular congruence. The condition for modular congruence is that the remainders resulting from dividing{ (m^e)×d} by n and m by n must have comparable values. This property indicates modular congruence. Additionally, it is useful for particular operations because this connection also implies that the two exponentiations can be varied in sequence in eq (1).

RSA employs both a public key and a private key. The public key, which is used to encrypt messages, is available to everyone. It is intended that utilizing the private key is the only way to quickly decode communications encrypted using the public key. The private key is represented by the integer d, whereas the public key is represented by the numbers n and e. However, since n is used at several points during the decryption process, it is feasible that it may also be regarded as a component of the private key. The word "message" is shortened to the letter M.

2.5.1 RSA Key generation

The following process is used to create the RSA algorithm's keys:

1. First, P and Q should be two separate prime numbers (numbers p and q be selected at random).
2. Compute

   $n = p \times q$ ……………………………………………………...(2)

   (The modulus for both the public and the private keys is n). where n is a number that has been revealed publicly and is included in the public key.
3. Compute λ(n), where λ is Carmichael's totient function.
4. Choose an integer e such that 1 < **e** < λ(n). where, **e** having a short bit-length and small Hamming weight results in more efficient encryption – the most commonly chosen value for e is 2^{16} + 1 = 6553.
5. Then, **e** is released as part of the public key.
6. Determine d from the equation bellow

   $d \equiv e^{-1}$ …………………………………………………(3)

   (mod λ(n)); that is, d is the modular multiplicative inverse of e modulo λ(n).

   In the original RSA paper, the Euler totient function

   $\varphi(n) = (p - 1)\ (q - 1)$………… ………………………… (4)

is used instead of λ(n) for calculating the private exponent d. Since φ(n) is always divisible by λ(n), the algorithm works as well. The possibility of using the Euler totient function results also from Lagrange's theorem applied to the multiplicative group of integers modulo p×q. Thus any d satisfying d×e ≡ 1 (mod φ(n)) also satisfies d×e ≡ 1 (mod λ(n)), However, computing d modulo φ(n) will sometimes yield a result that is larger than necessary (i.e., d > λ(n)). Most of the implementations of RSA will accept exponents generated using either method (if they use the private exponent d at all, rather than using the optimized decryption method based on the Chinese remainder theorem described below), but some standards such as FIPS 186-4 may require that d < λ(n). It is always possible to reduce the size of an "oversized" private exponent modulo n to get a smaller equivalent exponent if the exponent does not meet this requirement.

Since any common factors of (p − 1) and (q − 1) are present in the factorization of n − 1 =(p×q) − 1 = (p − 1) (q − 1) + (p − 1) + (q − 1), it is recommended that (p − 1) and (q − 1) have only very small common factors, if any, besides the necessary 2. The authors of the original RSA paper carry out the key generation by choosing d and then computing e as the modular multiplicative inverse of d modulo φ(n), whereas most current implementations of RSA, such as those following PKCS#1, do the reverse (choose e and compute d). Since the chosen key may be short, but the calculated key is, the method used in the RSA article prioritizes decryption above encryption. In contrast, the contemporary technique promotes encryption above decryption.

2.5.2 RSA Encryption and decryption

The distribution of keys is a requirement for the implementation of our strategy. In this example, we will assume that (B) has something to convey to(A) and want to do it through messaging. In the case that they choose to work using RSA, (B) will need access to (A) the public key to encrypt the message, and (A) will need access to (B) the private key to decode the encrypted message. To allow (B) to transmit encrypted messages, (A) shares her public key (n, e) with him across a private but sometimes open channel. There will be moments when the public may use this channel. No one ever finds out who (A) is or where she hid key (d).

Here is a description of how encryption works: Having (A) a public key will allow (B) to contact her via M. To do it, He first uses an agreed-upon reversible technique known as a padding scheme to convert M (strictly speaking, the un-padded plaintext) into an integer m (strictly speaking, the padded plaintext), such that $0 \leq m < n$. Then he deciphers (A) message using her public key e to get at the ciphertext c.

$$c \equiv m^e \ (mod\ n)\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad (5)$$

Modular exponentiation enables this to be completed quite rapidly, even for very big integers. Then (B) sends c to (A). Observe that a ciphertext with c equal to m will result from at least nine different values of m, yet this is unlikely to happen in real life.

Then, the summary of the decryption process is as follows: Using her private key exponent d,(A) can compute m from c.

$$m \equiv c^d (mod\ n)\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad (6)$$

Given m, can recover the original message M by reversing the padding scheme.

2.5.3 Numerical example

Here is an example of RSA encryption and decryption. The parameters used here are artificially small, but one can also use OpenSSL to generate and examine a real keypair.

1. Choose two distinct prime numbers, such as

   $p = 61 \ and \ q = 53$.

2. Compute n = p×q giving

   $n = 61 * 53 = 3233$.

3. Compute Carmichael's totient function of the product as

λ(n) = lcm(p − 1, q − 1) giving

$$\lambda(3233) = lcm(60,52) = 780.$$

4. Choose any number 1 < e < 780 that is coprime to 780. Choosing a prime number for e leaves us only to check that e is not a divisor of 780.

$$let\ e = 17\ .$$

5. Compute d, the modular multiplicative inverse of e (mod λ(n)), yielding

$$d = 413, as\ 1 = (17 * 413) mod\ 780.$$

The public key is (n = 3233, e = 17). For a padded plaintext message m, the encryption function as in eq. 5

$$= m^{17}\ mod\ 3233.$$

The private key is (n = 3233, d = 413). For an encrypted ciphertext c, the decryption function as in eq.(6)

$$= c^{413}\ mod\ 3233.$$

For instance, to encrypt m = 65, then calculate

$$c = 65^{17}\ mod\ 3233 = 2790.$$

To decrypt c = 2790, then calculate

$$m = 2790^{413}\ mod\ 3233 = 65.$$

Using the modular exponentiation square-and-multiply approach, each of these computations may be performed quickly. It would be simple to factor n = 3233 (obtained by the publicly accessible public key) back to the primes p and q in our example, even if in reality the primes chosen would be considerably bigger. The private key is then retrieved by inverting e, which was also generated from the public key, to produce d. Modulus of factors calculations may be sped up by using the Chinese remainder theorem, which has many practical uses (mod p×q using mod p and mod q).

The components of the private key, d×p, d×q, and q_{inv}, may be calculated using the formula below:

$d_p = d\; mod(p-1)$……………………………………………..…….(7)

$= 413\; mod(61-1) = 53,$

As in eq.(7)

$= 413\; mod(53-1) = 49,$

$q_{inv} = q^{-1}\; mod\; p$……………………..……………………….(8)

$= 53^{-1}\; mod\; 61 = 38$

$\Rightarrow \left(q^{inv} * q\right) mod\; p = 38 * 53\; mod\; 61 = 1.$

The following describes how to effectively employ dp, dq, and qinv for decryption (encryption is effective by selecting an appropriate d and e pair):

$m_1 = c^{d_p}\; mod\; p$…….……………………………….……………..(9)

$= 2790^{53}\; mod\; 61 = 4,$

$m_2 = c^{d_p}\; mod\; q$…………………………………………………..…(10)

$= 2790^{49}\; mod\; 53 = 12,$

$h = \left(q_{inv} * (m_1 - m_2)\right) mod\; p$……………………………………..(11)

$= (38 * -8) mod\; 61 = 1,$

$m = m_2 + h * q$…………………………………………………………(12)

$= 12 + 1 * 53 = 65.$

2.6 Cloud Computing

Cloud computing is the on-demand availability of computer system resources, particularly data storage (cloud storage) and processing power, without the user's direct administration. Large clouds often spread their services across many sites, each of which is a data center. Cloud computing depends on resource sharing to accomplish coherence and often uses a "pay-as-you-go" approach, which may aid in decreasing capital expenditures but may also lead to unanticipated running expenses for uninformed users [49].

All of the following defining features are shown by the cloud computing model:

- By allowing users to more easily re-provision, add, and grow their technical infrastructure resources, cloud computing has the potential to boost an organization's overall agility.
- Cost savings are introduced by cloud service providers. In a public cloud-based delivery model, upfront investments like those made in hardware, such as servers, are transformed into recurring operating expenditures. Since infrastructure is generally supplied by a third party, and hence does not need to be acquired for rare or one-time demanding computer functions, this is said to reduce barriers to entry. Many different pricing models may be used in the realm of utility computing. These can range from "fine-grained" models to models that are based on the amount of actual usage. As well, as reduced internal Implementing projects that make use of cloud computing require IT expertise. Other articles go further into financial matters and may be found in the e-FISCAL project's state-of-the-art repository [50] [51]. The bulk of these publications concludes that the potential for savings is conditional on the nature of the activities being supported and the types already present.
- Users may access systems through a web browser even if they are in a different location or using a different device. This is possible due to device and location independence. Technology such as a personal computer or a mobile phone. This is possible because the infrastructure is hosted remotely (typically by a third party) and is accessible online.
- Since the data is saved on an external server that is managed by a provider, it is far simpler to keep a cloud environment up and running than it would be to invest in the infrastructure of a data center. Because the cloud service provider's IT department manages and updates the

system, cloud computing is more cost-effective than keeping a data center in-house.

- Resource and expense sharing across a wide user base are made possible by multitenancy, providing :
- inexpensively concentrating infrastructure (such as electricity, real estate, etc.)
- increased potential for handling peak demands (Users do not need to design and pay for resources and equipment to handle the highest possible load levels).
- system upgrades for systems that are normally barely utilized 10% to 20% of the time.
- The IT staff of service providers use web services as an interface to see things and build a cohesive structure and have a loose network of links.
- Instead of waiting for the data to be stored and sent by email, productivity may rise when numerous users may work on the same piece of information concurrently. Time is saved for everyone involved when fields are consistent since duplicate data entry is avoided and application software changes are not required.
- Because the availability of the cloud may be increased by employing many redundant locations, it is a viable option for usage in ensuring business continuity and reacting to calamities.
- Scalability and elasticity through fine-grained, self-service resource dynamic ("on-demand") provisioning in close to real-time (Note that different VM types, locations, operating systems, and cloud providers have different VM startup times), without requiring customers to plan for peak loads. This enables scaling up as usage requirements increase or down when resources are not being used. Because it takes less time to add new resources than it used to, The time-saving benefits of cloud

scaling also mean faster time-to-market, and greater enterprise agility and agility. To propose models of efficient elasticity, machine learning methods have recently been used as a method for regulating elasticity.

- Even if data centralization, more resources being allocated to security, and other factors may contribute to an improvement in security, Loss of control over some sensitive information and key stored vulnerabilities may exist. Most of the time, the security provided by these systems is on par with or even better than that provided by more conventional systems, because service providers can afford to invest resources in resolving security vulnerabilities that many customers either cannot afford to address or for which they lack the technical expertise [68]. However, when data is spread over a large area or across multiple devices, as well as in multi-tenant systems shared by offline users, the complexity of security increases exponentially. There's also a chance that users won't be able to access the security audit logs if they try. The desire of users to prevent the loss of information security and control over the underlying infrastructure has been a driving force in the creation of private clouds.

2.6.1 Types of cloud computing.

There are three methods for creating and deploying cloud computing services [52]:

1 .Public Cloud

In this model, the company providing cloud computing services, which is sometimes referred to as a third party since it provides cloud computing services to other businesses for a fee, owns and controls the cloud computing services. Users of this service use online apps, which are often accessed using a web browser.

2 .Private Cloud

Cloud computing services utilized just by one business or organization are referred to as private clouds. The private cloud resources may be housed within the business that owns the private cloud, or some businesses may use other cloud computing service providers to host their cloud. This model can be seen as a hybrid solution. The data center for cloud computing.

3 .Hybrid Cloud

In this model, the public cloud and private cloud are merged, and contemporary technologies are used to connect the services so that cloud users may use the general services offered, and these services often utilize additional services in the private cloud.

2.6.2 Types of cloud computing services.

The most important types of cloud computing services are software services, platform services, and infrastructure services.

1- IaaS

Companies may employ a service called "Infrastructure as a Service" which provides them with physical resources like servers, networks, and storage spaces and bills them on a pay-as-you-go basis. One of the most important advantages of this service is that it helps companies to avoid the price of owning servers, which saves them time and effort in managing and maintaining them and gives them flexibility in choosing server capacity depending on consumption. Along with these benefits, this service also helps organizations save money by not having to buy servers [53].

2 .Online Platform Service - PaaS

This service, also known as Platform as a Service, consists of the operating systems, databases, and software required to build and execute Internet-based applications. It also includes IaaS infrastructure services.

3 .Software Service - SaaS

The phrase "Software as a Service" refers to a kind of cloud-based computing service comprised of "PaaS" or "platform as a service" electronic platform services and "third-party software" that is operated over the Internet and is generally accessed using a web browser. The fact that the fee for using the service is paid when the user needs the programs is one of the most important benefits for the user of this service. This saves the user a substantial amount of money compared to the cost of purchasing and updating these software, as shown in figure 2.2. For a fee that may be paid either monthly or annually, Office can be accessed via the user's browser.

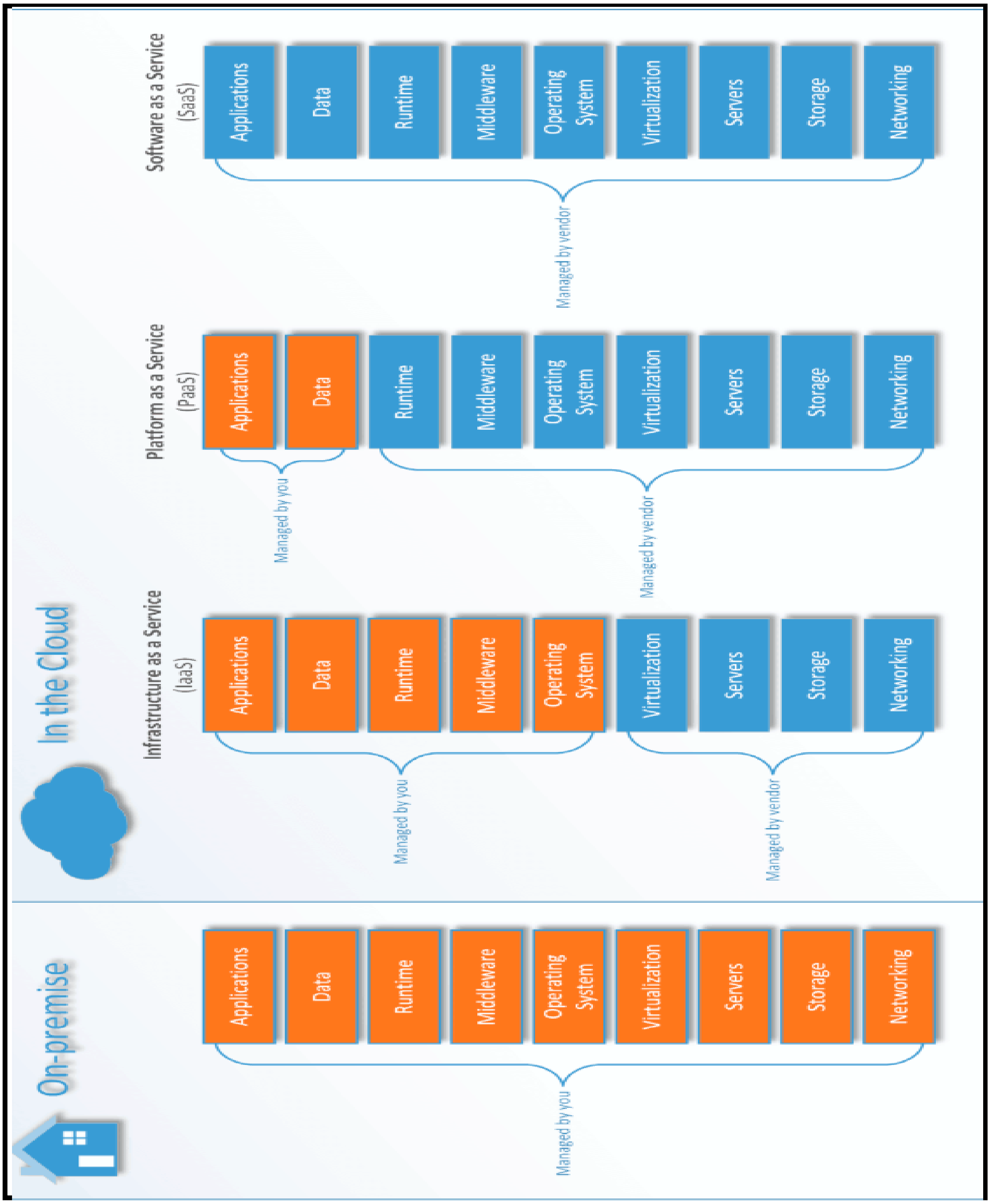


Figure (2.2): Electronic platform services

2.6.3 Cloud computing uses

There are many uses for cloud computing, and even if you are not aware of them, you likely use one of the services it offers. If you're using the internet for anything—from storing data to listening to music to playing games to watching live broadcasts—then you're using cloud computing services. However, there are many other uses for cloud computing as well, and the following are just a few of them [54]:

- **Saving and storing data (backup)**

  Google Drive and Drobox are just two of several similar free services. Large organizations often pay for this service to preserve multiple copies of their databases, as opposed to individuals. By storing data in the cloud, it is accessible from any location and device.

- **Live broadcast of audio and video**

  With the use of this service, you may show audio or video files on platforms provided by cloud computing service providers, whether you're watching a live broadcast or watching previously recorded content.

- **Customized software**

  This capacity makes it simpler for software developers to disseminate their goods broadly, which is a significant benefit of cloud computing. This reduces the program's vulnerability to hacking and ensures that users always have access to the most recent version of any software they use. The most popular services of this kind are Google Docs and Google Sheets.

