

Project Report (Major Project- II)

on

**A Novel Affirmation Structure In light of Biometric and Radio Fingerprinting
for the IoT in e-Health with Matrices**

Submitted in partial fulfilment of the requirements

for the award of the degree of

Master of Technology

in

Software Technology

By

Biplav Kumar

Roll No.: - 2K16/SWT/502

Under the guidance of

Dr. Manoj Kumar

Associate Professor



Department of Computer Science & Engineering

Delhi Technological University

(Formerly Delhi College of Engineering)

Bawana Road, Delhi 110042

2019



Delhi Technological University
(Formerly Delhi College of Engineering)
Bawana Road, New Delhi-42

DECLARATION

I hereby declare that the thesis entitled “**A Novel Affirmation Structure In light of Biometric and Radio Fingerprinting for the IoT in e-Health with Matrices**” which is being submitted to the Delhi Technological University, in partial fulfilment of the requirements for the award of the degree of Master of Technology in Software Technology is an authentic work carried out by me. The material contained in this thesis has not been submitted to any university or institution for the award of any degree.

DATE: 24/07/2020

SIGNATURE:

A handwritten signature in black ink, appearing to read "Biplav Kumar", written over a horizontal line.

Biplav Kumar

2K16/SWT/502

CERTIFICATE



Delhi Technological University

(Formerly Delhi College of Engineering)

Bawana Road, New Delhi-42

This is to certify that project report entitled “**A Novel Affirmation Structure In light of Biometric and Radio Fingerprinting for the IoT in e-Health with Matrices**” done by me for the Major Project 2 for the award of degree of Master of Technology Degree in Software Technology in the Department of Computer Science & Engineering, Delhi Technological University, New Delhi is an authentic work carried out by me.

Signature:

A handwritten signature in black ink, appearing to read "Biplav", with a long horizontal stroke extending to the right.

Student Name

Biplav Kumar

2K16/SWT/502

Above Statement given by Student is Correct.

A handwritten signature in black ink, appearing to read "Manoj", with a long horizontal stroke extending to the right.

Project Guide:

Dr. Manoj Kumar

Associate Professor

**Department of Computer
Science & Engineering**

**Delhi Technological
University, Delhi**

Acknowledgement

No volume of words is enough to express my gratitude towards my guide **Dr. Manoj Kumar**, Department of Computer Science & Engineering, Delhi Technological University, Delhi, who has been very concerned and has aided for all the materials essentials for the preparation of this project report. He has helped me to explore this vast topic in an organized manner and provided me all the ideas on how to work towards a research-oriented venture.

I am also thankful to **Dr. Rajni Jindal**, HoD of Computer Science & Engineering Department and **Dr. Ruchika Malhotra** , Coordinator , for the motivation and inspiration that triggered me for the project work.

I would also like to thank the staff members and my colleagues who were always there at the need of hour and provided with all the help and facilities, which I required, for the completion of my project work.

Most importantly, I would like to thank my parents and the almighty for showing me the right direction, to help me stay calm in the oddest of the times and keep moving even at times when there was no hope.



Biplav Kumar
(2K16/SWT/502)

ABSTRACT

An overall system of Internet of Things (IoT) will be the next generation that associates various application domains, usefulness, along innovation. The articles were interestingly addressable as well as utilize fixed correspondence convention with impart over the heterogeneous systems administration condition. Whenever, wherever interfacing anything thought brought out critical headways in the human services space. This thesis primarily focuses about the actualized true situation of keen self-governing doctor's facility administration with the IoT. This thesis also, goes for clarifying about innovation perceptions behind this area has a human services by data on information displaying of medicinal applications, diagnosis gadgets, information approval of basic occurrence information, information connectivity of different techniques information to various frameworks information, work process or the procedure stream behind the specialized tasks on the wireless-coordination, middleware layer, database, application administrations.

Indexed Terms—Security, Privacy, Biometric, Finger Print Detection.

Table Of Contents

CHAPTER 1

INTRODUCTION	1
1.1 Background	1
1.2 Internet of Things	2
1.2.1 Types of Sensors	4
1.3 Healthcare System and Internet of Things	5
1.4 Biometric and Radio Fingerprinting	6
1.5 Security Concerns on Internet Based Modules	6
1.6 Authentication Protocols	9
1.6.1 Authentication Using Biometrics	9
1.6.2 Issues Faced by Biometric Systems	10
1.7 Problem Statement	10
1.8 Purpose of The Project	11

CHAPTER 2

LITERATURE SURVEY	12
--------------------------	-----------

CHAPTER 3

METHODOLOGY	16
3.1 Authentication Techniques	16
3.1.1 Biometric Based	16
3.1.2 Radio Fingerprinting Technique	16
3.2 Existing Work	17
3.3 Proposed Method	18
3.3.1 Algorithm and Framework	19
3.3.2 Proposed Algorithm	20
3.3.3 Requirements:	22

3.3.4 Architecture of Secure e-Health	22
3.4 Data Acquisition and Sensing	25
3.5 Device to Network Authentication	30
3.6 Implementation	31
CHAPTER 4	
EXPERIMENTAL RESULTS	33
4.1 Action Responses	35
CHAPTER 5	
CONCLUSION AND FUTURE WORK	38
5.1 Conclusion	38
References	40

List of Figures

Figure 1.1: Normal ECG sinus signal.....	3
Figure 1.2: Vulnerabilities and patient data.....	8
Figure 3.1: Example of user validations.....	18
Figure 3.2: Medical Data Validations.....	18
Figure 3.3: Algorithm framework.....	20
Figure 3.4: ESP8266 Wi-Fi module.....	22
Figure 3.5: Model of Hospital management system (HMS).....	24
Figure 3.6: Secure e-Health monitoring framework architecture.....	24
Figure 3.7: DTLS handshake.....	27
Figure 3.8: Circuitry of the model.....	29
Figure 3.9: Experimental Setup.....	29
Figure 3.10: Authentication through radio fingerprint for PDA device.....	30
Figure 3.11: Schema of BSN care network.....	31
Figure 3.12: ThingSpeak™ web page.....	31
Figure 3.13: Creating channel on ThingSpeak site.....	32
Figure 3.14: Device connectivity through API key.....	32
Figure 4.1: Sample output.....	33
Figure 4.2: Heart-rate and date values.....	34
Figure 4.3: Systolic pressure.....	34
Figure 4.4: Diastolic Pressure.....	34
Figure 4.5: Alert messages sent to the phone.....	35
Figure 4.6: Frequency generation.....	36
Figure 4.7: Throughput comparison.....	36