- **data analysis**

  The ever-increasing volume of data is one of the most crucial challenges facing firms of all types, including public and private organizations today, making the analysis of data on desktop computers inefficient despite their remarkable capabilities. As a result, since the majority of cloud computing service providers provide a variety of platforms for data analytics, many institutions use cloud computing services to analyze their data.

- **Application development and testing**

  While cloud computing service providers offer numerous specialized platforms for developers (programmers) to enable them to develop cutting-edge applications and test them before making them available to users, there are times when a software developer needs to use high-end devices to develop a particular program and other times when the developer cannot obtain a computer. As a result of these capabilities, it turns to cloud computing platforms for this.

- **Hosting websites and applications**

  This service offers freedom in determining the resources required to operate websites, web apps, or application programming interfaces (APIs) while enabling the option of hosting these types of applications.

2.7 Data Security in Cloud Computing using RSA

The ability of cloud computing to reduce computing costs has made it the most widely studied emergent paradigm. Internet-based technology that provides on-demand services to customers is the most fascinating and alluring innovation of our day. For obvious reasons, security is a major issue that prevents the widespread use of cloud computing. Since cloud computing is still a new concept, this is to be expected. Various security issues have been raised concerning cloud computing since the user does not have direct physical access to the data. It's clear that cloud computing has huge potential and is also quite efficient. It suggested a technique using the RSA algorithm to assure the security of the data [55].

2.8 Data Security Issues in the Cloud

1. **Privacy and Confidentiality**: There should be some assurance that access to the client's hosted data in the cloud will only be permitted by those with the proper authorization. Another issue that might potentially endanger cloud data is cloud staff having improper access to sensitive client information. Cloud users should be provided guarantees regarding the security of their data, and suitable procedures, privacy policies, and practices should be in place [56].
2. **Data integrity**: The capacity to determine precisely what happened to a given dataset and when it happened is just as important as protecting the security of the data stored in the cloud. The client must be made aware of the type of data being kept in the cloud, its origin, and any integrity protections that have been put in place by the cloud service provider. Cloud service providers need to have procedures in place to protect the integrity of the data and to know what occurred to a dataset and when it happened. This is in addition to ensuring data security. The cloud service provider must inform the customer of the type of data being stored in the cloud, its source, and any integrity safeguards that have been implemented.
3. **Data placement and relocating**: Cloud computing provides a high level of data mobility. ConsUsers typically do not understand where their data is stored. The location of the device used to store confidential information in the cloud may be of interest to organizations. It is also suggested that they choose a location that has some personal significance (e.g., data to be kept in India). It is thus necessary for the Cloud provider and the customer to enter into a written contract specifying the location or known server where the data will remain. Also, the security of systems, particularly the security of data, should be ensured by cloud providers, who should also offer strong authentication to protect client data. The transfer of data between locations is another

problem. Data is first kept at a location determined by the cloud service provider as being suitable. However, it frequently relocates from one location to another. Cloud service providers have agreements with one another and share resources.

4. **Data Availability**: Customer data is typically saved in chunks on several servers, generally located in various regions or Clouds. In this case, As the availability of seamless and uninterruptible supply becomes more and more challenging, data availability emerges as a serious genuine concern [57].

2.9 The hardware component of the Sensing Area

2.9.1 Arduino (Node MCU)

An open-source and affordable Internet of Things platform is NodMcu. A hardware platform based on the ESP-12 module and a firmware platform based on the ESP8266 Wi-Fi SoC made up the first components. Support for the 32-bit ESP32 MCU was later added [58].

You may get prototype board designs for use with the free, open-source NodeMCU firmware. Node and MCU are abbreviations for the microcontroller (micro-controller unit). In a strictly techical sense, "NodeMCU" refers exclusively to the firmware and not to the associated development kits.

Lua is a scripting language used by the firmware. The firmware is based on the eLua project and was developed using the Espressif Non-OS SDK for ESP8266. It makes use of a lot of free source programs, including SPIFFS and lua-cjson. Users must choose the proper hardware for their project and develop firmware that is optimal for their requirements due to limitations on the resources that are available. The 32-bit microcontroller ESP32 has also been supported. Circuit boards with a Dual In-Line package (DIP) are often utilized as prototype hardware. This board has a USB controller as well as a second, smaller board with a surface-mounted microprocessor and antenna. It is simple to prototype on breadboards thanks to the DIP format selection. The ESP-12 module of the ESP8266, which is a Wi-Fi SoC combined with a Tensilica Xtensa LX106 core and is extensively utilized in IoT applications, served as the design's basic foundation [58].

It can list the uses of the nodemcu as follow:

- Internet Smoked Alarm.
- VR Tracker.
- Octopod.
- Serial Port Monitor.
- ESP Lamp.
- Incubator Controller.
- IoT home automation.
- Security Alarms.

The advantage of the nodmcu is listed below :

- Open-source
- Arduino-like hardware
- Status LED
- MicroUSB port
- Reset/Flash buttons
- Interactive and Programmable
- Low cost
- ESP8266 with inbuilt wifi
- USB to UART converter
- GPIO pins

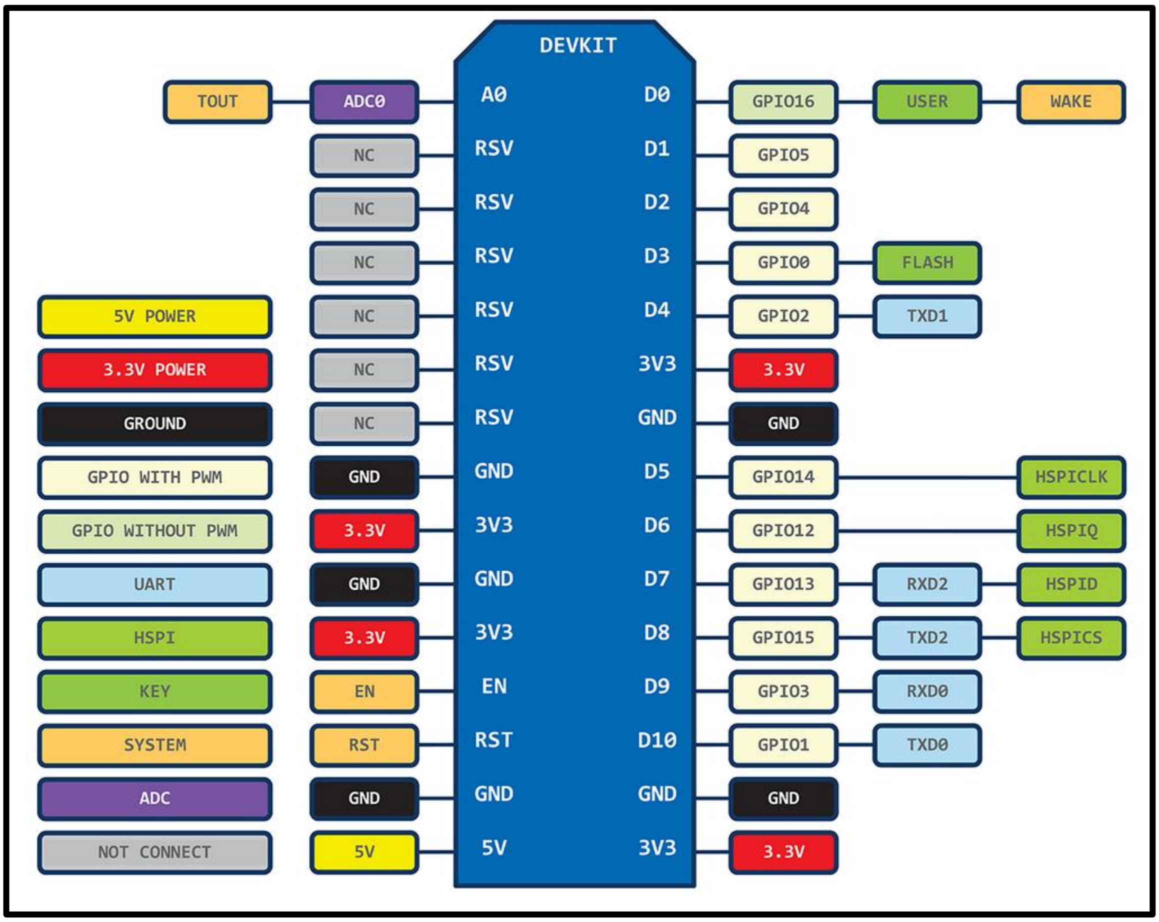


Fig. (2.3): output Pins of the Node MCU

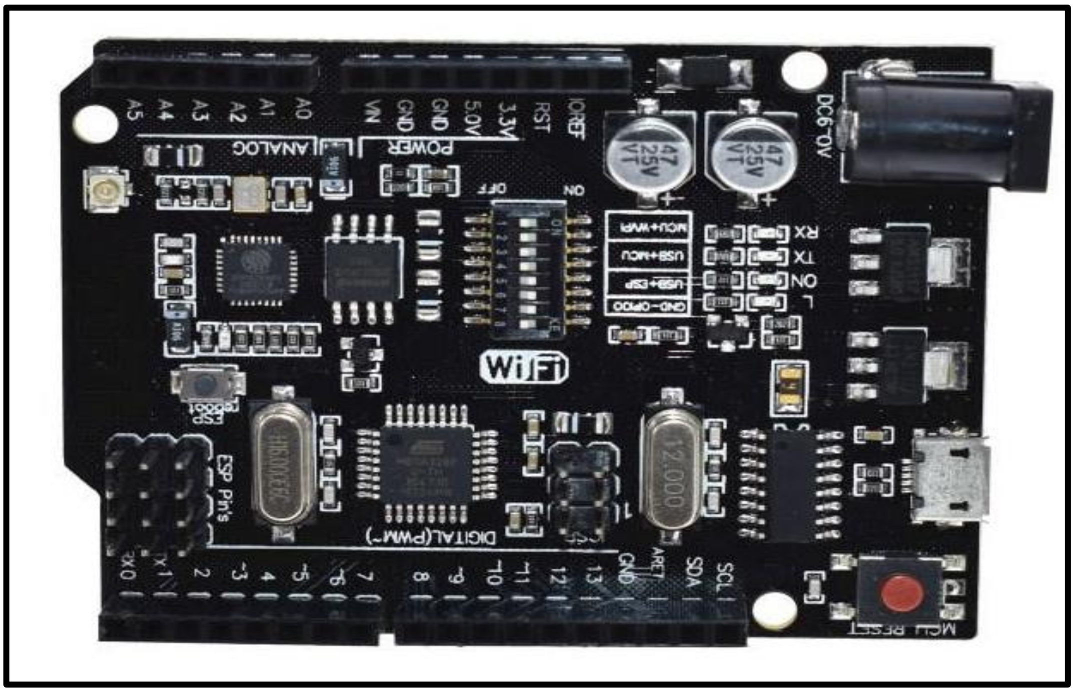


Fig. (2.4): Node MCU hardware model ESP8266

2.9.2 Heart rate sensor

A portable monitoring device called a heart rate monitor (HRM) allows for both real-time heart rate measurement and display as well as heart rate recording for future studies. The user's heart rate may be recorded while they are engaging in physical activity, which is one of its main applications. There is information regarding monitoring one's heart rate [59].

Electrical and optical heat rate sensors are the two types available. Each electrical monitor consists of a transmitter and a receiver that is worn to the chest. A radio signal is sent when a heartbeat is detected, and the receiver utilizes this signal to show or calculate the current heart rate. The chest strap itself may be the source of this signal, or it may be an unexplained radio pulse (such as Bluetooth, ANT, or other low-power radio links). Both eavesdropping and using a user's receiver to pick up signals from other nearby transmitters are now impossible thanks to recent improvements in technology. Eavesdropping can no longer be done (a phenomenon known as cross-talk interference). It's vital to keep in mind that older radio transmission technology called Polar 5.1 kHz could potentially be used below the waves. 2.4 GHz is the frequency that Bluetooth and Ant+ both utilize since higher-frequency signals cannot pass through water.

Modern devices use the optical method, which includes shining light through the skin from an LED and detecting how the light is scattered by blood vessels to get a heart rate. Some of these technological instruments can monitor blood oxygen saturation in addition to heart rate (SpO2). As previously indicated, certain modern optical sensors can also send data.

Modern gadgets may be used to show and/or gather data, such as watches and cell phones. Some gadgets can track many metrics at once, including heart rate and oxygen saturation. These might have sensors that measure distance, speed, and position, such as accelerometers, gyroscopes, and GPS. In recent years, Heart rate monitors are already a commonplace inclusion in smartwatches, greatly enhancing their appeal. PPG sensors are often used in some smart watches, smart bands, and mobile devices. The shape of the sensor used for heart rate is shown in figure (2.5).

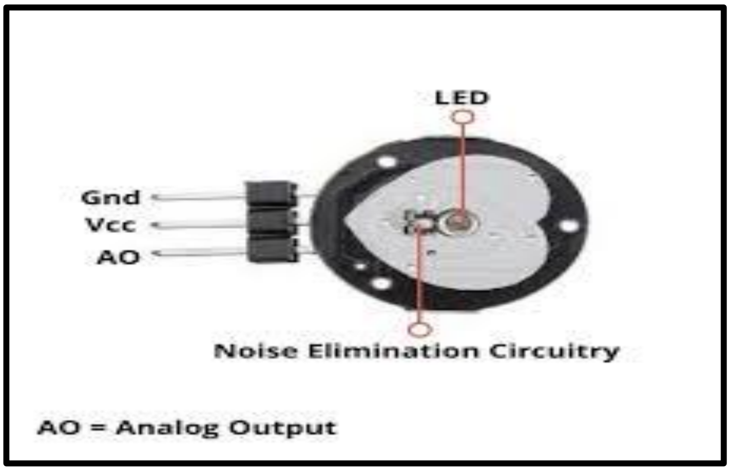


Fig. (2.5): Heart rate sensor

2.9.3 Temperature sensor

It's challenging to define the idea of temperature. Temperature is typically used as a qualitative criterion to categorize whether a substance seems to be hot or cold. More specifically, every molecular component of matter that moves has a unique kinetic energy and motion. Temperature is inversely related to the average kinetic energy of molecules, even though it is not an independent measure of energy. Temperature is a property of physics that describes the average amount of molecule kinetic energy. This implies that when the temperature rises, the molecules move more quickly the hotter it is. At absolute zero, the temperature is 0 kelvin (or -273.15 degrees Celsius) since the molecules are not vibrating at all. As shown in figure (2.6) [60].

Any instrument used to measure temperature is referred to as a "thermometer." The molecular kinetic state cannot be directly detected by thermometers; instead, they monitor thermometric variables, which are qualities that vary under the molecular kinetic state. There are several ways to measure temperature, depending on the thermometric variable. Thermistors and

Resistance Temperature Detectors are types of constant temperature sensors used in oceanography (RTDs).

Figure (2.6): Sensor for digital temperature

2.9.4 Sound Sensor

A sound sensor records the acoustic waves and displays a vibrational representation of the sound. It has a sensitive capacitively electret microphone built right into it. The electret fil min microphone vibrates in response to the acoustic pulse, which shifts capacitance and results in a micro voltage change. Following that, the blue potentiometer-controlled threshold is checked by the LM393 comparator in the module after the micro voltage has been transmitted there. The sound sensor illustrated in figure (2.7) generates low-level signals if the ambient sound intensity is below the threshold; high-level signals when the threshold is not reached [61].

Main Features

measuring the sound's strength (note: the vibrational principle can only be used to detect the presence of sound); Adjustable sensitivity (you can use the blue potentiometer shown in the picture); Working Voltage: 3.3V~5V; Output

Mode: Digital Switch Output (low level under working mode); Mounting Hole; Size of PCB: 3.2cm x 1.7cm

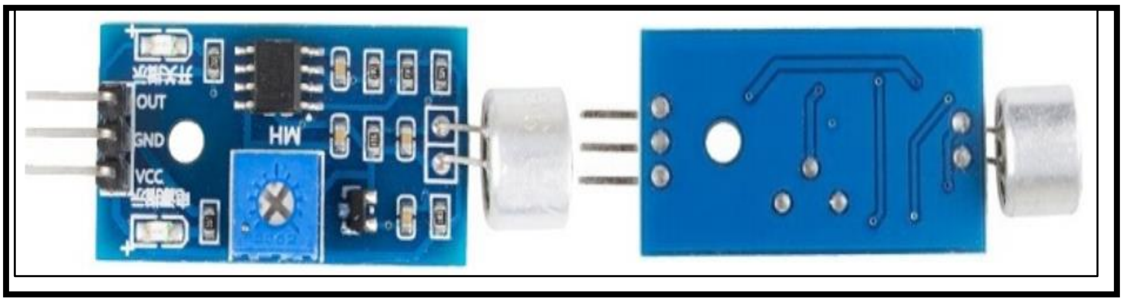


Figure (2.7): Sound Sensor Module

Chapter Three

Proposed Framework

CHAPTER THREE

Proposed Framework

3.1 Introduction

Hospital operations have been enhanced thanks to the "Internet of Things", particularly in terms of patient care. In this regard, the international research firm "Gartner" forecasts that by 2020, there will be more than 20 billion connections and 646 million medical devices with the Internet of Things capabilities. This indicates that the IoT market share (25%) is expected to come from the healthcare sector. Any gadget may be connected to another device through the Internet to establish the "Internet of Things," which is a large network of interconnected "things," including interlinked interactions between things and people as well as between things and other things. By enabling patients to spend more time conversing with their doctors, the integration of medical devices and the availability of data, exchange capabilities have improved how doctors treat patients, protected their safety and health, and encouraged patient participation.

3.2 Proposal Health Care Monitoring System design

In this section, the specifics of the system's operation as described here and as seen in figure (3.1). Where the movement of data from the patient to the doctor's device has been mapped in detail.