Chapter 1

INTRODUCTION

1.1 Background

The great many people who are in need of ongoing medical treatment and the rising health care costs of medical services have sparked the idea of remote health observation. In the long term tracking, administration and therapeutic exposure to individual physiological knowledge throughout parallel to the limited therapeutic wellness area covered by the existing methods, investigators have found uses of these innovations in personalized medicine in interactive remote monitoring frameworks. Various wearable sensors connected to the patient's body could also be used to do the same. Such access points focus on ensuring that vital signals and health are regularly measured (Gope & Hwang, 2015), such as heart rate, blood pressure, temperature, etc. The obtained information is first transmitted wirelessly to small distances via connected networks to localized portals (cell-phones, tablets PDAs, etc). Then it's submitted into a clinical repository, which is subsequently, processed and interpreted by the medical practitioners. Using the observational data as well as the course of action via support networks, which also allow those certain individuals connect directly to a wide range of observed data, the quality of life can indeed be smarter predicted and recommended by the physiologist, early diagnosis and proper medical care and treatment actions which are especially helpful at enhancing the quality of life and wellbeing. This startling technology might turn the world's medical systems and help cut-down overall-care costs dramatically and increase diagnostic speed and efficiency.

Completely computerized, computerised therapeutic records by the institutionalized medicinal services IoT over the specialized conveyance framework empower the "advanced healing facility". This to be sure prompts a specialized worldview needs a return to and tweaking in the information displaying, information sharing by information mapping with various frameworks, business process work processes with appropriate information benefits (Jain et al., 2016). Setting effective restorative applications require coordination of various sorts of sound, video, discrete or simple information from different therapeutic gadgets. The whole therapeutic IOT (Jain et al., 2006) stage should be based on Administration Arranged Design with the well characterize middleware,

database, process setup achievability, information displaying, mapping, information collection for various restorative gadgets information coordination, constant and cluster medicinal investigation calculations and safety efforts. The innovation brings out a worldview path for latest advancements in modern era.

The advancement of IT and communication engineering and communication instrumentality is adding another paradigm, the Internet of Things (IoT). IoT makes people and objects in the physical world to communicate with one another in a mechanical system that works, conveying knowledge areas such as systems delivering intelligent, transmitting information to a place like intelligence transfer systems. the great city, smart and beautiful city, medical framework and strengthened as part of the many digital outcomes (Wortmann & Flüchter, 2015). IoT is defined as the framework for billions of people, devices and communications, integrated seamlessly into their daily processes through controllers and sensors. The "Internet of Things" will rule the world and serve as a common platform for connecting the physical, the physical objects, the devices, humans, allowing new ways of working, communicating, controlling, functioning and living. The increasing health care costs as well as the proliferation of chronic illnesses worldwide desperately call for a transition in health-care from hospitals to a community focused on people and social welfare (Niranjana & Balamurugan, 2015; Rahmani et al., 2015).

The expense of connected Internet of Things apps, cellphones and networks continues to decrease. Everyone and everything can conveniently be seen digitally 24hrs per day over wifi networks. Interaction is quicker, more omnipresent and affordable and will certainly affect people to have access to knowledge and significant data. Technological progress and Internet of Things became fuelled by the introduction of radio frequency identification (RFID) related sensors and technological approaches as well as other linked frameworks.

1.2 Internet of Things

The existing Web is developing increasingly into the IoT-environment in which various devices interact and share data for enhanced functionality and productivity. The IoT deals with many numbers of things, such as devices, sensors, and applicable data, numerous real security trends need to be dealt with (Bardyn et al., 2016). One essential characteristic of IoT is the service customization. In IoT, the current main stream of Human-to-Device communication will be gathered to Human-to-Human (H2H), Human-to-Thing (H2T), and Thing-to-Thing (T2T). The H2T channel is still crucial, as humans often trigger various services (Gia et al., 2014). The ECG

signal, as shown in Figure 1.1, has a unique morphological shape due to the anatomical structure of the heart and physiological conditions. The ECG morphology consists of, but not limited to, the P, R, and T waves amplitudes, the slope information for each segment, and the temporal distance between wave boundaries (Satija et al., 2017).

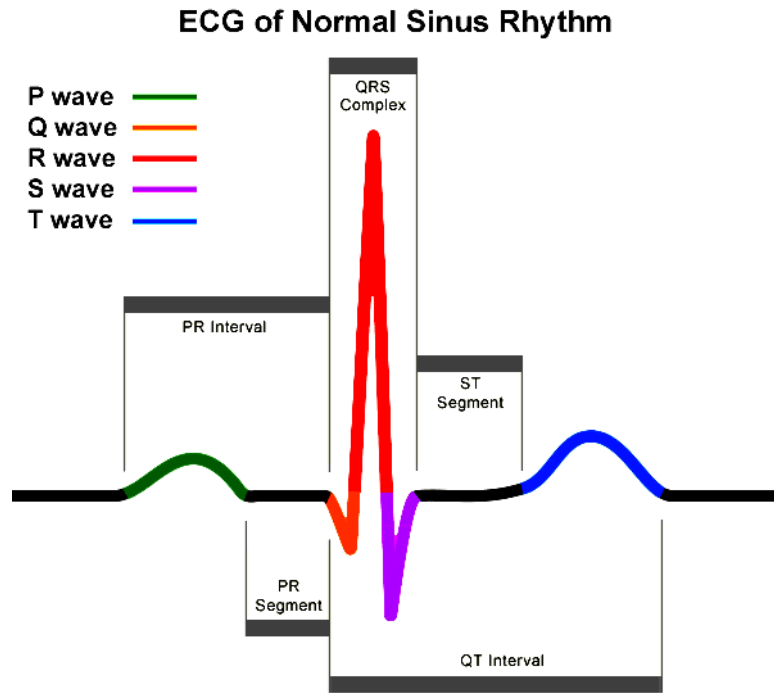


Figure 1.1: Normal ECG sinus signal (*Source: skippinghearts.de*)

With the development of IoT and biometric innovation, validation is by and large totally rethought. Sending IoT security is one of the immense difficulties in the between associated world, and it requires an answer that depends on the most grounded verifications. This is the overcome new universe of the Web of Things (IoT). The security vulnerabilities of the IoT are near as shifted as the gadgets and sensors associated with it. Existing techniques for verification, for example, passwords supported by a moment factor, are being rendered unsettled because of human mistake and the upgraded complexity of malware and different assaults.

The IoT might enable the patients to still be in various places, including house, workplace, social setting or automobiles, etc. while tracking the person's medical parameters with wearable body sensors, wherein, the physiological sensors are still attached and wirelessly transmitting data to the physician or hospital database. The device could have several advantages while utilizing the IoT's modular *body sensors network* (BSN) programme for e-Health including heart diseases control, elderly tracking as well as data collection, security and monitoring of individual's

fitness (Chiuchisan et al., 2014; Rahmani et al., 2015). The primary aim of the modular BSN programme would be to facilitate the current medical process through real-time processing and data collection of both the heart rates and vital symptoms of medical information for clients.

1.2.1 Types of Sensors

A. Finger Print Sensor:

The examples of rubbing edges and valleys on a person's fingertips are remarkable to that person. For quite a long time, law authorization has been arranging and deciding personality by coordinating key purposes of edge endings and bifurcations (Wayman 2001). Fingerprints are one of a kind for each finger of a man including indistinguishable twins.

B. Facial Picture:

A few ways to deal with displaying facial pictures in the obvious range are Important Part Investigation, Nearby Element Examination, neural systems, versatile chart hypothesis, and multi-determination examination. Significant advantages of facial recognition are that it is non-nosy, without hands, and persistent and acknowledged by generally clients (Galbally et al., 2014).

C. Hand Detection:

These techniques for individual confirmation are entrenched. Hand detection has been accessible for more than twenty years.

D. Mark Classifications:

Advantages of mark biometric frameworks:

1. While it is anything but difficult to duplicate the picture of a mark, it is to a great degree hard to impersonate the conduct of marking;
2. Low classifications Rates (FAR);
3. Individuals are accustomed to marking archives, so signature detections frameworks are not apparent to be obtrusive.

E. Voice or Discourse Recognition:

Entirely, the voice is likewise a physiological characteristic on the grounds that everyone has an alternate pitch, however, voice recognition is predominantly in light of the investigation of the way a man talks, normally delegated social.

1.3 Healthcare System and Internet of Things

Health care system is among the biggest issues confronting any country at the moment. Even though the health care sector decides to invest in IT, the expected increase in health and safety and quality had not yet been accomplished in line with expectations. Medical institutions mostly depend nowadays on provided facts and decision-making based on medical history and written prescriptions. The integration of biomedical infrastructure and IoT technologies could help biomedical providers concentrate their attention on statistically significant information and better quality of care, allowing prompt, efficient and early diagnosis with lower expenses. By the utilization of RFID identifiers, detectors/sensors and advanced devices the Internet of things will offer several advantages to medical care. This facilitates online communication, recognizing and monitoring individual patients, addresses of physician's records and monitoring of patient's health records including devices, storage, risk mitigation as well as prescription counterfeiting, respectively.

This empowers people, technologies, cognitive applications including complex frameworks smartly that also provide an efficient health and tracking framework, tracking of biomedical assets as well as the mechanism for managing biomedical wastes (Hiremath et al., 2014). Wear-able sensors on the patient's body, for example in this case, will also keep an eye on body temperature, heart rate, platelet counts, insulin and blood pressure as well as continuously submit these records to tablets or smartphones of doctors and also to prescription reaffirmation, traipses, etc. (Haghi et al., 2017).

The Internet of Things is going to revolutionize healthcare in terms of investment, security, privacy, reliability and return- on-investment (ROI), if truly trusted by medical enterprises and community. The tracking and monitoring of patients and healthcare actors are one of the biggest challenging research directions for IoT Healthcare.

Consider an example wherein, the patient wears a monitoring device to collect own physical and sleep activities information. These monitoring devices can be sensors/RFID tags which are strategically placed on the human body. Sensors/RFID tags can be used as per required implementation for e.g. stand-alone devices or can be embedded into jewellery, surgically embedded on the skin/other body part, can be attached to user's clothes or shoes, thus creating WBSN. Each such node in the WBSN is typically capable of sensing, sampling, processing, and wirelessly communicating one or more physiological signals.

Treatment course and results can too be monitored and analysed in the same way. If someone travelling overseas fell ill, they could provide captured details to local doctors giving immediate access to health records and history, and can get more appropriate treatment as a result. The medicines prescribed by Doctors is available to Pharmacist also. Referring to the given data, any sort of allergies can be taken into account while issuing prescription by the pharmacist. A practitioner attending any sort of traffic accident could check an individual's blood type and pre-existing conditions mentioned in his/her profile.

1.4 Biometric and Radio Fingerprinting

The ceaseless BSN requires continuous confirmation for verified data to set up belief. In context of guaranteeing that the captured data is legit and not erroneous, data verification and validation are vital components within the BSN framework. For this reason, one can utilize verification instrument to guarantee the rightness of information root some time recently the information is utilized for restorative determination. Verification tools based on techniques such as mystery keys, watchword, and tokens have vulnerabilities for the BSN framework. One of the reasons is that on the off chance that a third party gets to the accreditations, at that point he can mimic the real understanding induces information creation and information judgment challenges.

Likewise, after starting verification utilizing such accreditations, there's no insurance that the information is still comes from the verified patients all through the sessions. The framework of BSN requests ceaseless observing of the patients suggesting that the checked information ought to be approved on a nonstop premise till the end of the sessions (Bao et al., 2006; Chowdhury et al., 2010). The BSN's framework ought to guarantee not as it were that the checked information has a place within the real understanding amid the entire observing sessions but also that it is uploaded utilizing the proper gadgets. This could be accomplished utilizing biometrics and radio fingerprinting techniques as they offer coordinate affiliation in relation to the clients as well as the sensor gadgets.

1.5 Security Concerns on Internet Based Modules

The BSN framework security is one of the foremost basic viewpoints of the framework. Individuals have a vast point of view as far as security is concerned and subsequently, it has been addressed in numerous processes. Generally, security may be a context comparative to security of the framework as an entirety. Presently, communication in

between sensors applications (such as BSNs) in health care are mostly remote in nature. This poses various security threats to the framework. There are various security concerns with cloud based systems been posed over to the remotely sensed gadgets. We have portrayed the key authorization necessities in Internet of Things based health care framework implementing BSNs.