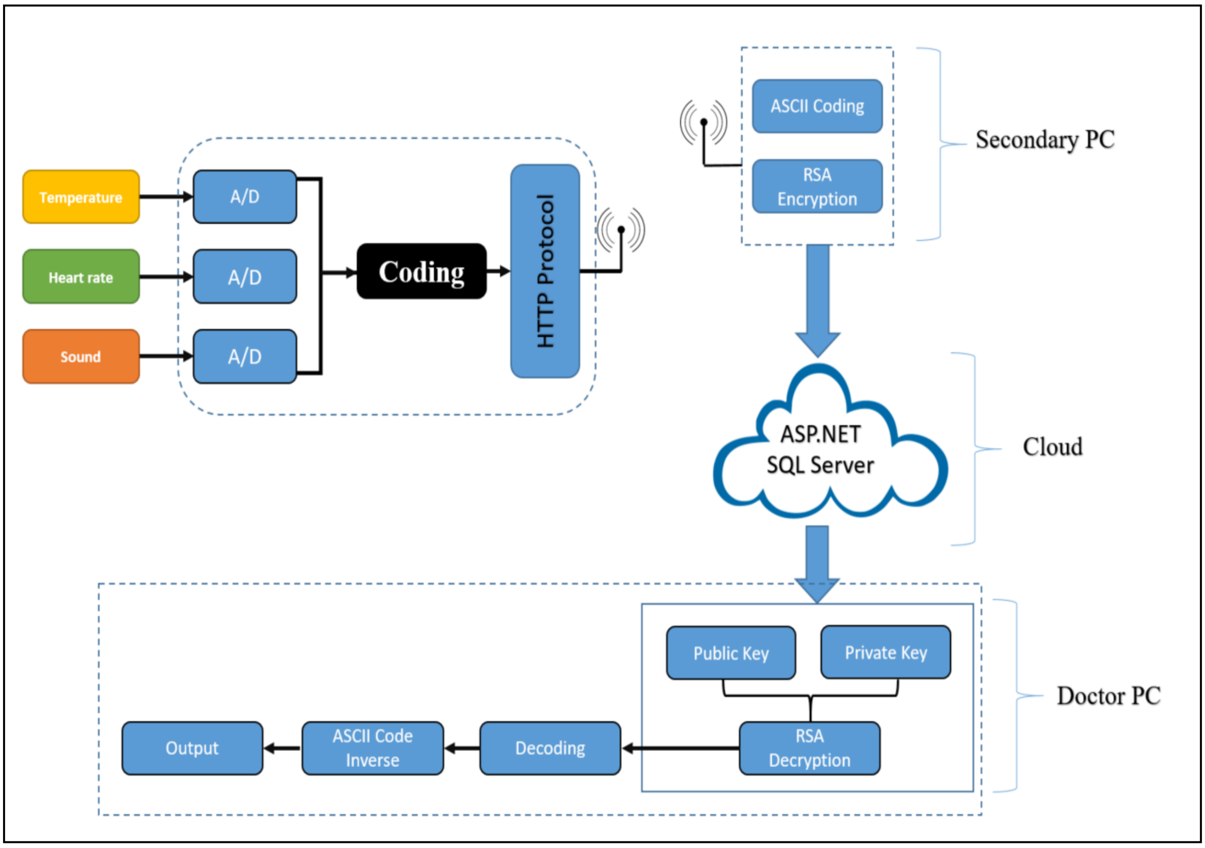


Fig.(3.1): An e-healthcare monitoring system's framework

IoTs are now one of the most potent communication protocols of the twenty-first century. Because of their connection and processing capability, all of the everyday items we use become a part of the internet in the IoT ecosystem. IoT diffuses the Internet's concept and makes it more general. IoT enables unified communications between many types of electronic devices. In other domains, such as healthcare technology, the IoT has therefore gotten more inventive.

In healthcare technology, the Internet of Things included several varieties of low-cost sensors, both implantable and wearable, that allow seniors to access current medical healthcare services anywhere and at any time, so improving their quality of life. This article proposes designs based on the validity of the Internet of Things, which are divided into four steps and shown in Figure (3.2).

The next section provides a more comprehensive explanation of each level of this architecture.

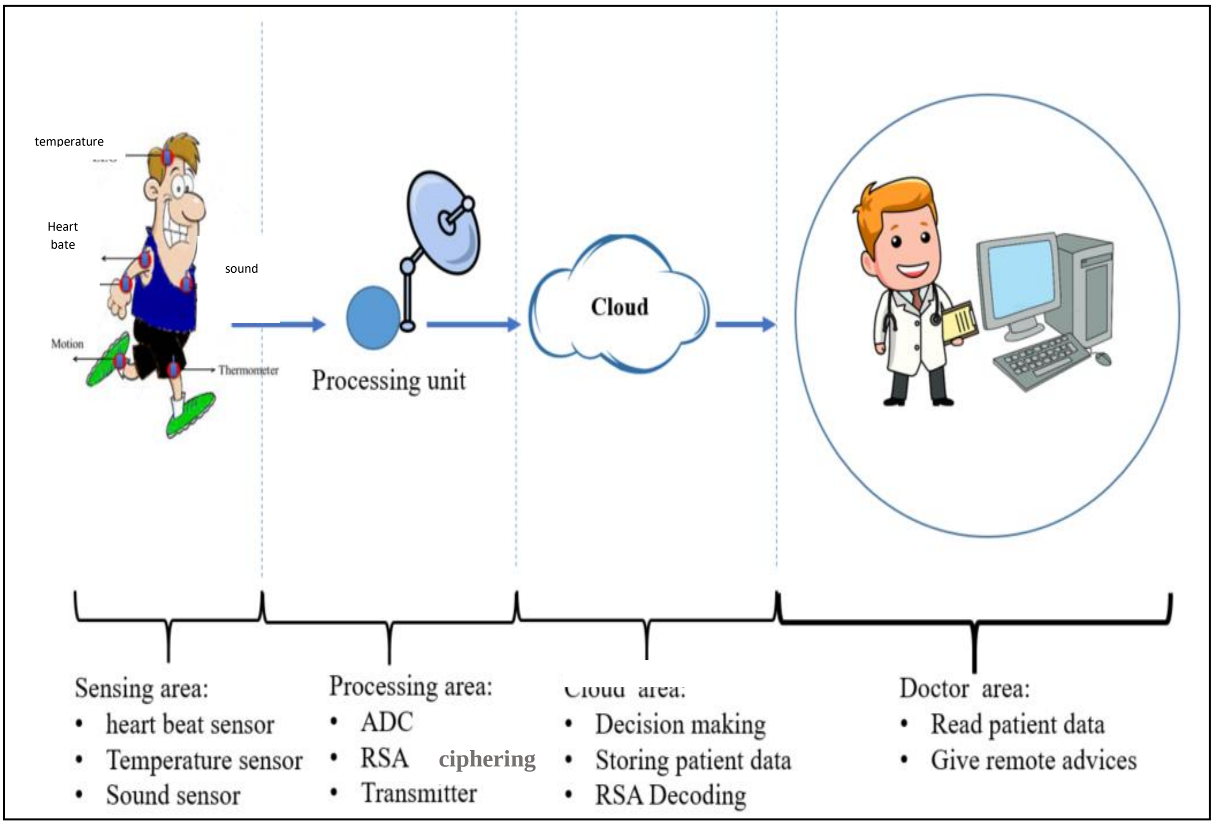


Fig. (3.2): IoT scenario presented for body care system.

1. **The WBSN stage (area -1-),** Currently, some sensors are implanted beneath the skin or worn on the body (intra-body sensors). These sensors might be ones that measured body temperature, heart rate, cough sound, or any number of other parameters. The master node (MN) receives the data from the sensors and transmits it by the 802.15.6 wireless standard. transmits information to the local processing unit (LPU), which might be a computer, a tablet, or a smartphone**.**
2. **The internet stage. (stage -2-) ,** To link levels 2 and 3, this level makes use of directed media like fiber optics or wireless technologies that are already available**.**
3. **Data storage and analyzing stage (stage -3-),** Information is retained

4. **Health-care-service stage (stage -4-),** During this time, patients receive medical care. The information may be given to medical professionals, hospitals, or middle-class families.

3.3 The proposed method

In the form of the proposed system, it will explain each part and how to apply it as follows

3.3.1. Sensors (I/P)

In this part, the sensors (temperature, heart rate, sound) pick up vital signals from the human body, and these signals are in the form of electrical signals and collected via the Arduino.

3.3.2 ADC

The Arduino gathers the analog electrical impulses from the sensors and transforms them into digital output using the Arduino program which is based on C language. This digital output is a high and low value represented by 1,0 respect. These digital outputs are subsequently sent to the Arduino's Wi-Fi.

3.3.3 Data coding

A rule for transforming information (for example, a letter, word, phrase, or sign) into another form or representation - usually abbreviated or secret - (one sign against another), not necessarily of the same type or length. In communication Communication and information processing Data processing, encoding Encoding is the process by which information is converted from a source code into symbols to be communicated to a target. Decoding is the reverse process, which is the conversion of these codes back into information understood by the receiver. One of the reasons for resorting to coding is to enable communication in cases where it is impossible, or difficult, to use plain language, whether spoken or written.

3.3.4 HTTP protocol

Web Protocol for Hypertext It serves as the primary and most popular means of transmitting data on the World Wide Web. It is a stateless protocol for resource transfers across the Internet. The main goal in creating it was to figure out how to transmit and receive pages.

Web browsers employ the user agent, which is port 80 on the server and is part of the seventh layer of the Internet Protocol packet system. To collect the required pages, it typically cooperates with the fourth layer, more especially with the Transport Control Protocol, before the TCP protocol's role begins to take over

3.3.5 Connected sensors;

The temperature, heart rate sensor, and sound sensor have been linked with the microprocessor ESP32 to read the temperature, heart rate, and sound level for the human body. For synchronization, each sensor needed a 2-wire connection, while the other line was used to relay data from the master to the slave. To establish the connection, the master always sends a message to the slave, to which the slave responds. Without a request from the master, the slave is unable to transmit a message. In this context, the master also creates the clock.

There is no need for an extra line of specification since each slave has a distinct address. The unique address of the slave is used to determine how the master and slave communicate. Only the slave's address should be included in the message if the master wishes communication with the slave. The master microcontroller (ESP32) initially provides a 7-bit address followed by a 1-bit read and writes after giving the start signal.

The mechanics of connecting sensors to the Arduino will be explained as follows

1- Temperature sensor;

In this part, the temperature sensor was linked, which has three terminals: one for supplying voltage to the sensor, one for ground, and one for data transfer. As shown in Fig.(3.3), the temperature sensor is linked to the CPU by connecting the voltage terminal to pin 5v, the ground terminal to the ground pin, and the data transfer terminal to pin (13).

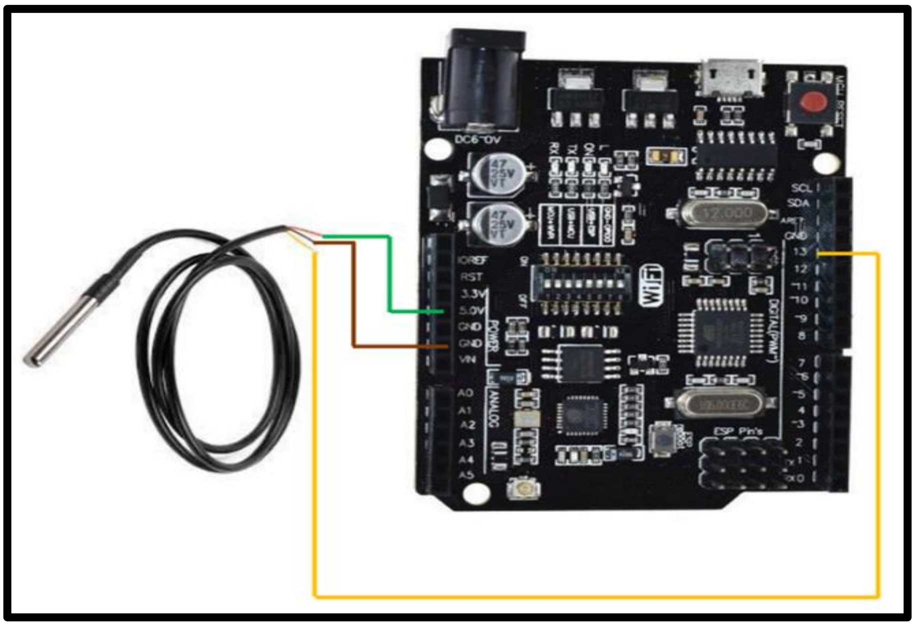


Fig. (3.3): Heat sensor connection

2- Heart rate sensor

The heart rate sensor is linked in this section, which has three terminals: one for giving power to the sensor, one for grounding, and one for transferring data. When linked to the processing unit, the voltage end is attached to the voltage pin 5v, the ground end is connected to the ground pin, and the data transfer end is connected to the data transfer pin A0, as indicated in figure (3.4).

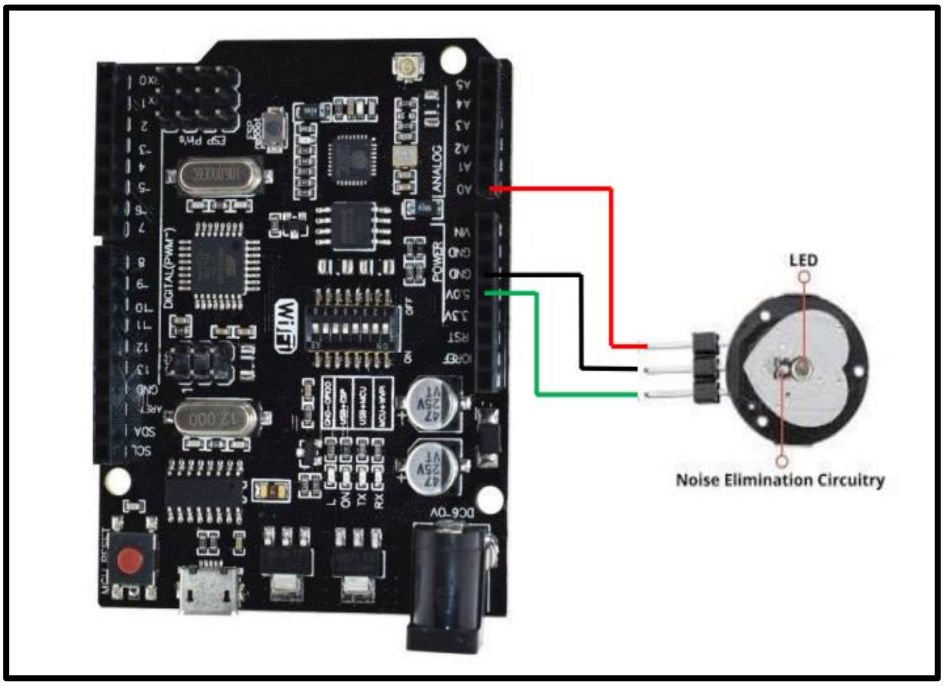


Fig. (3.4): Heart rate sensor connection

3- Sound sensor;

The sound sensor is linked in this section, which has three terminals: one for giving voltage to the sensor, another for grounding, and another for transferring data. It is linked to the processing unit as shown in the picture by connecting the voltage end to voltage pin 5v, the ground end to the ground pin, and the data transfer end to data transfer pin A1 on the processing unit (3.5).

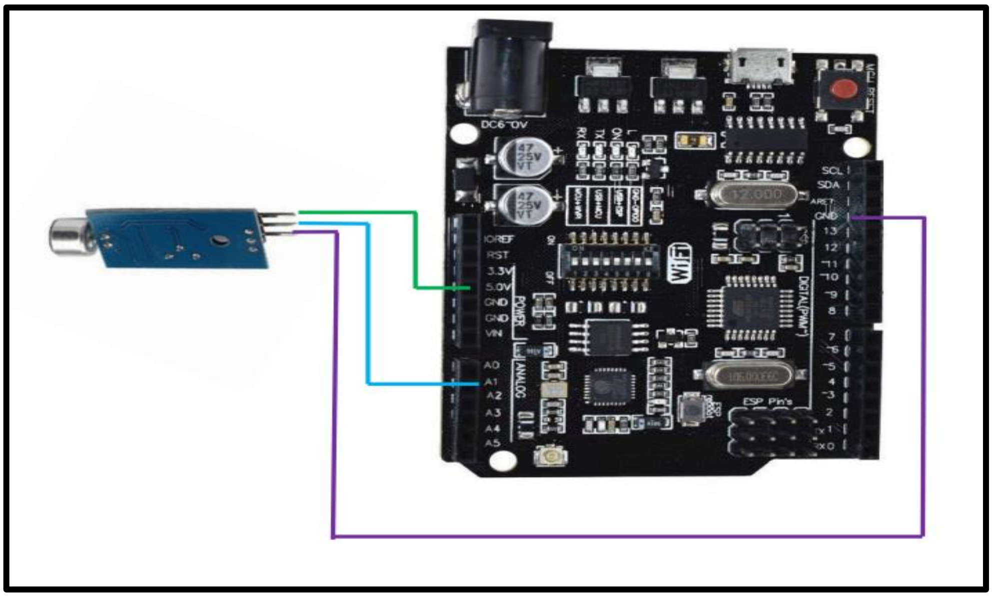


Fig. (3.5): sound sensor connection

4- Overall map of the practical part

The whole system among three sensors and the processing unit is depicted in this figure (3.6).