A. Data Privacy

Similar to WSNs, the protection of knowledge in IoT based RPMs is considered the greatest concern. The details through release is to be assured. BSN should not move the essential data of patients to other or local networks. The sensor hubs capture and provide the facilitator with sensitive information in an IoT-based medical application. An interceptor can listen and collect basic information in between the transfers. Such listening will bring serious damage to the patients because the adversary could use the information obtained for many unlawful objectives.

B. Data Integrity

It does not guarantee the information is stored secretly by external changes. An attacker can modify data permanently by including a few components or by inspecting information in a bundle. The mediator will obtain this updated material. In some situations the need for a decision is particularly dangerous in the case of life-critical (when circumstances are changed). In fact, the awful contact atmosphere will trigger misfortune in knowledge.

C. Anonymity

The untraceabilities that render the adversary unable to determine and can't say apart if two conversations arise out of the same (obfuscated) patents are once more valuable commodity of the confession (see Figure 1.2). Therefore, in wireless connectivity, surveillance encompasses the package origin (i.e. sensor information). It could be a advantage which can improve privacy.

D. Secure Localization

For the most BSN implementations, a precise measurement of the patents region is necessary. The need for an intelligent portion helps an adversary to dispense almost constant information by describing incorrect flag characteristics. Actually, for a secure and safe IoT healthcare framework to work including BSNs, all above mentioned protection needs to be taken care of by the environment and to eventually be capable of addressing different security hazards and

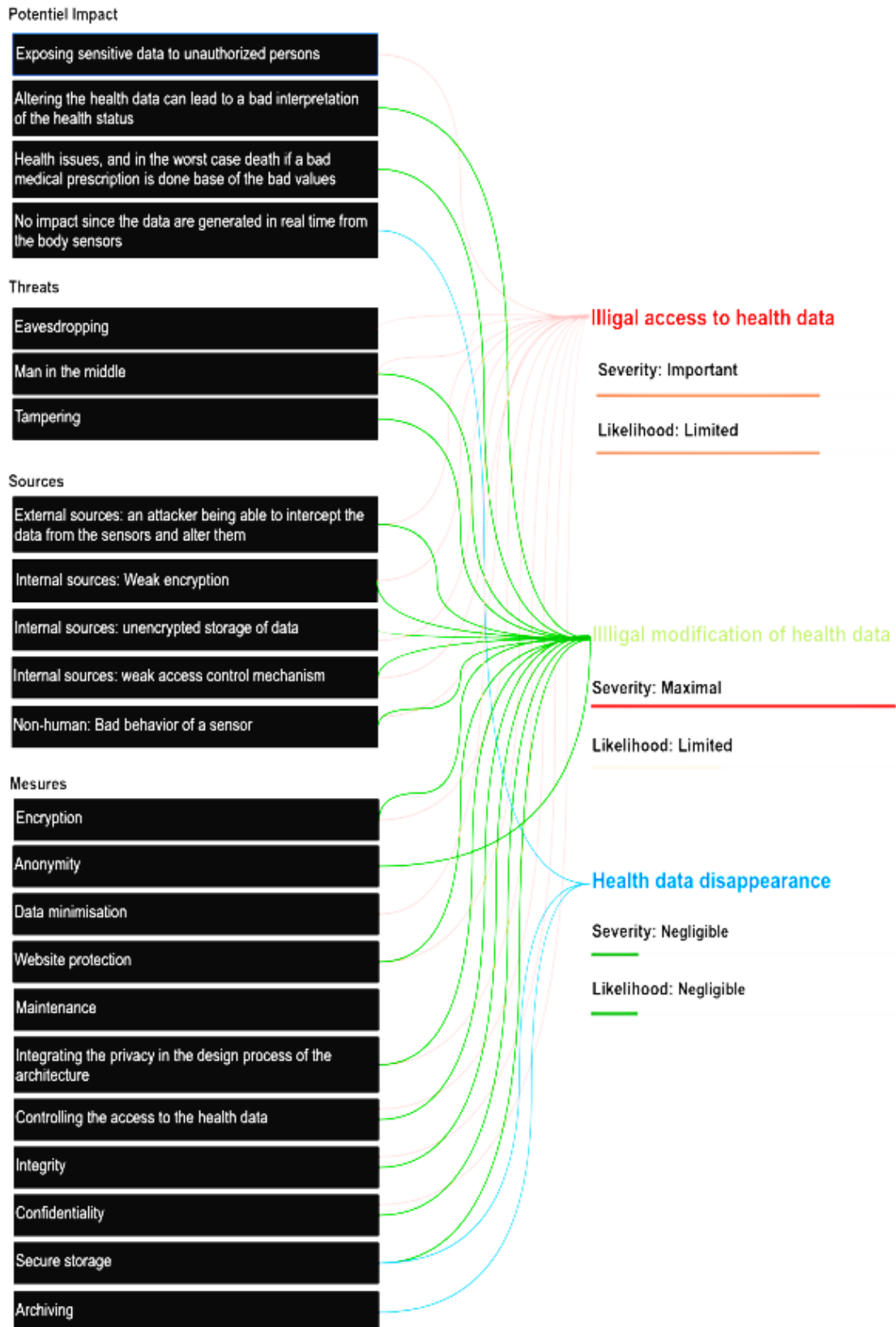


Figure 1.2: Vulnerabilities and patient data

attacks such as manipulation of details, pantomime, listening, repeat, etc. Table II describes the various possible disruptions in Wireless-based health care systems utilising BSNs and IoT.

1.6 Authentication Protocols

1.6.1 Authentication Using Biometrics

The biometric systems for individual identification are expert and smart systems in which interests and demands are rapidly increased in many sectors, such as healthcare applications (Fatemian & Hatzinakos, 2009), security systems, and telecommunications. In the authentication systems, an individual person presents himself/herself as a specific individual and the system checks for his/her biometric features against a profile that exists based on a specific individuals' file to find the match, where this is usually known as a One-to-One matching system. In the next stage, the system will search for the unknown individual (biometric); in this case, the system checks the presented biometric against all of the others in the dataset, which described as a One-to-Many (N) matching system.

Biometric attributes can be isolated into two principle classes, as spoke to in the accompanying instances. Physiological is identified with the state of the body. Illustrations incorporate, however are not restricted to unique mark, confront recognition, hand and palm geometry and iris recognition. Social is identified with the conduct of a man. Trademark executed by utilizing biometrics are mark check, keystroke flow, and voice (Horroo & Sardana, 2012).