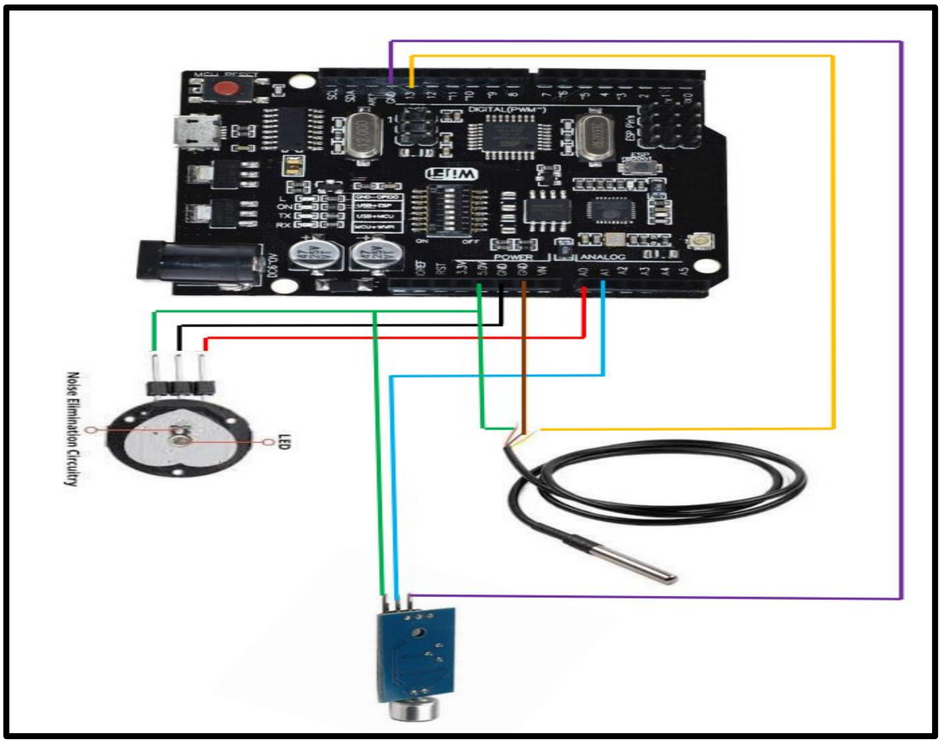


Fig. (3.6): whole system component connection

3.3.6 Wifi Adapter

Utilizing the Wi-Fi protocol, the data acquired from the three sensors (which were Digitized and encoded electrical impulses) will be transmitted to the secondary computer, which may carefully monitor the patient.

3.3.7 Secondary PC

It is permissible for the secondary computer to talk about mapping, as well as talk about the encryption algorithm and its mechanism of work as shown in the flow chart drawn in figure (3.7).

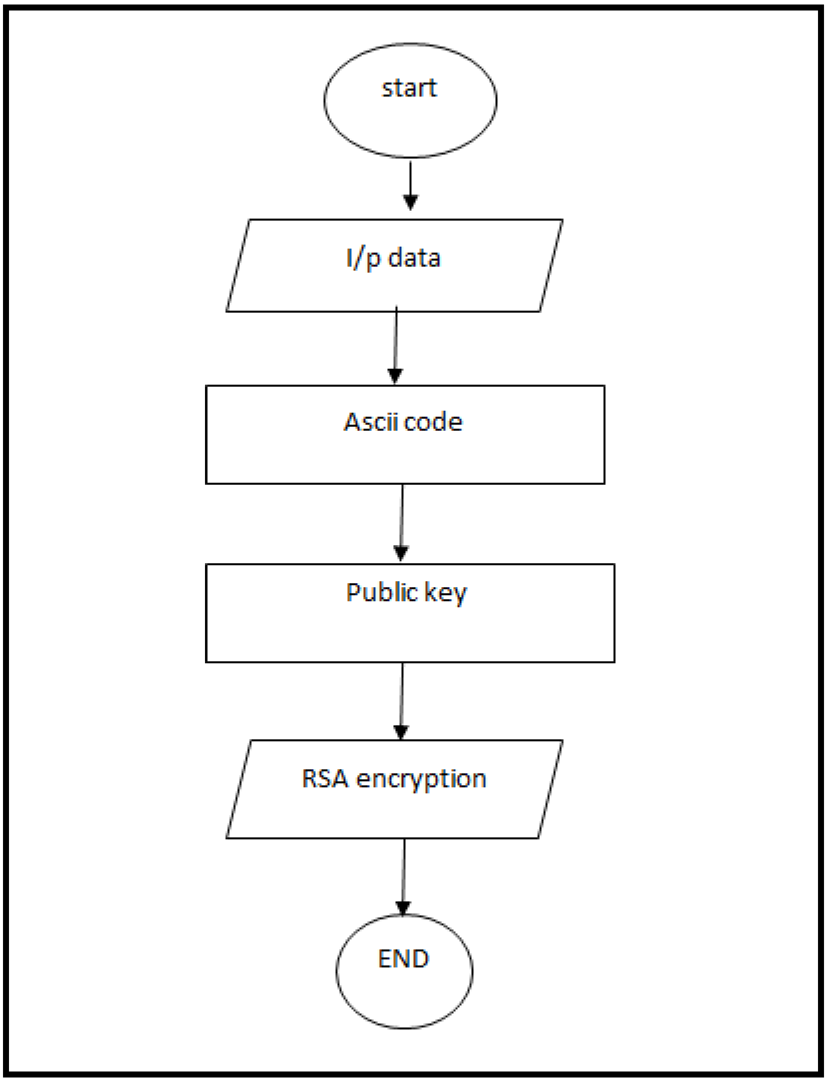


Figure (3.7): mechanism of Secondary PC of the encryption

3.3.7.1 ASCII code

The ASCII standard is a computer symbol representation system, that defines a correspondence relationship between a numeric value of a bit sequence and a symbol or graphic used in a written language. Since computers can only process electrical impulses that are either zero or one or the bit in a programming language,

3.3.7.2 RSA algorithm Encryption

Using the initial value, the public key was generated and thus the data was encrypted using the RSA algorithm, as shown in figure (3.8), which shows us the flow chart of the system used for the RSA encryption.

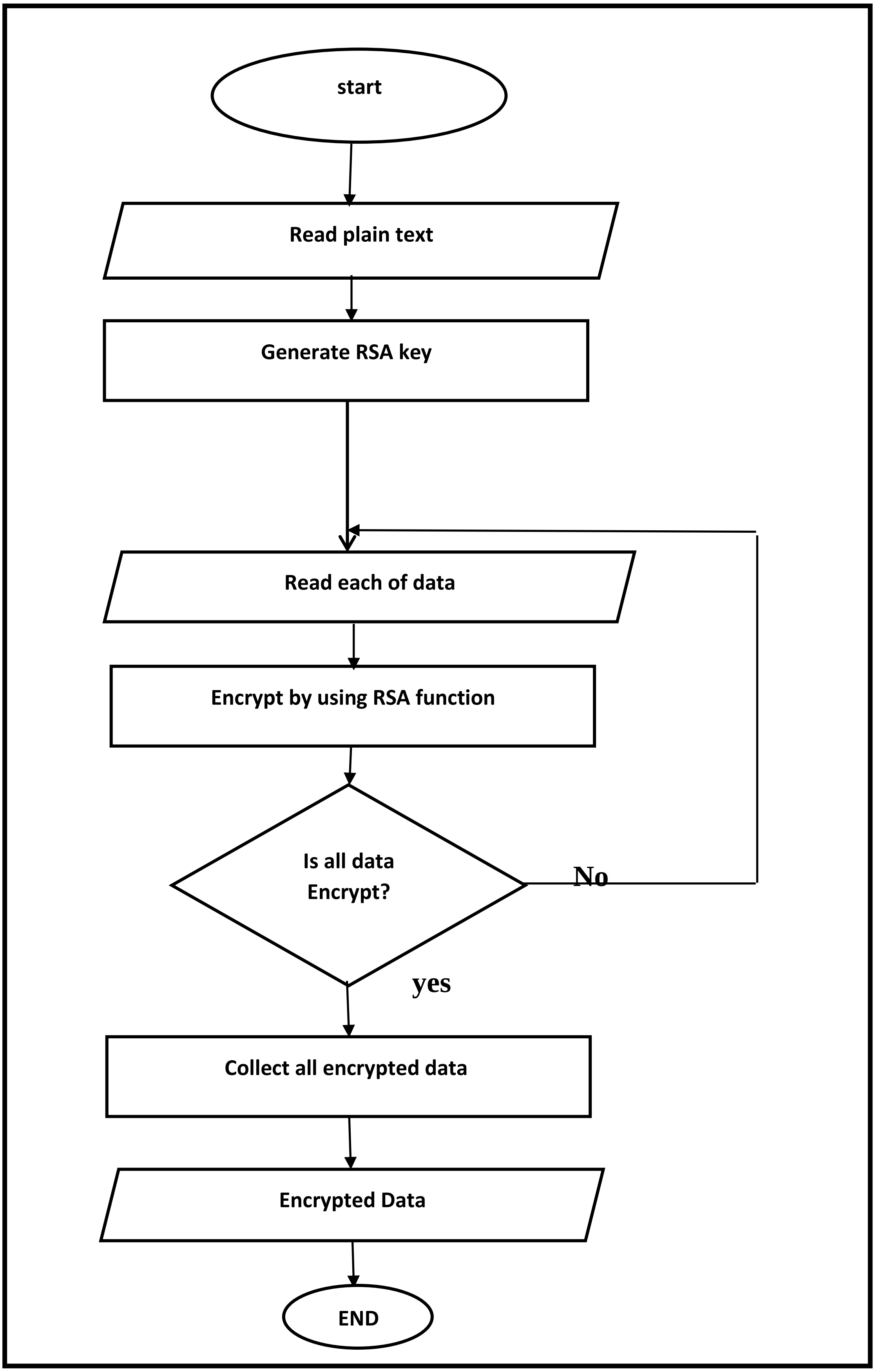


Figure (3.8): Flow chart for RSA encryption

3.3.8 The Doctor PC

It is acceptable for the doctor's computer to discuss remapping as well as the decryption method and how it works, as indicated in the flowchart in figure (3. 9).

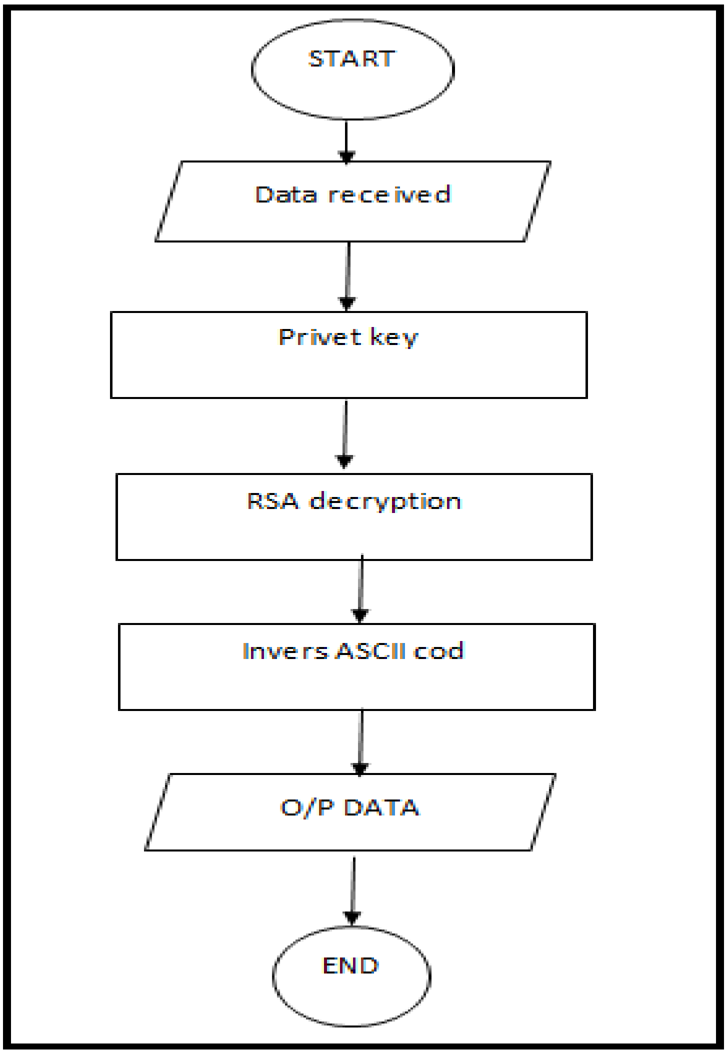


Figure (3.9): procedure and machinist at doctor's computer.

3.3.8.1 Initial value

Any two distinct large random prime numbers are used here to compute the private key and the public key of the encryption method utilizing the algorithm functions and equations described in chapter two.

3.3.8.2 Public key Gen.

The RSA algorithm uses a public and private key. Anyone attempting to get in touch with the key owner must be aware of the public key, which is merely the encryption key. As its name indicates, it is a public key. It's okay for everyone to know him. Which is generated in the doctor's computer and sent to the secondary computer, through which the encryption algorithm is run and the results are displayed in the secondary computer.

3.3.8.3 Privet key

Only the public key can be used to encrypt the information data, and the private key is required to decrypt this data. As its name indicates, it is a private key. Nobody should know that. RSA database keys are generated in the manner previously described in Chapter 2 in detail and here only a doctor can follow up on patients

3.3.8.4 RSA algorithm decryption

As illustrated in figure (3.10), which displays the flow chart of the system used for the RSA decryption, the Privet key was produced using the initial value, and as a result, the data was decrypted using the RSA technique.

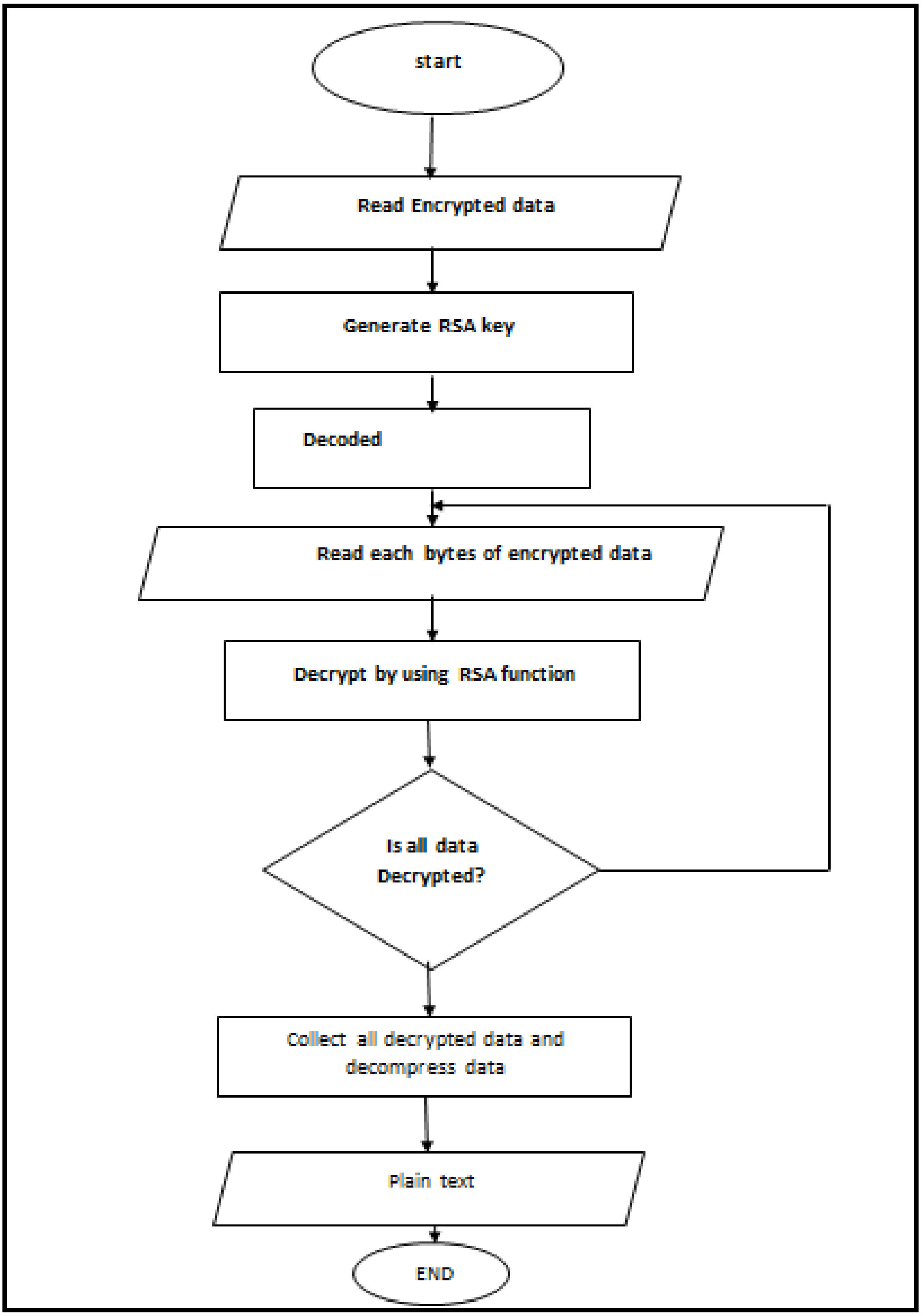

start
Read Encrypted data
Generate RSA key
Decoded
Read each bytes of encrypted data
Decrypt by using RSA function
Is all data Decrypted?
Collect all decrypted data and decompress data
Plain text
END

Figure (3.10): Flow chart for RSA decryption

3.3.8.5 Decoding

Coding involves reinterpreting the encoded data into a form similar to the original form of the data that can be displayed

3.3.8.6 DE mapping

In this part, The ASCII code process will be reversed and the data returned to its original form.

3.3.8.7 Cloud type (Hybrid cloud);

In the previous chapter, he discussed the cloud and its types in general, and in this section, the hybrid cloud type employed in the practical portion of the proposed system will be described. Since it integrates both public and private clouds, it is considered cloud computing. As opposed to this, a hybrid cloud integrates and organizes the benefits and services offered by both public and private clouds.

The hybrid cloud was chosen from among the types of clouds because it represents an excellent choice due to its main advantages, including:

- Scalability.
- Quick response.
- Reliability.
- The administration.
- Security.
- Low Price.

3.3.8.8 Cloud service (IaaS):

IaaS is a type of cloud computing service that lets you process, store, and connect on-demand and pay-per-use. (SaaS), (PaaS), and (IaaS) are three different types of cloud services. Reduce local data center maintenance, save on hardware costs, and get real-time insights into your business by moving your enterprise infrastructure to IaaS services. With the flexibility to change your IT resource allocation in response to demand, IaaS solutions are available. In addition, they improve the reliability of your core infrastructure and enable the rapid deployment of additional applications.

Reasons to use IaaS

- costs are optimized while capital expenditures are decreased.
- The scale and performance of IT workloads are increased.
- Improves supportability, stability, and dependability.
- Enhances disaster recovery and business continuity.
- Security is increased.
- Helps you develop and more rapidly release new applications to consumers.

3.3.8.9 ASP.Net core

Technology helps to build high-performance websites and helps to make Web API Server, which is a server without interfaces and which will be the source of data for many parties, including mobile applications that need to store their data on the Internet. The primary Asp.net is the update, updated and free version of the old technology called Asp.net. The programming language used in this technology is C#, which is rich in the definition.

Chapter Four

Result and Discussion

CHAPTER FOUR
RESULT AND DISCUSSION

4.1 Performance Evaluation

` The scheme in Figure (3.2) was implemented using the software. Whereas MATLAB simulation language was used and the results were as shown in the following curves. Where an important metric is the bit error rate (BER) along with the RSA algorithm and without RSA on two types of channels, flat fading and AWGN

4.2 The AWGN channel with RSA

In this part the performance of the system is discussed using AWGN channels in the case of ciphring represented by the red curve, and in the absence of ciphering represented by the blue curve. as in Figure(4.1);

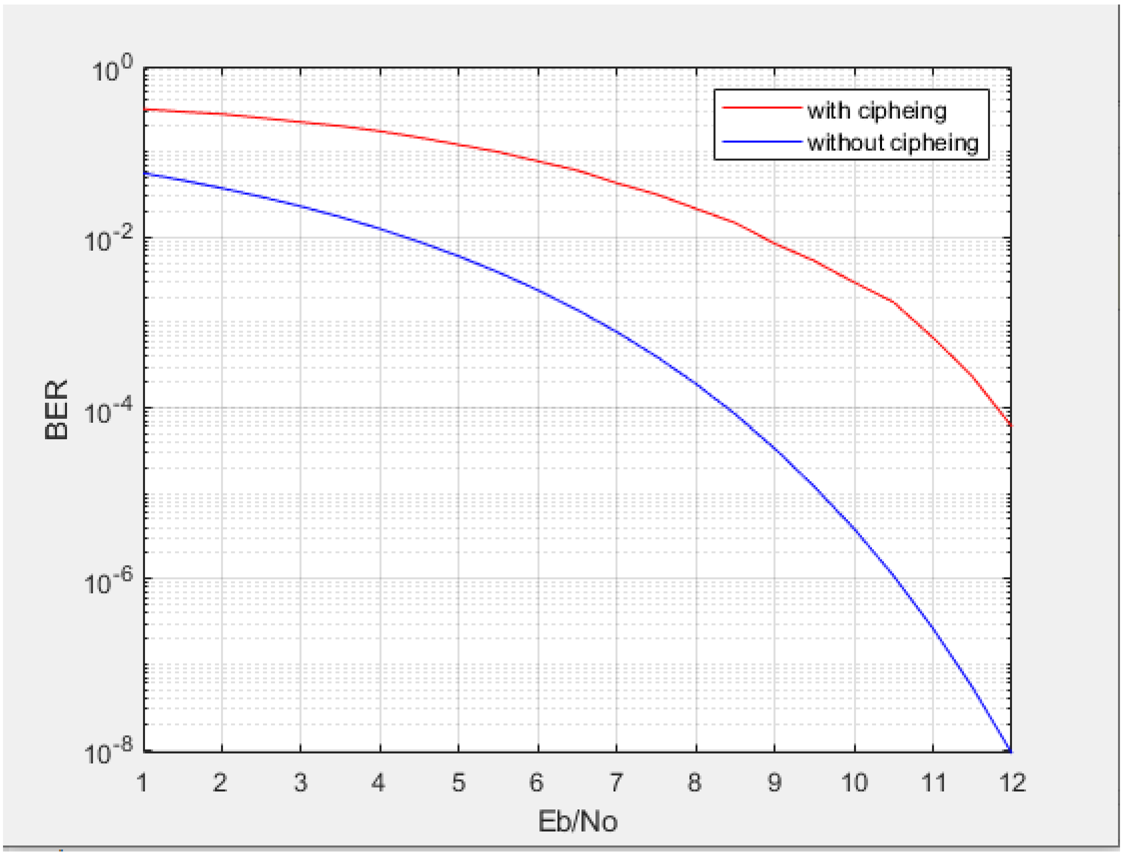


Figure (4.1): ciphering and without ciphering curve in AWGN channel

We find that the relationship between Eb/No and BER is an inverse relationship for the coding curves and without the coding curves because the higher the (Eb/No) the less the effect of noise on the signal due to the energy difference between them. We note that ber for encryption is slightly higher than without encryption because the encryption process increased the number of bits sent and thus led to an increase in the bits in which an error occurred and this leads to increased security of the transmitted data

4.3 Flat fading channel with RSA:

In this part the performance of the system is discussed using flat fading channels in the case of ciphring represented by the red curve, and in the absence of ciphering represented by the blue curve. as in Figure (4.2)

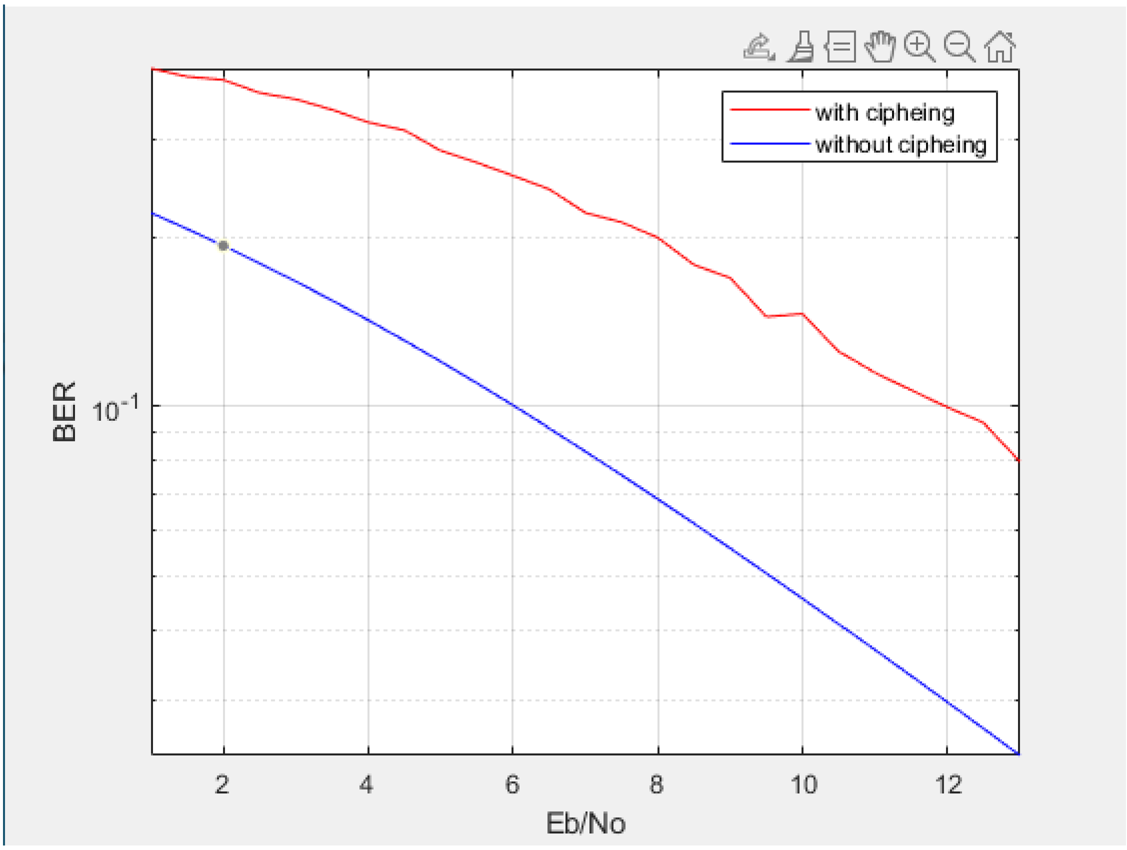


Figure (4.2):ciphering and without ciphering curve in flat fading channel

We find that the relationship between Eb/No and BER is an inverse relationship for the ciphering curves and without the ciphering curves because the higher the (Eb/No) the less the effect of noise on the signal due to the energy difference between them. We note that ber for encryption is slightly higher than without encryption because the encryption process increased the number of bits sent and thus led to an increase in the bits in which an error occurred and this leads to increased security of the transmitted data.

We also note that in each run we find the noise random and therefore its effect on the data is random so we will notice slight differences between the curves in each run but the values and limits are almost equal and the system performance is stable

4.4 Decryption failure (DF);

It is the condition that occurs if the decryption bits get an error due to the strength of the encryption and the system is unable to extract the sent message.

There is a relationship between the decoding failure that increases with increasing (p, q) values which are represented by figure (4.3);

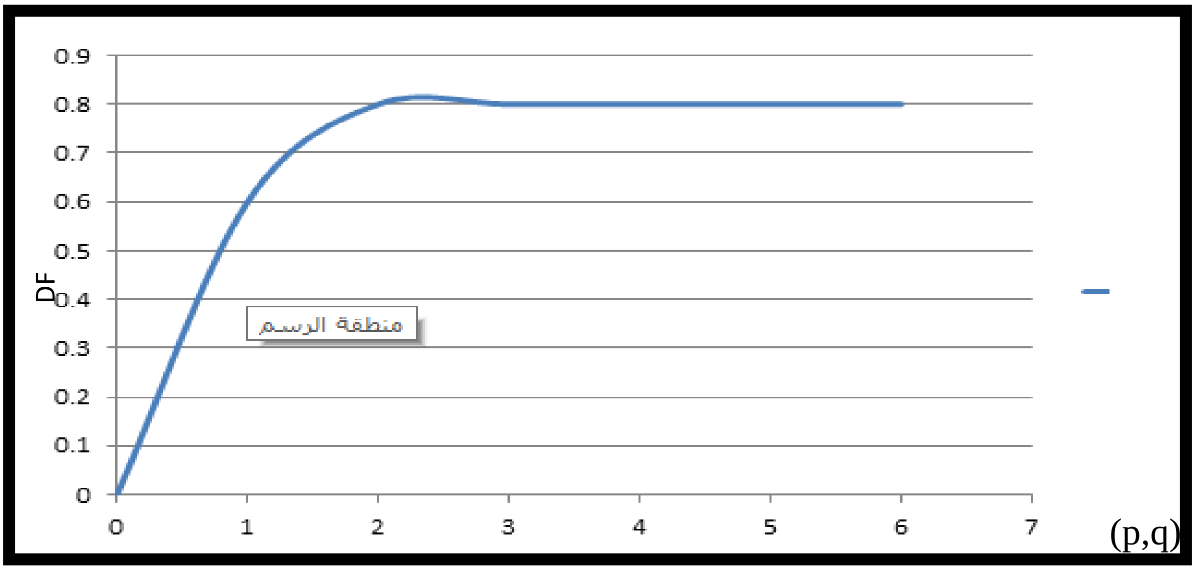


Fig (4.3); decryption failure(DF)

From Figure (4,9), it has the advantage of allowing you to regulate the cipher's strength. For example, if we use a communication system with a high BER, we recommend using low P and q values to keep the DF low, and if the system has a low BER, we recommend using high P and q values to keep the DF high, but this value is considered too low for a robust system because its bit-error rate is low.

As a result, the suggested system may adapt to this system and raise or reduce the encryption strength as desired by the user.

On the other hand, some systems, such as those that utilize the TCP / IP protocol, may fix a very big error or retransmit it again, where the error rate is zero, allowing the suggested encryption to be used to its maximum efficiency. Maximum security and extremely high transaction values.

The data was transported across the cloud using the TCP / IP protocol when the system was developed and realistically implemented. This protocol does not tolerate and correct faults. Therefore, in all tested circumstances, there was no difficulty in delivering data from the patient to the doctor entirely and without mistakes. As a result, the suggested system is very efficient in data transfer and encryption.

4.5 Examples of encryption and decryption of messages

Examples of implementing the mechanism of sending a message, encrypting and decrypting it using the Matlab program**;**

Table (4.1): Implementation of RSA encryption and decryption for P=13 and q=23

Parameters	P=13	q=23	N=299
Public key	5		
Privet key	53		
Message	12345		
ASCII code of inter message in hexadecimal	49 50 51 52 53		
Cipher text of the entered message	82 150 181 117 40		
Decryption ASCII code of the message	49 50 51 52 53		
Decryption of message	12345		

Table (4.2): Implementation of RSA encryption and decryption for P=23 and Q=61

Parameters	P=23	Q=61	N=299
Public key	7		
Privet key	943		
Message	12345		
ASCII code of inter message in hexadecimal	49 50 51 52 53		
Cipher text of the entered message	324 560 523 1383 28		
Decryption ASCII code of message	49 50 51 52 53		
Decryption of message	12345		

Table(4.3): implementation of RSA encryption and decryption for P=61 and Q=97

Parameters	P=61	Q=97	N=5917
Public key	7		
Privet key	823		
Message	12345		
ASCII code of inter message in hexadecimal	49 50 51 52 53		
Cipher text of the entered message	751 5562 3268 5592 5823		
Decryption ASCII code of the message	49 50 51 52 53		
Decryption of message	12345		

4.6 Practical Performance Evaluation;

The scheme in Figure 3.2 was implemented using the software. Where the C# language was chosen because it is a programming language that supports the platforms that generate Windows software used and the results were as shown in the following curves.

4.6.1 Heart rate measurement

The figure in the results above depicts the heart rate over time, which is measured for a patient when the device is set up in practice

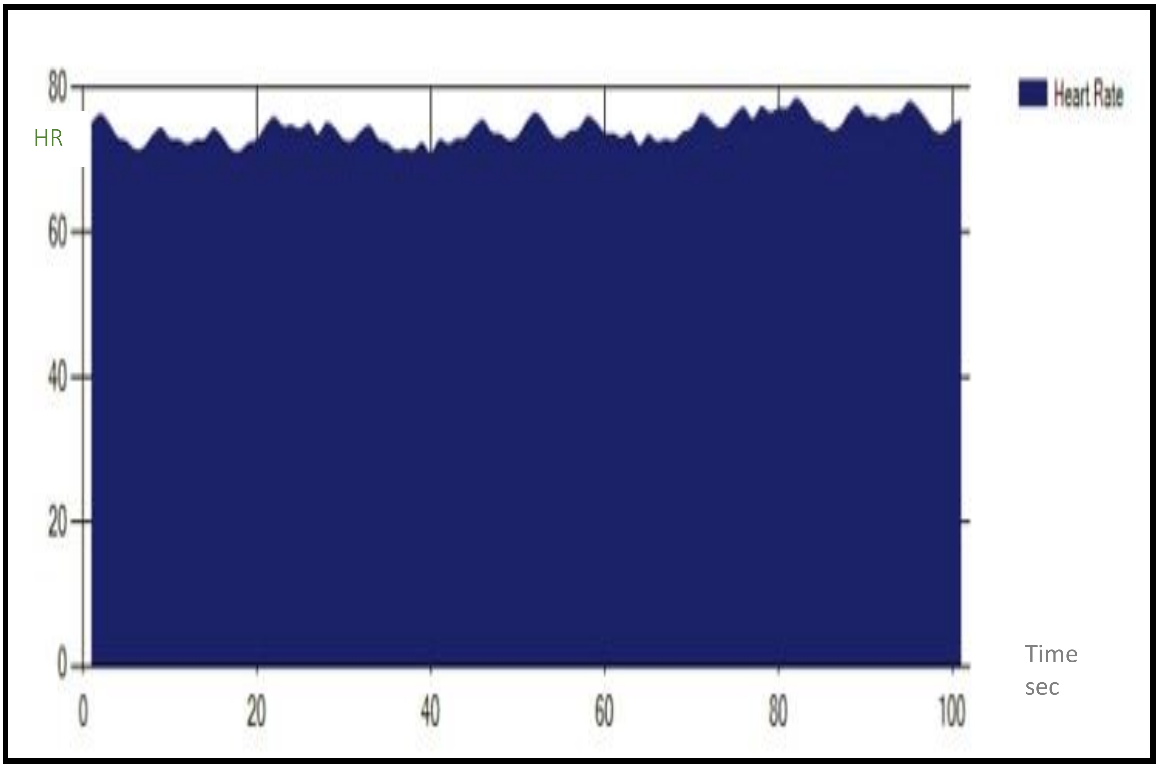


Figure (4.4): Heart rate is measured.

4.6.2 Temperature measurement

The temperature over time, which is measured in practice for a patient with the device set up, is depicted in the results above in the figure.