Biometric-based authentication represents one of the authentication methods that truly identifies the real applicant as a particular-individual than the other traditional methods, such as passwords, ID cards, and watermarks. Although, some biometrics methods currently exist, these methods are not robust enough against forgery. Whereas the private biometric passes are not protected, spoofing attack shall occur either digitally or physically. For instance, our fingerprints could exist on glasses, doors, and tables; thus, it is possible to be acquired and used. Recently, many researchers (Sidek et al., 2012) have suggested the Electrocardiogram (ECG) as a biometrics method for individuals' authentication. For many decades ago, the ECG has been used as a heart condition diagnosing and monitoring. And, it is still the fast and the non-invasive method for identifying the primary heart problems (Odinaka et al., 2012; Poree et al., 2016).

1.6.2 Issues Faced by Biometric Systems

A few issues related to unimodal biometrics are mentioned below:

- (i) Noise in detected information - A unique mark picture with a scar or a voice test modified by frosty is a case of loud information.
- (ii) Intra-class variations - These variations occur mostly for a client who is mistakenly gets associated with the saved attributes (e.g., erroneous facial stance), or when the templates saved for a client gets altered amid validation.
- (iii) Inter-class resemblances – With a biometric-based framework including an extensive number of clients, there might be interclass similitudes (cover) in the component space of various clients.
- (iv) Non-all-inclusiveness - The biometric framework will be unable to gain significant biometric information from a subset of clients. A unique mark biometric framework, for instance, may extricate inaccurate particulars highlights from the fingerprints of specific people, because of lack of quality in the features. Multimodal-biometric systems tend to the issue of non-all-inclusiveness since different attributes guarantee adequate populace scope.
- (v) Spoof assaults - This sort of assault is particularly important when social characteristics, for example, signature or voice is utilized. Be that as it may, physical characteristics, for example, fingerprints are likewise powerless to caricaturing assaults. Multimodal likewise discourages mocking since it would be troublesome for an impostor to parody different biometric characteristics of a bona fide client at the same time.

1.7 Problem Statement

Since from the beginning of hospital they used to maintain patient's information in paper format. So, it may lose or torn or data may be secretly leaked to third person with known or unknown persons. So, to avoid these difficulties the system e generation patient management systems came into existence. even though the patient credentials are known to the persons inside the hospitals who are working there. So now we are proposing the mechanism where password is secured and patient ID is known to all and password is concerns person finger print sensor or iris by that the data and account will be secure and if patient enters into hospital he/she logs in and save the data and health reports also saves in scanned manner and those privileges also given to a limited people like lab technicians, nurses, medical-shops and Doctors.

1.8 Purpose of The Project

This work centers around the four fundamental perspectives, for example, information models, engineering, work processes – process streams, database choices of the keen healing facility administration framework empowered with IOT restorative gadgets.

A. Therapeutic Gadgets Tallied

All the IoT therapeutic gadgets can be arranged into prescription observing, essential sign checking, movement checking, security sign observing, tolerant personality and research centre checking. Here, the task concentrates just on Imperative Observing.

B. Fundamental Presumptions

In underlying examination, the patient observing in indispensable signs were distant from everyone else considered. For the outside framework coordination, the protection and infection conclusion frameworks are considered. If there should arise an occurrence of the work processes, caution on basic episode alone considered as an utilization case. As to gadget administration, the battery and vitality following issues are considered.

C. Framework Thought

Plan just considers the Administration Oriented Architecture. If there should be an occurrence of system, Wired, Remote, World Wide Web correspondence foundations are considered.

Chapter 2

LITERATURE SURVEY

The practical human services (Srivastava, 2013) data with the security esteems that are followed from the remote gadgets. It provides the patient human services being at the ease of staying at home. "e-ICU" therapeutic suit by Philips enables the medical staff to screen for imperative signs at an emergency unit. A cloud-based restorative stage is being developed by QUALCOMM, which conveys the information to alternate gadgets and interoperable with the HIPPA grumbling frameworks.

Personal "e-Health", self-administration of wellbeing position of privacy in each layer of the Validation techniques as well as protection strategies and correspondence designs are talked about as a major aspect of this work.

Silva et al., (Silva et al., 2011), dissected the execution of brushing the utilization of on-line mark and voice biometrics with a specific end goal to perform client validation in securing electronic therapeutic record. This paper, be that as it may, did not consider patients amid crisis circumstances that can't talk. Due to intrinsic large intra-class inconstancy, the use of on-line validation using biometrics seems likewise harmful. The author basically dissected data security and protection in medicinal services, and furthermore created. This exploration neglected to demonstrate how protection will be kept up at all levels.

Similarly, Mohan et al, (Mohan et al., 2009), produced a system for recording wellbeing records based upon some tolerance value. Although the approach is centred around inner risk and sharing, but it allows acknowledging the crisis for the wellbeing data captured.

Rahmani et al. (Rahmani et al., 2015), exemplified a system for storing wellbeing data in an electronically encrypted form. In their case, approach depends upon well-defined structures being specific in nature, while patient has the control over their own data. While designing they haven't considered the risk associated with the transferrable endorsement puzzle, however they let patients characterize their own encryption process. They foresee that patients might be aware of to whom to endorse when they make (or re-encode) EHRs.

Dube (Dube et al., 2015), utilized Speedy Reaction (QR) codes and cell phones to get to crisis data while saving patient protection of perilous data. The technique utilized was to upload crisis data on advanced cell's secure screen as a two-dimensional barcode tag. In order to examine and decode this encrypted code all one need is an advanced mobile phone application or just a QR code scanner. But in this it is assumed that a patient will carry the cell phone amid a crisis, accordingly it is thought to be unfeasible based on human services.

Brandt (2015), considered to create a framework that can provide partial access to patients data for analysis. The major drawback for this system is that, the patient ought to deal with different keys for different entities and facts involved be it a social insurance suppliers, the nonappearance of a productive client disavowal instrument, requirement for an outer key bond bidding specialist, and the requirement for patients to check the medicinal services supplier's accreditations in proposes a secured EHR framework, Human services framework for Persistent Protection (HCPP) in light of cryptographic developments and existing remote system. Their work outlines plan conventions for secure medicinal services framework utilizing cryptographic instruments.

Mohammed et al. (Mohammed et al., 2014) built a mobile application for the health care approach based on the Google's Android process, known as ' Electro Cardiogram (ECG) Android App.' The programme incorporates cloud computing services and Internet of Things (IoT) and allows any concluding customer to monitor ECG waves and record details on the platform. The data recorded can be sent to the private, consolidated server of the individual or to a different cloud that holds all the information verified and can be accessed by restorative staff for review. Their major concern was to develop a framework and software convening cloud-based services along with IoT applications.