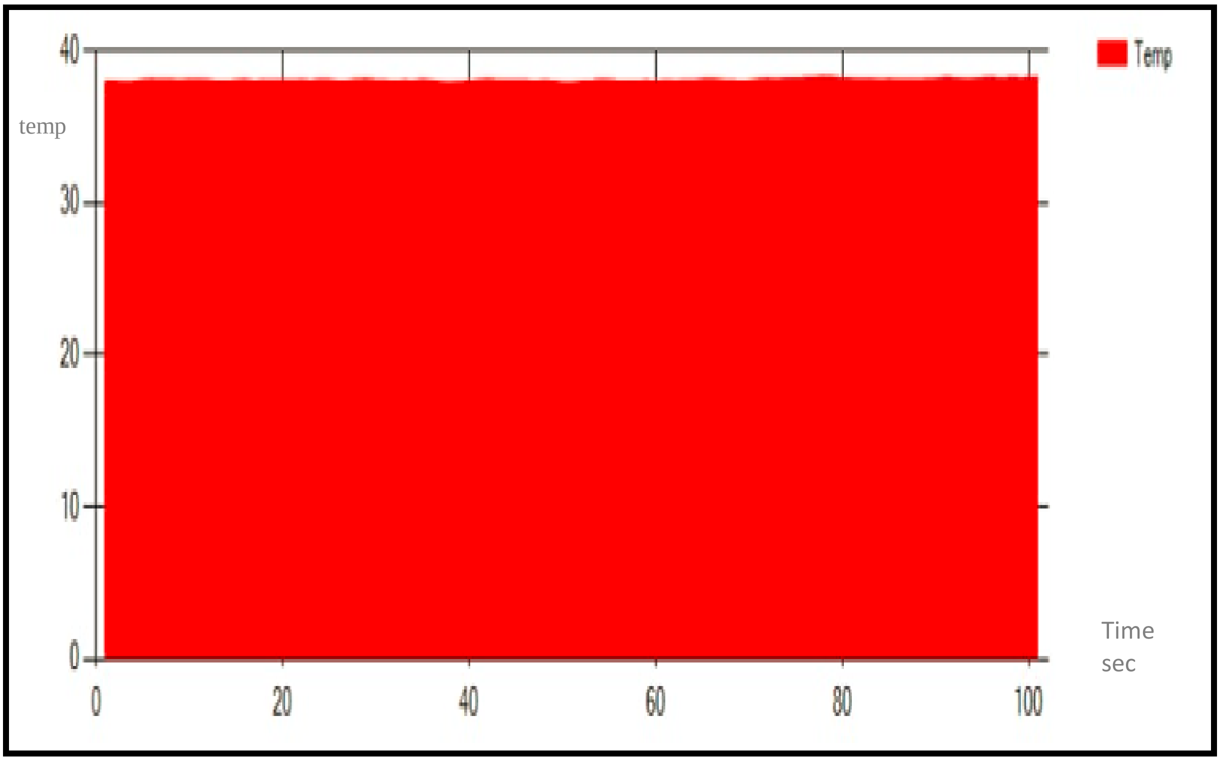


Figure (4.5): Temperature is measured.

4.6.3 Cough measurement

The figure in the findings above depicts the Cough over time, which is measured for a patient using the device in a clinical setting.

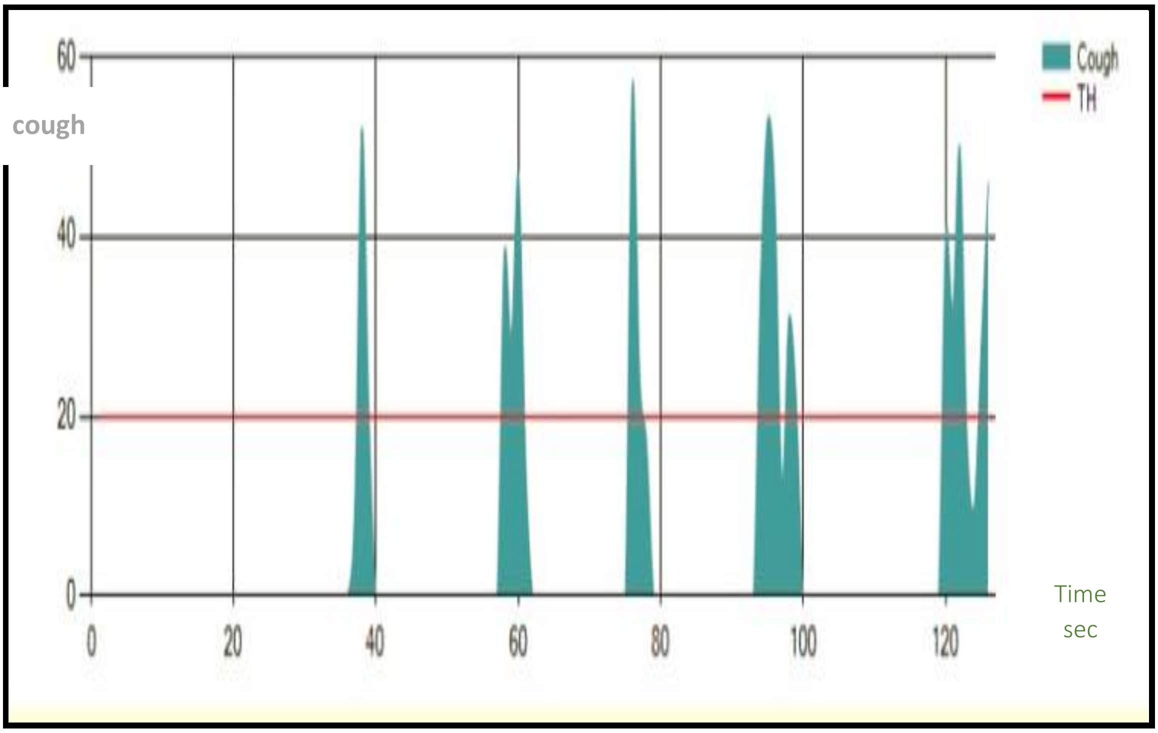


Figure (4.6): **The measurement of Cough in real life.**

4.7 Secondary pc GUI

In this section, the graphical user interface that appears to us after using the device in practice, which is near the patient and tracks his condition in the process

Inside the hospital or even if it is in the patient's home, this interface appears to us where

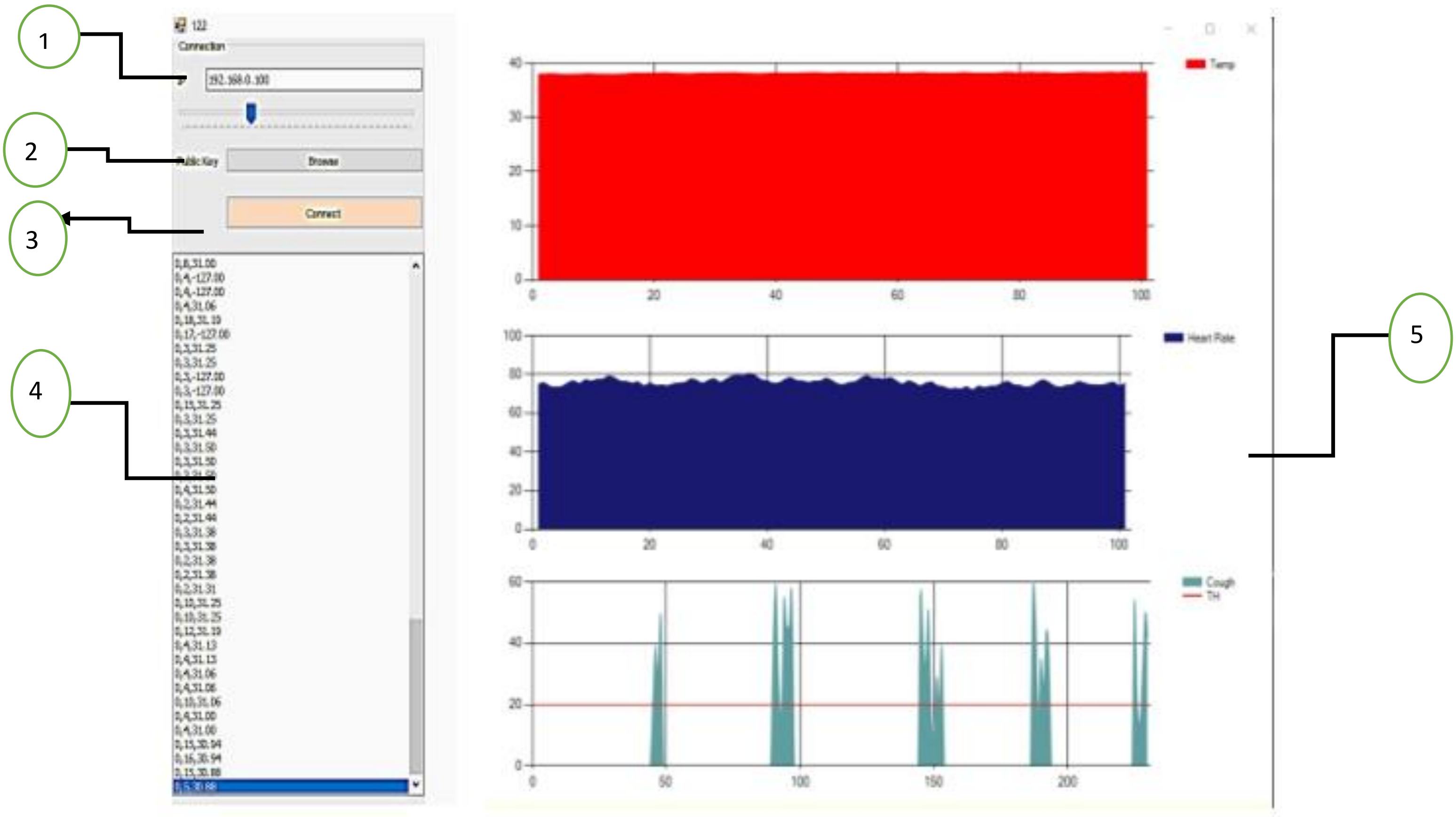
1- it must put the IP of the patient's computer

2- It represents the public key entry generated using the RSA algorithm

3- Representing the operation of the interface and showing the results

4- It represents the digital display of the results for each of the temperature, sound, and heart rate

5-Presentation of the results in curves



IP 192.168.0.100

```
0,8,31.00
0,4,-127.00
0,4,-127.00
0,4,31.06
0,18,31.19
0,17,-127.00
0,3,31.25
0,3,31.25
0,3,-127.00
0,3,-127.00
0,15,31.25
0,3,31.25
0,3,31.44
0,3,31.50
0,3,31.50
0,2,31.50
0,4,31.50
0,2,31.44
0,2,31.44
0,3,31.38
0,3,31.38
0,2,31.38
0,2,31.38
0,2,31.31
0,10,31.25
0,10,31.25
0,12,31.19
0,4,31.13
0,4,31.13
0,4,31.06
0,4,31.06
0,10,31.06
0,4,31.00
0,4,31.00
0,15,30.94
0,16,30.94
0,15,30.88
0,5,30.88
```

Figure (4.7): The Secondary pc GUI

4.8 Doctor GUI

In this section, the graphical user interface that appears to us after using the device in practice, which is close to the doctor where the doctor monitors the patient's condition, follows up, and takes the necessary action for him according to his health condition, and it will explain the details of the graphic user interface in detail as follows;

1- It is the Internet address or website link, and it is an essential part of the Uniform Resource Identifier, through which Internet sites are identified.

2- Here it will generate the cryptographic keys for the RSA algorithm (public and private) that will be generated when the key generation key is pressed.

3- In this key, the encryption key will be entered and run to open the encrypted data and display it in the interface

4- After selecting the private key, it will start booting with the start key

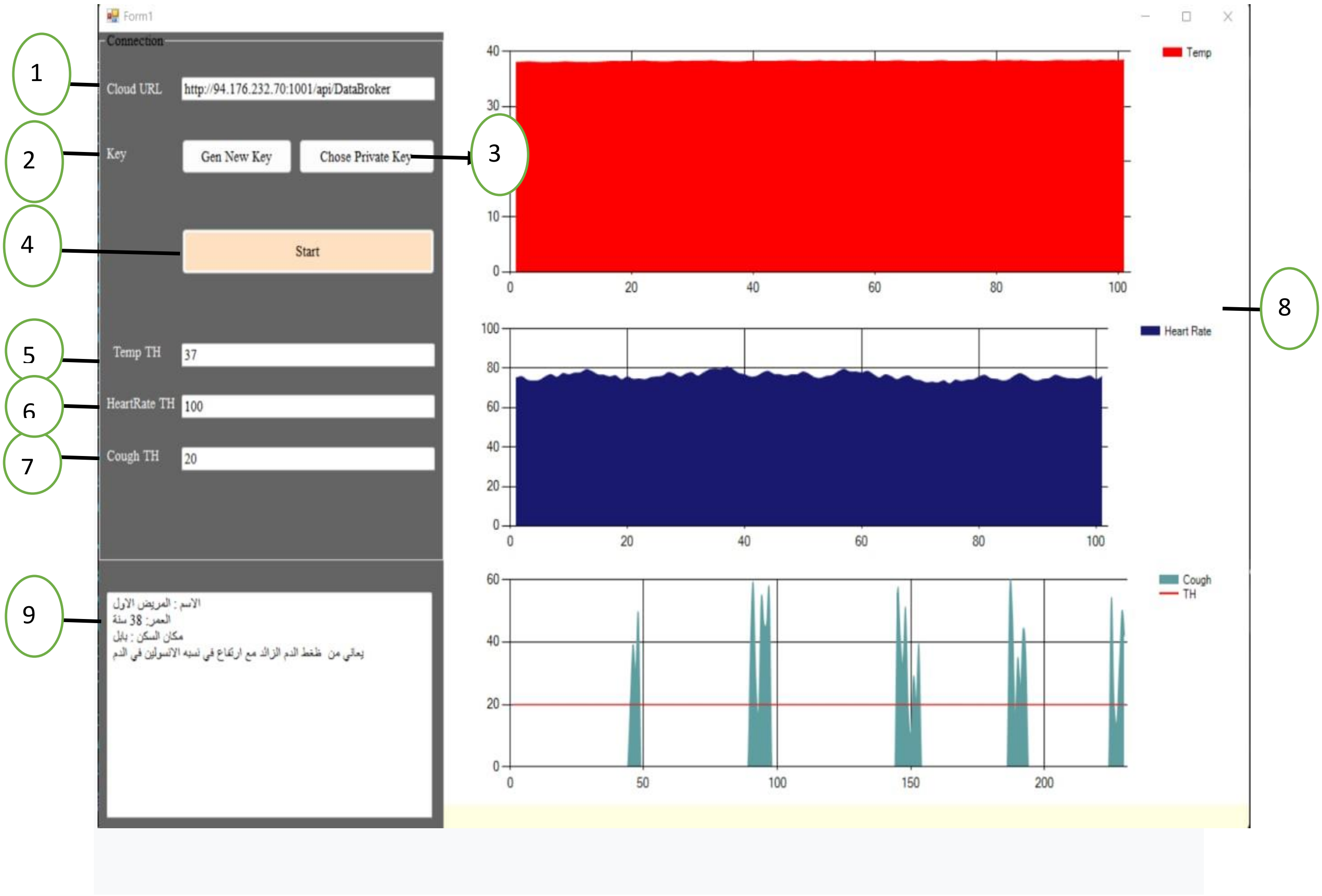
5- That it defines the temperature threshold that when the patient’s temperature is exceeded, an emergency will be announced and the doctor will be alerted to take the necessary measures for the case, which has been set at a temperature of 37 degrees, and this threshold can be changed according to the condition, gender, age and according to the doctor’s opinion

6- That it defines the heart rate threshold that when the patient's heart rate is exceeded, an emergency will be declared and the doctor will be alerted to take the necessary measures for the case, which have been set at a rate of 100 beats per minute.

7- That it defines the cough sound threshold that when exceeded by the patient's coughing sound, an emergency will be declared and the doctor will be alerted to take the necessary measures for the case, which is set at 60 dB. The patient's health status, gender, age, and the doctor's recommendation may all influence this limit.

8- Display results in curves for a temperature, heart rate, and cough sound

9- This part can be called the notes board where he can write anything related to the patient from his name, age, other diseases, and previous diagnoses so that the doctor can follow the patient's condition and know all the previous procedures



Cloud URL http://94.176.232.70:1001/api/DataBroker

Temp TH 37

HeartRate TH 100

Cough TH 20

الاسم : المريض الاول
العمر: 38 سنة
مكان السكن : بابل
يعاني من ظغط الدم الزائد مع ارتفاع في نسبه الانسولين في الدم

Figure (4.8): Doctor GUI

4.9 Data Reading Comparison

The proposed system was tested against a reference device (electronic thermometer, heart rate ox meter, and digital sound level meter). This subsection, looked at different ages and genders of people, female and male, and used the proposed framework and compared it to reference devices. All data is collected at the same time and from a different hand. In the proposed system, it can see the data close by while measuring heart rate, sound, and temperature. As the normal temperatures should be from 35 to 37 degrees, which is not heat, and more than that, is considered high, as for the sound of a normal cough as well, it ranges between 20db and 60db, and if the degree increases more than that, it will be a stronger and more severe cough, and thus it is considered a critical condition. The heart rate ranges during rest and should be between 60 and 100 beats per minute, if it rises more than that it is considered a dangerous and embarrassing condition. The measured data with different ages are listed in the tables (4.5):

Table (4.4): Measurement values for males using reference devices against the proposed framework

Gender	Sl. No.	Reference devices				Proposed framework		
		Age	Heart rate	sound	Temperature	Heart rate	sound	Temperature
Male	1.	8	80	50	36.6	85	55	37.1
Male	2.	15	85	57	37	81	59	37
Male	3.	35	88	60	36	91	59	36.2
Male	4.	43	115	62	35.5	120	63	36.1
Male	5.	65	67	53	36.7	65	53	37