Microsoft has launched a web page (Sunyaev, 2013) in which Google Wellbeing's PHR customers can trade their individual data on a Microsoft Wellbeing Vault account. While Google Wellbeing's downturn illustrates the difficulties of developing an internet PHR sector, by 2015, PHRs will see a 33 percent increase in sales as professionals allow patients to use IT systems for their well-being. Engineering of the Microsoft Associated Wellness System (CHF) (Tyagi et al., 2016) consists of process models, service models and information models.

Gomez et al., (Gomez et al., 2016) presented a design based on a cosmology able of observing the wellbeing of patients

with inveterate infections and giving fitness suggestions. Creators had executed the framework by planning the setting exhibit.

Khoi et al. (Khoi et al., 2015) highlighted the importance of IoT-based health surveillance using remote tools in order to provide care and comfort to elderly people at home itself. Their focus was on the network communication perspective for this remote health surveillance framework and to create a skeleton to evaluate and compare different network communications protocols.

Kitson (2011) center around isolating crisis information from the center of EHR frameworks keeping in mind the end goal to limit the measure of spilled information in instances of crisis. Corresponding model have used different cloud service providers, whilst keeping the information between framework and these providers separate and the data presentation i.e. the way the data is been put forward is been taken care by the framework while utilizing "push" and "draw" techniques to deal with overall methodologies for upgrading and understanding protection amid crisis get to.

Babu et al., (Babu et al., 2013) ideates about a system that uses wearable sensors to monitor and analyse various physiological parameters such as blood pressure and body temperature. In this the wearable transfers the captured data to a gateway server using Bluetooth connection. Further the gateway server converts the received data into an Observation and Measurement file and stores it on a remote server for later analysis by health experts through the Internet. On combining all this with a medical storage which is cloud-based, a health surveillance system is established which enables the access to the same remotely saved data by the medical staff via online mode through content service application.

Recently, Dias & Paulo Silva Cunha (2018), proposed the utilization of biometric distinguishing proof to get to a focal wellbeing record database through wearable devices. The technique utilized was to give the professionals a versatile framework through which they access important qualities of patients EHR utilizing the patient's unique mark amid a crisis. In spite of the fact that, this paper focuses on providing significant access to a patient's wellbeing record remotely whilst providing security authorization and validation using a biometric framework.

It takes into account the patient's unique fingerprint for verification (singular biometrics), but which has its own drawbacks associated. Additionally, on analysing it showed a normal reaction time of 19.8 seconds with around trial bucket of huge chunk of patients from the database. In this paper, we have an expectation of faster reaction time by implementing 6 multimodal biometrics.

Mainetti et al. (2016) proposed an IoT-based Ambient Assisted Living (AAL) system, which, has been designed in order to create better living conditions for older people. The proposal was having a prime objective of keeping the elderly healthy whilst balancing their convenience by keeping their choice of being at ease at their own home. Proposal too were made to overcome the challenges associated with transmission of healthcare data with the available network infrastructure, especially in remote areas, using CoAP. However, they lack in area of authentication and access control, and privacy while focusing mainly on encryption of the data.

Verma & Sood (2018) proposed a concept of fog computing along with a smart gateway to be used for monitoring health of patients remotely. At data acquisition layer using IoT sensors the data is being captured, and the same gets analysed at the fog layer. At the advent of any crisis an alert is sent to the upper layer. However, knowing that their proposed system deals with sensitive information they haven't taken in account most crucial aspect of the system i.e. security and the privacy concerns.

In short on summarizing, all the above previous works lacks in in-depth analysis of various security aspects, specifically those been associated with the access control. In our proposition, the concept incorporates security as one of the core modules of the smart e-health management system, this is realised by enabling a security layer at the application level and by configuring the data flow to be done in encrypted form in between different components.

Chapter 3

METHODOLOGY

In this thesis we have designed and developed an IoT based healthcare system in MATLAB's ThingSpeak™ and also evaluate and verify it by MATLAB program.

3.1 Authentication Techniques

Confirmation could be a crucial pre-condition for maintaining system usability for approved customers in any application environment. The confirms are made with codes, secret buttons, tokens and biometric and fingerprint highlights. We affirm that we posses something (tokens, cryptographer keys), something which belongs to us (physiological and behaviours, such as signatures, confrontations, irises, palm images, expression, hand morphology, deoxyribonucleic acid (DNA), etc.); We do not learn something, and we are not sure that the number of people in question is a good thing. Slavic motion, pattern and characteristic of electrocardiography (ECG) Verification mechanisms can allow either of these (information, rights, and inherent) parameters to be used if a material existing demonstrates its identity. A effective way of reducing the probability of false proof for a product is to incorporate identifying elements, culminating in the testing of multiples variables.

3.1.1 Biometric Based

Compared with the watchword or token-based authentication, biometric verification is deemed much more rooted as the biometric features of each person are clearly recognizable, non-transferable and non-reproductive. Verifications of multi-factor are deemed more dependent than a standard test measurement.

3.1.2 Radio Fingerprinting Technique

The technique of radio fingerprinting employs the properties of remote sensors and their specific traits of representing data to be one of a kind in having a distinguishing proof. The radio fingerprints are created by dissecting the properties of radio flag and are decided by extricating gadget particular highlights that are caused

by equipment impedance. The radio fingerprints are devised by extracting the information from the radio flag for particular properties such as frequency, sufficiency, and stage (Bao et al., 2006; Jain et al., 2016). This process of radio fingerprinting comprises of pre-processing, location, include extraction, and classification forms stages. The sole purpose of this radio fingerprinting is to uniquely distinguish the transmitter being free of any identifier within the information payload that can be produced effectively. This property can be utilized to track cellular phones or other remote gadgets, and to avoid extortion and cell phone cloning.

Three IoT modules are required to enable ubicompatibility: a) Software for installing, executing and implementing methods of communication; b) tools which can be accessed on many technologies and shown for various purposes. This chapter also discusses the several progress which could be defined in some of these sectors throughout the 3 segments. The RFID (RFID) transition is probably the most important improvement in the view of data that validates remote communications mapping of microchips. They help to show indications that embody all the electronic standards of that same profession. The free RFID labels on the battery use the control of the browsing flag by reading the ID to the RFID peruser. In many areas, particularly in the commercial and business administrations. It has been introduced. These applications can be found in moving (tokens replacement, entry tags) and in controlling programming. Unlocked labels have now been used in many bank cards and road toll labels, some of the world's largest organizations.