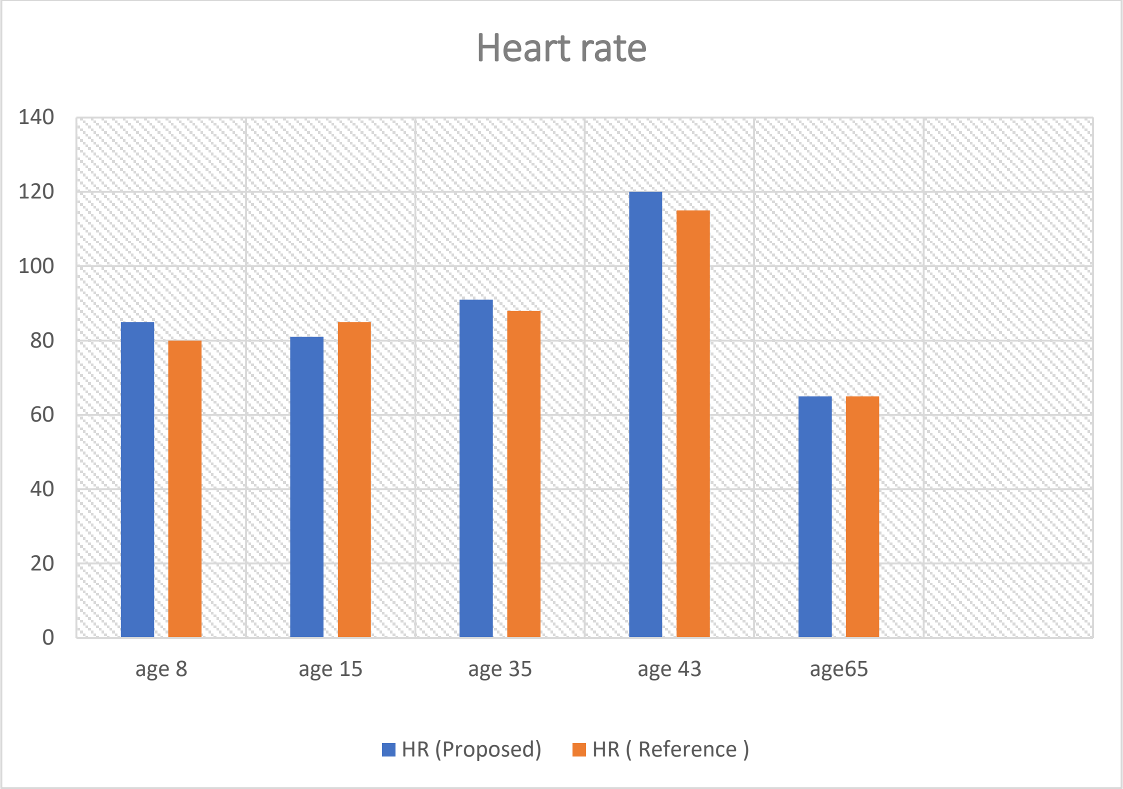


Figure (4.9): comparison of the measures of heart rate using a proposed framework with a reference device

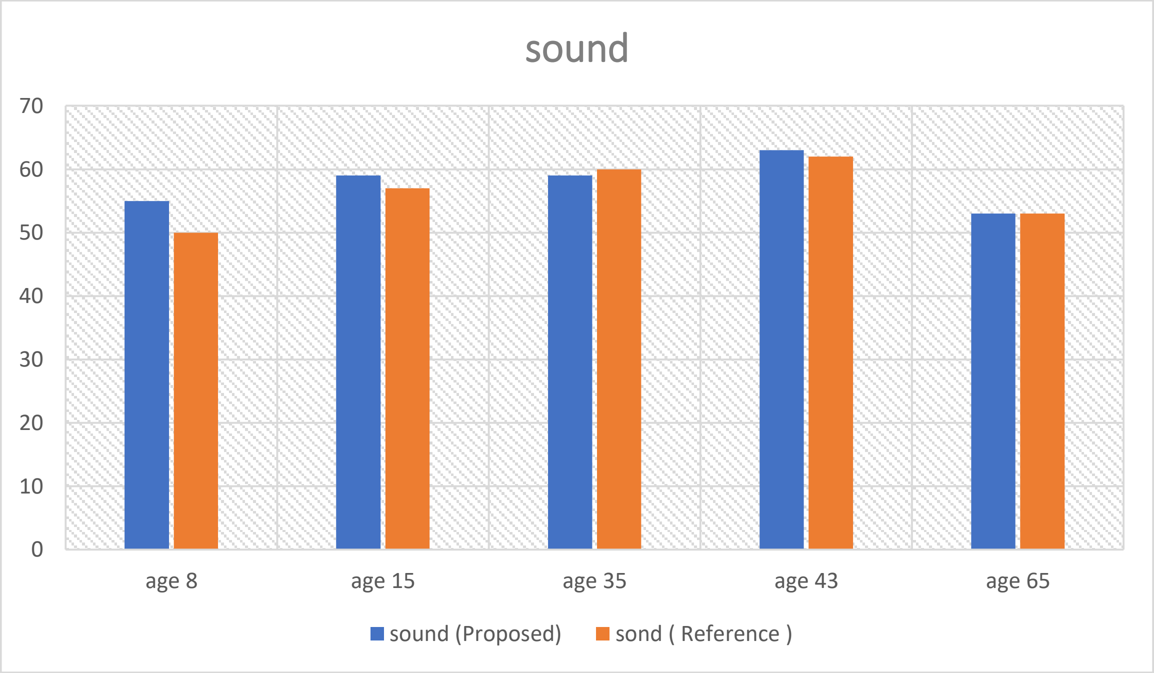


Figure (4.10): comparison of the measures sound using a proposed framework with a reference device

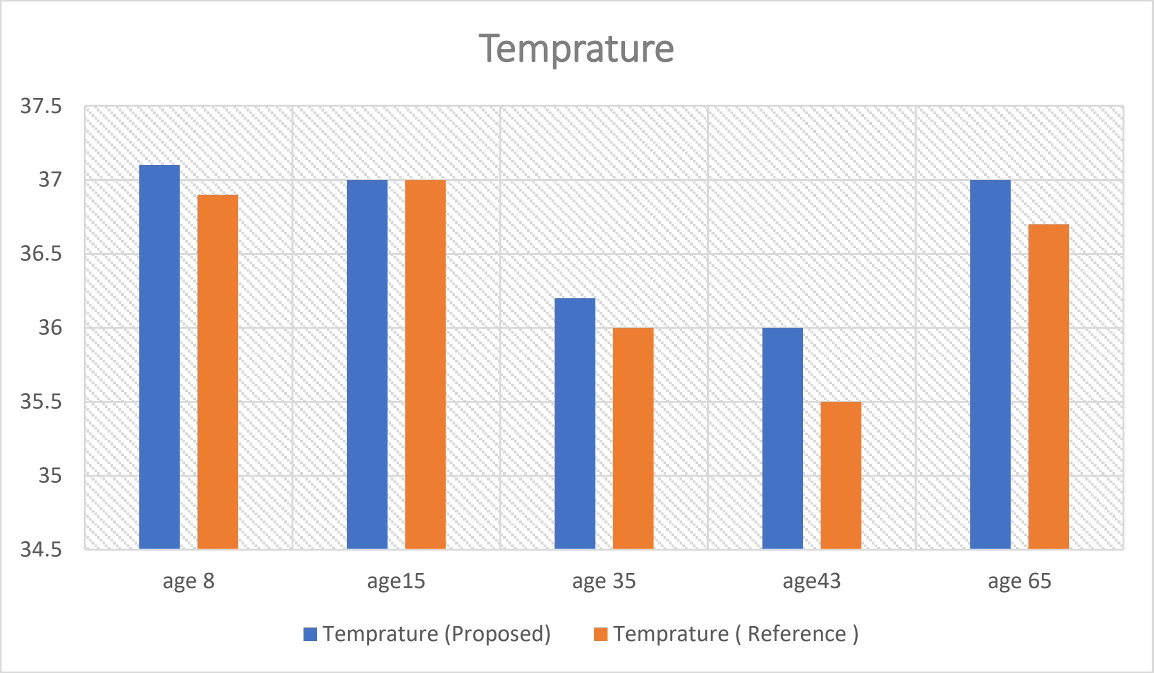


Figure (4.11): comparison of the measures temperature using a proposed framework with a reference device

Table (4.5): Measurement values for females using reference devices against the proposed framework

Gender	Sl. No.	Reference devices				Proposed framework		
		Age	Heart rate	sound	Temperature	Heart rate	sound	Temperature
Female	1.	10	80	51	36.7	78	54	37.2
Female	2.	14	81	55	36.6	85	58	36.9
Female	3.	25	83	60	35.5	85	61	36
Female	4.	37	72	54	36	72	56	36
Female	5.	70	71	50	36.3	67	51	36.7

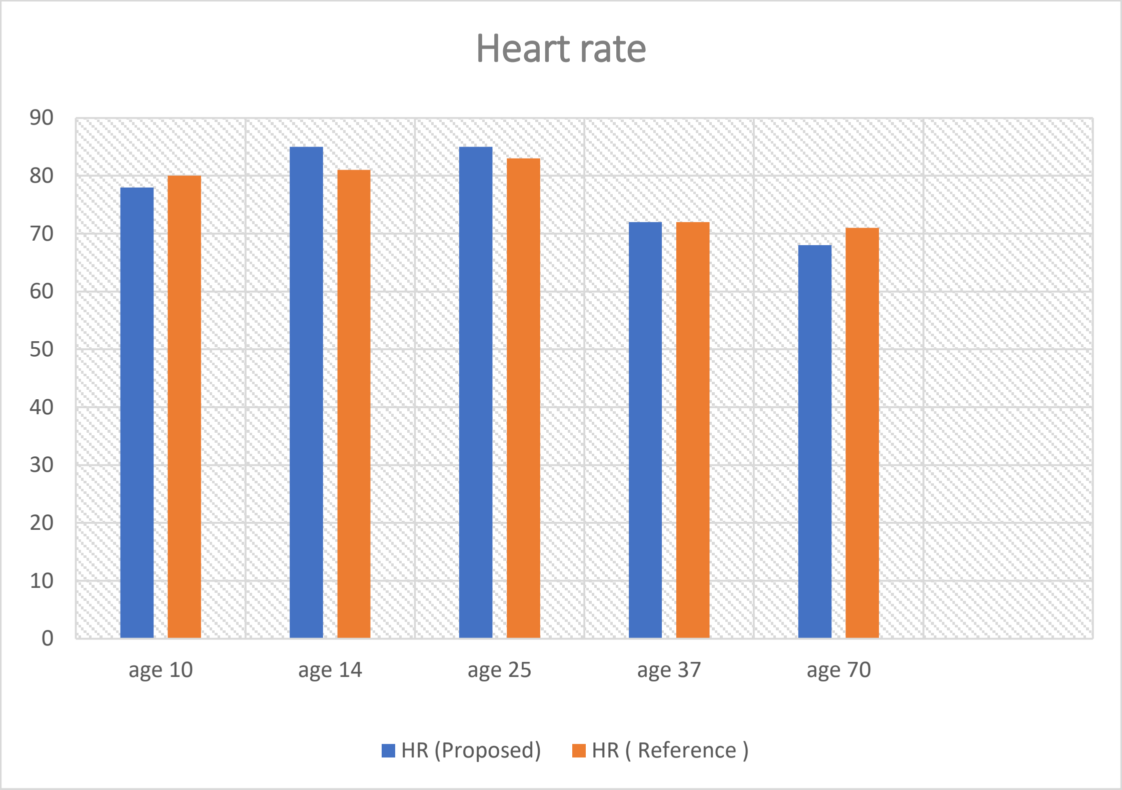


Figure (4.12): comparison of the measures of heart rate using a proposed framework with a reference device

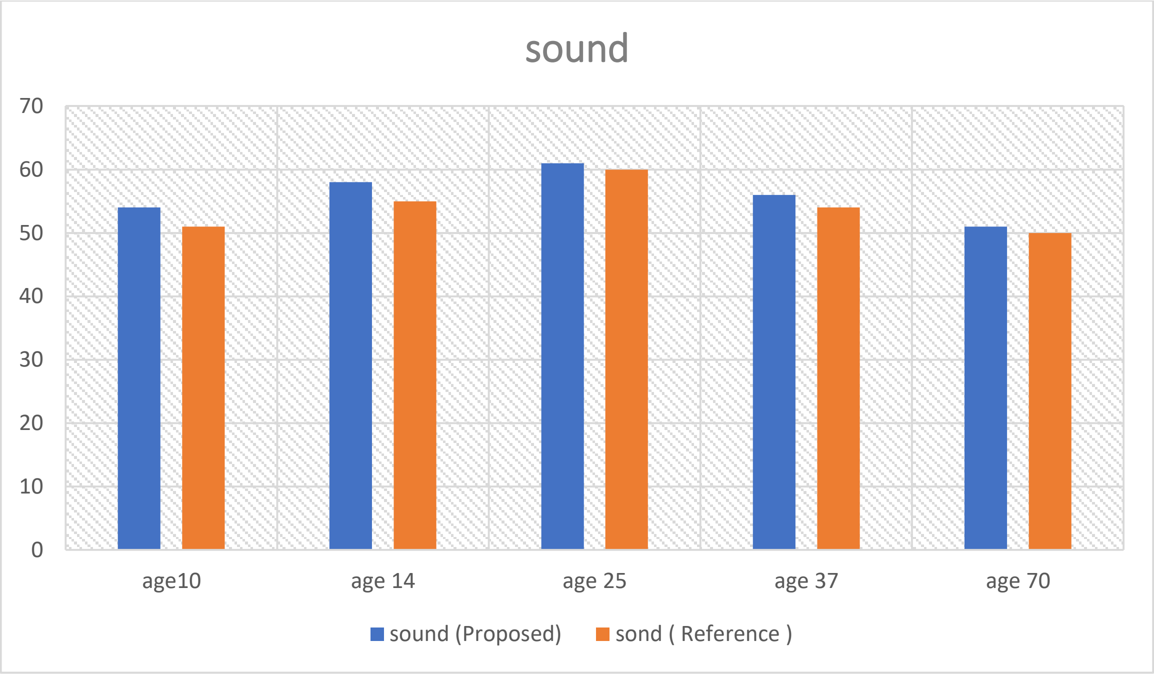


Figure (4.13): comparison of the measures sound using a proposed framework with a reference device

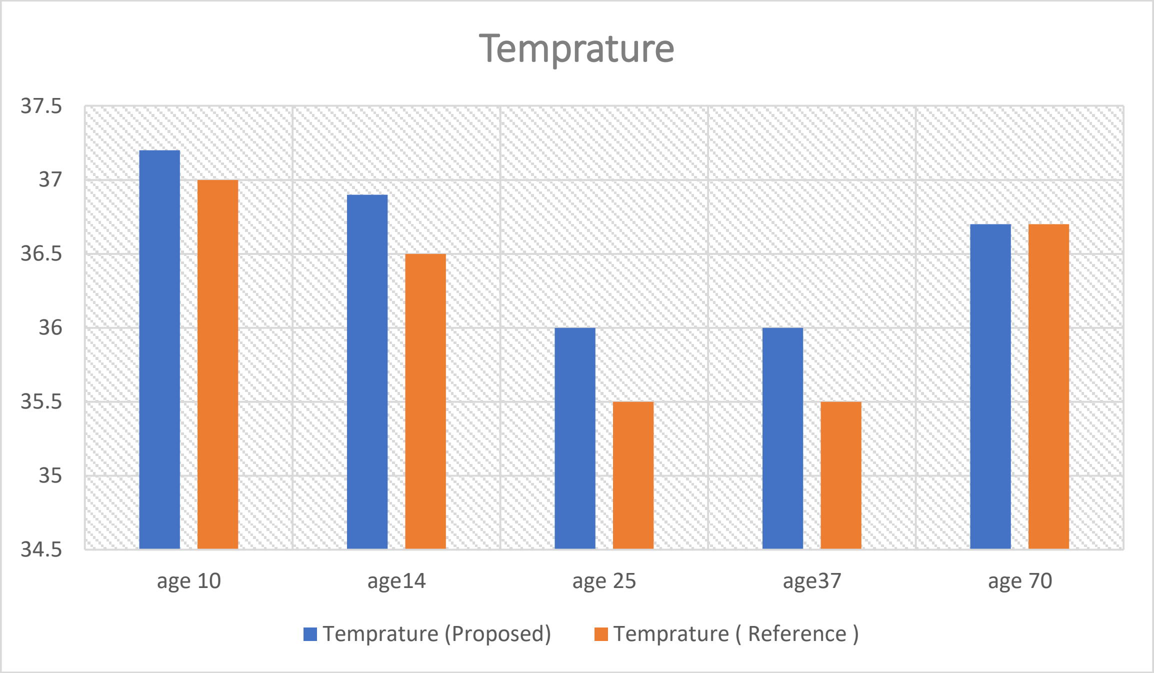


Figure (4.14) comparison of the measures temperature using a proposed framework with a reference device

4.10 comparisons with some researchers:

Table (4.6); Comparison with some research by other researchers

Authors	Year	Proposed	Best search result	The result of our system
-M. Shankar Lingam -Raghavendra Gs -Arun Kumar- -V. Anand	**2020**	In this paper, we propose encryption and data aggregation techniques to enhance the security of healthcare	Encrypted using data compression level up to 12.4	Data transmission from the sensors is encrypted with the RSA algorithm and sent through the cloud for

		systems using IoT sensors and devices.		only the doctor to receive, where the data is encrypted in a strong, efficient and successful way.
Kadhim Takleef Kadhim	**2020**	New people control system suffering from heart disease is proposed in this thesis	The proposed system has been designed and successfully implemented based on Internet of Things (IoT) technology and the system can be used to sense a sudden change in vital signs of patients of all ages.	
-Kedir Mamo Besher **Zareen Subah-** **-Dr. Mohammed Zamshed Ali**	**2020**	Suggesting an encryption algorithm embedded in the sensor to the patient immediately before sending it	Encrypted using the suggestion to add one number or one letter to the sent message	
-RanjeetaPandhare **-Swatee S. Nikam**	**2021**	Use the AES encryption algorithm to get effective data	Create encryption more efficient and powerful than other	

		encryption across the Internet of Things	algorithms	

- When data is compressed at a level higher than 12.4, this data will be distorted and thus limited to a certain size of transmitted data. Thus, our search is better in terms of the amount of data transmitted.
- In the second research, we found that the data was successfully collected and transmitted using the Internet of Things, but without the use of encryption for this data, and therefore it is vulnerable, so our research is better in terms of patient data safety.
- The encryption algorithm level is very weak and insecure as it is suggested to add one number or one letter to the sent message so that this algorithm is almost worthless and the hacker can easily detect it. The RSA encryption algorithm we used is very strong and cannot be hacked.
- In the fourth research, this encryption algorithm is effective in encrypting data, but it is very slow compared to the RSA algorithm because it contains computational complexities that make it take a long time, and types of computers with a powerful processor must be able to encrypt, and it is also a symmetric algorithm that is the same as the encryption key in decryption which the hacker can decrypt using all possible combinations

Chapter Five

Conclusion and Future Works

CHAPTER FIVE

CONCLUSION AND FUTURE WORKS

5.1 Conclusions

1. Practical application is very beneficial because it reduces direct patient contact and remote follow-up, gradually reduces the use of human resources and increases the operational efficiency of advanced and affordable technology resources.
2. The proposed system provides direct access to patient data through the use of the doctor's personal computer from anywhere so that it is a high-quality environment that is easy to use reliably via the cloud.
3. The system provides instant alerts in case of an emergency regarding the patient's vital signs, thus prompt and timely treatment
4. Ease of developing the implemented system in practice by adding devices and sensors and programming them in proportion to the function for which they were designed, making it a high-quality and accurate development environment.
5. The speed of your Internet network is an important factor in transmitting reports and data between the local server and the cloud for this system.
6. The use of system data graphical user interface makes the system highly efficient for display and information exchange.