3.2 Existing Work

Here first for storing and retrieving patients we can utilize biometric mechanism for storing user data. While login user can check by which mechanism his/her can login (Figure 3.1) and its time complexity are more and takes more time for data retrieval process we overcome these challenges in proposed work.

Process approval affirms whether the gadget occasions regions per the predefined system. Plan approval checks whether the gadget activity fulfils the client requires. Information confirmation affirms the information inside the range and according to the information arrangement and information is a current one, not the old chronicle which is known as the leftover information of the instrument data as well.

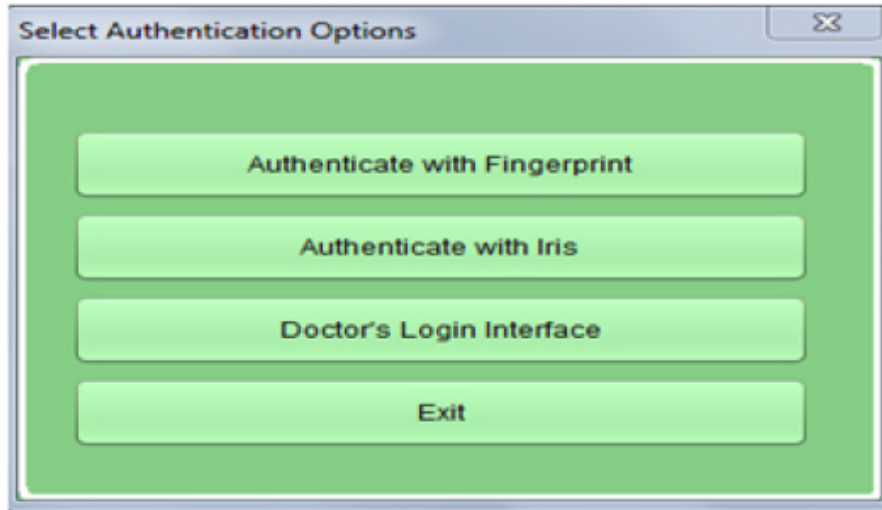


Figure 3.1: Example of user validations

3.3 Proposed Method

We suggest a three-part vision framework to facilitate the investigation of information, clear tools and quiet practices based on the quality of work. Keep in mind that security enhancement advocates are a major issue that will not be explored here.

Here in proposed work we perform the testing by different methodologies and easier process with much more secured manner (Figure 3.2).



Figure 3.2: Medical Data Validations

Process approval affirms whether the gadget occasions are according to the predefined methodology. Outline approval checks whether the gadget activity fulfils the client requires. Information check affirms the information inside the range and according to the information configuration and information is of a current one, not the old chronicle which is known as the lingering information of the instrument. Relationship of Cutting edge medicinal equipments drew from benchmarks for information according to particular, information approval regulations for various IoT powered medical devices as indicated in Figure 3.2.

However, it entails as the therapeutic sensor hubs have limited control storage, memory and contact transmitting rates, security arrangements must be resource-efficient. Therefore, it is difficult to use repetitive cryptography approaches that involve daunting calculations and therapeutic sensor hubs are quickly displaced or stolen as they are tiny in measurements.

We employed DTLS (Datagram Transport Layer Security) handshake convention as it's the IoT's main IP authentication system. Typically the first move towards a safe and efficient verification and approval approach to IoT-based healthcare apps, utilising sound e-health doors, is to provide our knowledge. We explain the approach proposed from the point of view of safety and execution. In order to verify the definition, we also demonstrate our IoT architecture model with a keen door in e-Health and explain the strategy and execution of our model.

3.3.1 Algorithm and Framework

Here in the algorithm we propose the maintenance time, top asymmetry, flag to commotion proportion, the determination between two distinguished pinnacles, the reaction time should support overly analyzed-periods in its life period to affirm exactness. Figure 3.3 shows the proposed algorithm for authentication of IoT based e-Health module. The gadget tests affirm the fundamental execution of gadget though user-based tests affirm the logic layer importance of information in choice help, arrange ability test for affirming the secured correspondence without losing esteem. The client encounter test centres around simple work processes, clear directions, important help messages and simple-basic UIs.

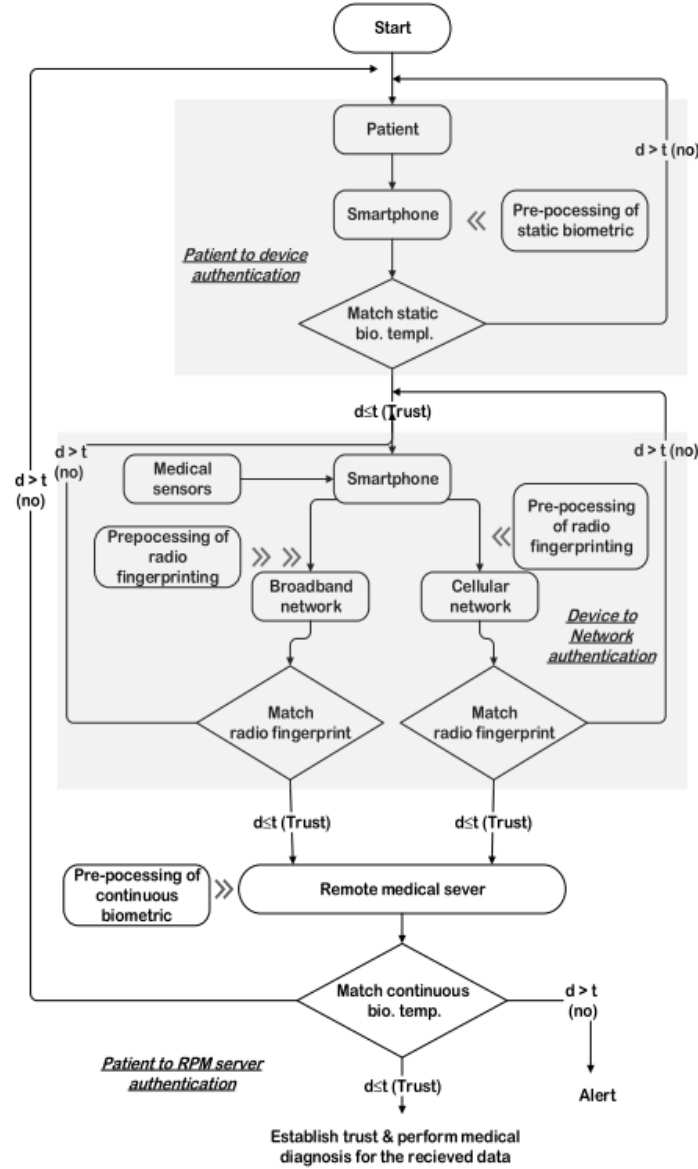


Figure 3.3: Algorithm framework

3.3.2 Proposed Algorithm

The proposed system has four steps.