5.2 Future Works

The future suggested by the authors is summarized as follow:

1. Including more sensors by the demands of the medical institution. Using the required hardware and software components to identify emergency vital signs that affect the patient's situation through a comparison of the measurement data for the measured vital signs for all patients and extract the worst critical condition among them and then send a report of the critical condition that needs medical intervention faster than others.
2. Use urgent alarms depending on the worst critical status among patients through calls, E-mail, or SMS notifications.
3. Use machine learning /AI to identify and classify to separate urgent and normal data.

References

[1] P. Gope and T. Hwang, "Untraceable sensor movement in distributed IoT infrastructure," *IEEE Sensors Journal,* vol. 15, no. 9, pp. 5340-5348, 2015.

[2] P. Gope and T. Hwang, "A realistic lightweight authentication protocol preserving strong anonymity for securing RFID system," *computers & security,* vol. 55, pp. 271-280, 2015.

[3] Y. Liao, M. S. Leeson, M. D. Higgins, and C. Bai, "Analysis of in-to-out wireless body area network systems: Towards QoS-aware health internet of things applications," *Electronics,* vol. 5, no. 3, p. 38, 2016.

[4] V. Mainanwal, M. Gupta, and S. K. Upadhayay, "A survey on wireless body area network: Security technology and its design methodology issue," in *2015 international conference on innovations in information, embedded and communication systems (ICIIECS)*, 2015: IEEE, pp. 1-5.

[5] P. Gope and T. Hwang, "BSN-Care: A secure IoT-based modern healthcare system using body sensor network," *IEEE sensors journal,* vol. 16, no. 5, pp. 1368-1376, 2015.

[6] S. R. Islam, D. Kwak, M. H. Kabir, M. Hossain, and K.-S. Kwak, "The internet of things for health care: a comprehensive survey," *IEEE access,* vol. 3, pp. 678-708, 2015.

[7] Y. J. Fan, Y. H. Yin, L. Da Xu, Y. Zeng, and F. Wu, "IoT-based smart rehabilitation system," *IEEE transactions on industrial informatics,* vol. 10, no. 2, pp. 1568-1577, 2014.

[8] H. Moosavi and F. M. Bui, "Optimal relay selection and power control with quality-of-service provisioning in wireless body area networks," *IEEE Transactions on Wireless Communications,* vol. 15, no. 8, pp. 5497-5510, 2016.

[9] X. Chen, M. Ma, and A. Liu, "Dynamic power management and adaptive packet size selection for IoT in e-Healthcare," *Computers & Electrical Engineering,* vol. 65, pp. 357-375, 2018.

[10] A. Alkhayyat, O. Gazi, and S. B. Sadkhan, "The role of delay and connectivity in throughput reduction of cooperative decentralized wireless networks," *Mathematical Problems in Engineering,* vol. 2015, 2015.

[11] J. Who and F. E. Consultation, "Diet, nutrition and the prevention of chronic diseases," *World Health Organ Tech Rep Ser,* vol. 916, no. i-viii, pp. 1-149, 2003.

[12] S. Cirani, M. Picone, P. Gonizzi, L. Veltri, and G. Ferrari, "Iot-oas: An oauth-based authorization service architecture for secure services in iot scenarios," *IEEE sensors journal,* vol. 15, no. 2, pp. 1224-1234, 2014.

References

[15] A. Darwish, A. E. Hassanien, M. Elhoseny, A. K. Sangaiah, and K. Muhammad, "The impact of the hybrid platform of internet of things and cloud computing on healthcare systems: opportunities, challenges, and open problems," *Journal of Ambient Intelligence and Humanized Computing,* vol. 10, pp. 4151-4166, 2019.

[16] E. Luo, M. Z. A. Bhuiyan, G. Wang, M. A. Rahman, J. Wu, and M. Atiquzzaman, "Privacyprotector: Privacy-protected patient data collection in IoT-based healthcare systems," *IEEE Communications Magazine,* vol. 56, no. 2, pp. 163-168, 2018.

[17] B. Farahani, F. Firouzi, V. Chang, M. Badaroglu, N. Constant, and K. Mankodiya, "Towards fog-driven IoT eHealth: Promises and challenges of IoT in medicine and healthcare," *Future Generation Computer Systems,* vol. 78, pp. 659-676, 2018.

[18] F. Ali *et al.*, "Type-2 fuzzy ontology–aided recommendation systems for IoT–based healthcare," *Computer Communications,* vol. 119, pp. 138-155, 2018.

[19] G. Rathee, A. Sharma, H. Saini, R. Kumar, and R. Iqbal, "A hybrid framework for multimedia data processing in IoT-healthcare using blockchain technology," *Multimedia Tools and Applications,* vol. 79, no. 15-16, pp. 9711-9733, 2020.

[20] J. A. Alzubi, "Blockchain-based Lamport Merkle digital signature: authentication tool in IoT healthcare," *Computer Communications,* vol. 170, pp. 200-208, 2021.

[21] X. Jia, D. He, N. Kumar, and K.-K. R. Choo, "Authenticated key agreement scheme for fog-driven IoT healthcare system," *Wireless Networks,* vol. 25, pp. 4737-4750, 2019.

[22] B. Preveze, A. Alkhayyat, F. Abedi, A. M. Jawad, and A. S. Abosinnee, "SDN-Driven Internet of Health Things: A Novel Adaptive Switching Technique for Hospital Healthcare Monitoring System," *Wireless Communications and Mobile Computing,* vol. 2022, 2022.

[23] C. M. Kumar, R. Amin, and M. Brindha, "Cryptanalysis and improvement of REAS-TMIS: Resource-efficient authentication scheme for telecare medical information system," *Security and Privacy,* vol. 6, no. 1, p. e268, 2023.

[24] V. Kumar, M. S. Mahmoud, A. Alkhayyat, J. Srinivas, M. Ahmad, and A. Kumari, "RAPCHI: Robust authentication protocol for IoMT-based cloud-healthcare infrastructure," *The Journal of Supercomputing,* vol. 78, no. 14, pp. 16167-16196, 2022

[25] D. M. Barakah and M. Ammad-uddin, "A survey of challenges and applications of wireless body area network (WBAN) and role of a virtual doctor server in existing architecture," in *2012 Third International Conference on Intelligent Systems Modelling and Simulation*, 2012: IEEE, pp. 214-219.

[26] S. Ullah *et al.*, "A comprehensive survey of wireless body area networks: On PHY, MAC, and network layers solutions," *Journal of medical systems,* vol. 36, pp. 1065-1094, 2012.

[27] M. Asam *et al.*, "Challenges in wireless body area network," *International Journal of Advanced Computer Science and Applications,* vol. 10, no. 11, 2019.

[28] N. Javaid, N. A. Khan, M. Shakir, M. A. Khan, S. H. Bouk, and Z. A. Khan, "Ubiquitous healthcare in wireless body area networks-a survey," *arXiv preprint arXiv:1303.2062,* 2013.

[29] R. K. Kodali, G. Swamy, and B. Lakshmi, "An implementation of IoT for healthcare," in *2015 IEEE Recent Advances in Intelligent Computational Systems (RAICS)*, 2015: IEEE, pp. 411-416.

[30] S. Tyagi, A. Agarwal, and P. Maheshwari, "A conceptual framework for IoT-based healthcare system using cloud computing," in *2016 6th International Conference-Cloud System and Big Data Engineering (Confluence)*, 2016: IEEE, pp. 503-507.

[31] U. Satija, B. Ramkumar, and M. S. Manikandan, "Real-time signal quality-aware ECG telemetry system for IoT-based health care monitoring," *IEEE Internet of Things Journal,* vol. 4, no. 3, pp. 815-823, 2017.

[32] A. D. Acharya and S. N. Patil, "IoT based health care monitoring kit," in *2020 Fourth international conference on computing methodologies and communication (ICCMC)*, 2020: IEEE, pp. 363-368.

[33] M. Janveja and G. Trivedi, "An area and power efficient VLSI architecture for ECG feature extraction for wearable IoT healthcare applications," *Integration,* vol. 82, pp. 96-103, 2022.

[34] D. S. R. Krishnan, S. C. Gupta, and T. Choudhury, "An IoT based patient health monitoring system," in *2018 international conference on advances in computing and communication engineering (ICACCE)*, 2018: IEEE, pp. 01-07.

[35] H. Nozari, M. Fallah, H. Kazemipoor, and S. E. Najafi, "Big data analysis of IoT-based supply chain management considering FMCG industries," *Бизнес-информатика,* vol. 15, no. 1 (eng), pp. 78-96, 2021.

[36] W. Diffie and M. E. Hellman, "New directions in cryptography," in *Democratizing Cryptography: The Work of Whitfield Diffie and Martin Hellman*, 2022, pp. 365-390.

[37] M. L. Sahari and I. Boukemara, "A pseudo-random numbers generator based on a novel 3D chaotic map with an application to color image encryption," *Nonlinear Dynamics,* vol. 94, pp. 723-744, 2018.

[38] F. Farsana and K. Gopakumar, "A novel approach for speech encryption: Zaslavsky map as pseudo random number generator," *Procedia computer science,* vol. 93, pp. 816-823, 2016.

[39] M. Backes and B. Pfitzmann, "Relating symbolic and cryptographic secrecy," *IEEE Transactions on Dependable and Secure Computing,* vol. 2, no. 2, pp. 109-123, 2005.

[40] S. Nisha and M. Farik, "RSA Public Key Cryptography Algorithm," *A Review. International Journal of Scientific and Technological Research,* vol. 6, pp. 187-191, 2017.

[41] A. A. Ayele and V. Sreenivasarao, "A modified RSA encryption technique based on multiple public keys," *International Journal of Innovative Research in Computer and Communication Engineering,* vol. 1, no. 4, pp. 859-864, 2013.

[42] D. Mahto and D. K. Yadav, "Performance Analysis of RSA and Elliptic Curve Cryptography," *Int. J. Netw. Secur.,* vol. 20, no. 4, pp. 625-635, 2018.

[43] S. Venkatraman and A. Overmars, "New method of prime factorisation-based attacks on RSA Authentication in IoT," *Cryptography,* vol. 3, no. 3, p. 20, 2019.

[44] L. O. Mailloux, C. D. Lewis II, C. Riggs, and M. R. Grimaila, "Post-quantum cryptography: what advancements in quantum computing mean for it professionals," *IT Professional,* vol. 18, no. 5, pp. 42-47, 2016.

[45] M. Mumtaz and L. Ping, "Forty years of attacks on the RSA cryptosystem: A brief survey," *Journal of Discrete Mathematical Sciences and Cryptography,* vol. 22, no. 1, pp. 9-29, 2019.

[46] L. MATYSIAK, "Generalized RSA cipher and Diffie-Hellman protocol," *Journal of applied mathematics & informatics,* vol. 39, no. 1_2, pp. 93-103, 2021.

[47] P. C. Kocher, "Cryptanalysis of Diffie-Hellman, RSA, DSS, and other systems using timing attacks," in *Extended abstract*, 1995: Citeseer.

[48] M. Ahmed, B. Sanjabi, D. Aldiaz, A. Rezaei, and H. Omotunde, "Diffie-Hellman and its application in security protocols," *International Journal of Engineering Science and Innovative Technology (IJESIT)*, vol. 1, no. 2, pp. 69-73, 2012.

[49] M. Ahmed, B. Sanjabi, D. Aldiaz, A. Rezaei, and H. Omotunde, "Diffie-Hellman and its application in security protocols," *International Journal of Engineering Science and Innovative Technology (IJESIT)*, vol. 1, no. 2, pp. 69-73, 2012.

[50] M. Ahmed, B. Sanjabi, D. Aldiaz, A. Rezaei, and H. Omotunde, "Diffie-Hellman and its application in security protocols," *International Journal of Engineering Science and Innovative Technology (IJESIT)*, vol. 1, no. 2, pp. 69-73, 2012.

[51] M. Dečman and M. Vintar, "A possible solution for digital preservation of e-government: A centralised repository within a cloud computing framework," in *Aslib Proceedings*, 2013: Emerald Group Publishing Limited.

[52] A. P. Rajan, "Evolution of cloud storage as cloud computing infrastructure service," *arXiv preprint arXiv:1308.1303*, 2013.

[53] N. Serrano, G. Gallardo, and J. Hernantes, "Infrastructure as a service and cloud technologies," *IEEE Software*, vol. 32, no. 2, pp. 30-36, 2015.

[54] N. N. ALMutairi and S. F. Thuwaini, "Cloud computing uses for e-government in the middle east region opportunities and challenges," *International Journal of Business and Management*, vol. 10, no. 4, p. 60, 2015.

[55] U. Somani, K. Lakhani, and M. Mundra, "Implementing digital signature with RSA encryption algorithm to enhance the Data Security of cloud in Cloud Computing," in *2010 First International Conference On Parallel, Distributed and Grid Computing (PDGC 2010)*, 2010: IEEE, pp. 211-216.

الخلاصة

شهدت السنوات الأخيرة ارتفاعًا في عدد السكان المسنين (الذين تبلغ أعمارهم ٦٥ عامًا فأكثر) في عدد من البلدان ، حيث زاد عدد المسنين في العالم. نمت القدرة على إجراء مراقبة عن بعد لحالة الجسم والبيئة المحيطة من أجل فحص الحالة الصحية للأفراد الأكبر سنًا الذين لديهم موارد مالية محدودة والوصول إلى الخدمات الطبية المعاصرة. لذلك من الضروري مراقبة جميع الحركات والأنشطة الجسدية التي تتم في الحياة اليومية. تشكل شبكة منطقة الجسم اللاسلكية أحد أنظمة المراقبة (WBAN). يتكون WBAN من أجهزة استشعار موضوعة حول الجسم أو صغيرة بما يكفي لإدخالها داخل الجسم

لقد كان دمج وإدماج مستشعرات WBAN في إنترنت الأشياء (IoT) موضوعًا يحظى باهتمام كبير بين المجتمعات العلمية والصناعية نظرًا للتأثير الثوري الذي أحدثته على الوجود البشري. أدى التطور السريع لتكنولوجيا إنترنت الأشياء إلى تغيير الوجود البشري من خلال إدخال ، من بين ابتكارات أخرى ، الأدوات الذكية ، والرعاية الصحية الذكية ، والصناعة الذكية ، والمدن الذكية ، والشبكات الذكية.

أدى التطور السريع لتكنولوجيا إنترنت الأشياء إلى تغيير الوجود البشري من خلال إدخال ، من بين ابتكارات أخرى ، الأدوات الذكية ، والرعاية الصحية الذكية ، والصناعة الذكية ، والمدن الذكية ، والشبكات الذكية.

يهدف هذا العمل إلى تصميم نظام مراقبة جديد للمريض باستخدام خوارزمية أمان RSA ونقل المعلومات عبر وسيط لاسلكي من المريض إلى كمبيوتر الطبيب. يتكون النظام المقترح من ثلاثة أجزاء ، أولاً ، تم أخذ ثلاثة أجهزة استشعار في الاعتبار ، وهي معدل ضربات القلب ودرجة الحرارة والصوت. ثانيًا ، نظام جديد يقوم بمعالجة البيانات وتشفيرها باستخدام خوارزمية RSA والتي يمكن إرسالها عبر الإنترنت إلى الطبيب البعيد.

أخيرًا ، يتم تخزين البيانات ومعالجتها وفك تشفيرها في السحابة ثم حلها ليتم عرضها في جهاز كمبيوتر الطبيب. في كمبيوتر الطبيب ، يتم عرض البيانات باستخدام منصة جديدة مقترحة تتضمن عمر براءة الاختراع وجنس المريض ومعدل ضربات القلب ودرجة الحرارة وصوت السعال.

بالإضافة إلى ذلك ، تم تحليل أداء النظام باستخدام أدوات المحاكاة بواسطة Matlab. في المحاكاة ، يعتبر BER بمثابة مقياس أداء لإظهار تأثير استخدام خوارزمية RSA على الأداء.

الخلاصة

يوضح النظام المقترح أنه يمكن نقل البيانات عبر الوسائط اللاسلكية والإنترنت بأداء عالٍ من الموثوقية والأمان مقارنة بالعمل الأخير ، ثم طور واجهة مستخدم جديدة لعرض بيانات المريض بكفاءة.

يقترح استخدام التعلم الآلي لتحليل البيانات الواردة واقتراح الخدمة المناسبة للمريض.

وزارة التعليم العالي والبحث العلمي

جامعة بابــل / كلية الهندسة

قسم الهندسة الكهربائية

تصميم نظام مراقبة الرعاية الصحية باستخدام شبكة منطقة الجسم الآمنة غير المرنة بناءً على إنترنت الأشياء

رسالة
مقدمة الى كلية الهندسة في جامعة بابل
كجزء من متطلبات نيل درجة الماجستير في علوم الهندسة الكهربائية/اتصالات

من قبل

ضحى عاجل جاسم الحيدري

اشراف

الأستاذ الدكتور سعد سفاح حسون

١٤٤٤هـ ٢٠٢٢م