Step 1: Sensing data: biometric sensors collect the data of blood pressure, body temperature, pulse rate and heart beats.

Step 2: Comparison of data: Collected data are compared with the reference saved data of different parameters. Here four comparators used for four parameters.

Step 3: Analysis: After comparison of the data, all differences send to the microcontroller and microcontroller analysed it and give signal to the frequency generator.

Step 4: Frequency generation: When the sensed data is differed from the reference data, microcontroller send signals one after one for generation of the alarming signal. Frequency generator generates 1.0MHz. frequency for buzzer alarm and 2MHz. for activate auto phone call.

Algorithm 1: Structural decomposition and data validation of data Remanence from IOT medical devices

Input: IOT_MED: Devi= { IOT_MED_Reading.Patient}, I=1.....n

For Every Event of the Device(Devi) \in IOT_MED Do

Begin

 Authenticate Device

 CreateDatabaseConnection(con)

 InsertSmartDataObject(devil)

 ExecuteQuery(con)

 If Devi Triggers transmission Then

 CreateRootNode(Devil)

 Refer Device Definition Business rule from Database(con)

 Add SmartDataObjectTag in EXI XML()

 Get Attribute() and Attribute Value()

 Create EXIXML ChildNode for all attributes()

 Create EHC Record in EXIXML format()

 Normalize the EHC Record() as per standard(con)

 Validate Data for Device(Min.Max Range) from DB(con)

 Check for Datatype Dataformat, CorrectTimestamp

 SemanticAnnotation, from Device Standards Described in DB(con)

 If check or validation fails Then

 Follow the fallback Action as per WorkFlow configuration

 EndIf

 Process the EHC Record (Message Composition, content Categorization, Message Filtering, Data Aggregation, Parsing)

 Analyse the EHC Record for prediction Model, Pattern Definition, Frequency Tracking

 On the Fly Data Transformation (source, target) using Business Rules in DB (con)

 Repackage EHC Record into Target Data Model()

 Identify Network Connection

 Transmit EHC Record in the protocol transmission format

End

3.3.3 Requirements:

- Pulse Measuring sensor
- Wi-Fi module (ESP8266)
- Arduino Uno
- LCD Unit
- Bread Board
- 10k potentiometer
- 1k resistors
- 220-Ohm resistors
- LED
- Connecting wires (Male-Female type)

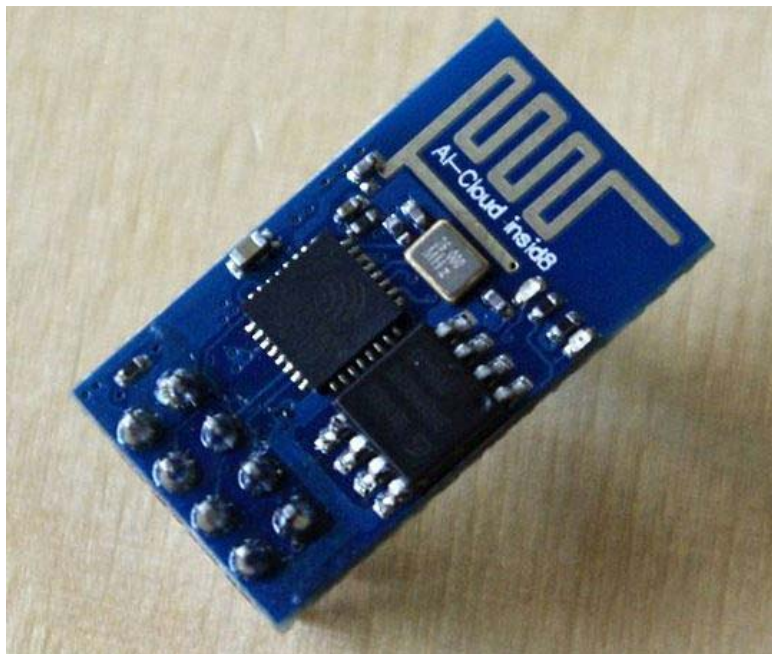


Figure 3.4: ESP8266 Wi-Fi module

ESP8266 Wi-Fi module (Figure 3.4) provides Wi-Fi connectivity to our setup and thereon to Internet. It costs less and highly effective and powerful. It can interface with any microcontroller and is prominently been used over IoT platform.

3.3.4 Architecture of Secure e-Health

Through the figure (Figure 3.5 & Figure 3.6 is) shown the design of a IoT-based health control framework using doors in the home / clinicfield(s). 5. In this context, body-wear or integrated sensors are able to capture the comprehension of health-related data, which facilitates person

conformity with different parameters. Moreover, the data setting (e.g. date, time, area and temperature) can be supplemented with this information to enable you to determine unusual designs and make more accurate inductions almost to the occasion. The emerging system implementation requires the use of primary elements:

- i) Bio-medical and environment impulses via the body as well as position are detected, used to treat and infer restorative conditions through means of the therapeutical sensor arrangement (MSN), activated by pervasive recognition, detection, and communication ability. The flag is then transmitted through remote or wired networking conventions including Serial Peripheral Interface Ethernet, Wi-Fi and IEEE 802.15.4 to the Portal.
- ii) As a point of contact between the MSN and local network switches, Intelligent eHealth Portal embraces a wide range of networking protocols. This collects information from various subnetworks, transforms the convention and provides certain higher departments, such as the aggregation of details, screening and reduction of measurements.
- iii) The Back-End Framework consists of the other modules, a near-by (in-hospitals) switch, a wide-spread cloud services stages, an information stock, huge expository information servers, and a neighbourhood health centre (DB) repository which sympathises with remote medical DB servers.
- iv) The accessibility to patient's well-being information within the cloud technology phase is classified as open (e.g. patient ID or blood sorting) and personal (e.g. DNA) information based on its relevance. The information gathered on well-being and environment refers to an invaluable pool of large data on observable clinical and pharmacological issues (e.g. identification of near infectious diseases).

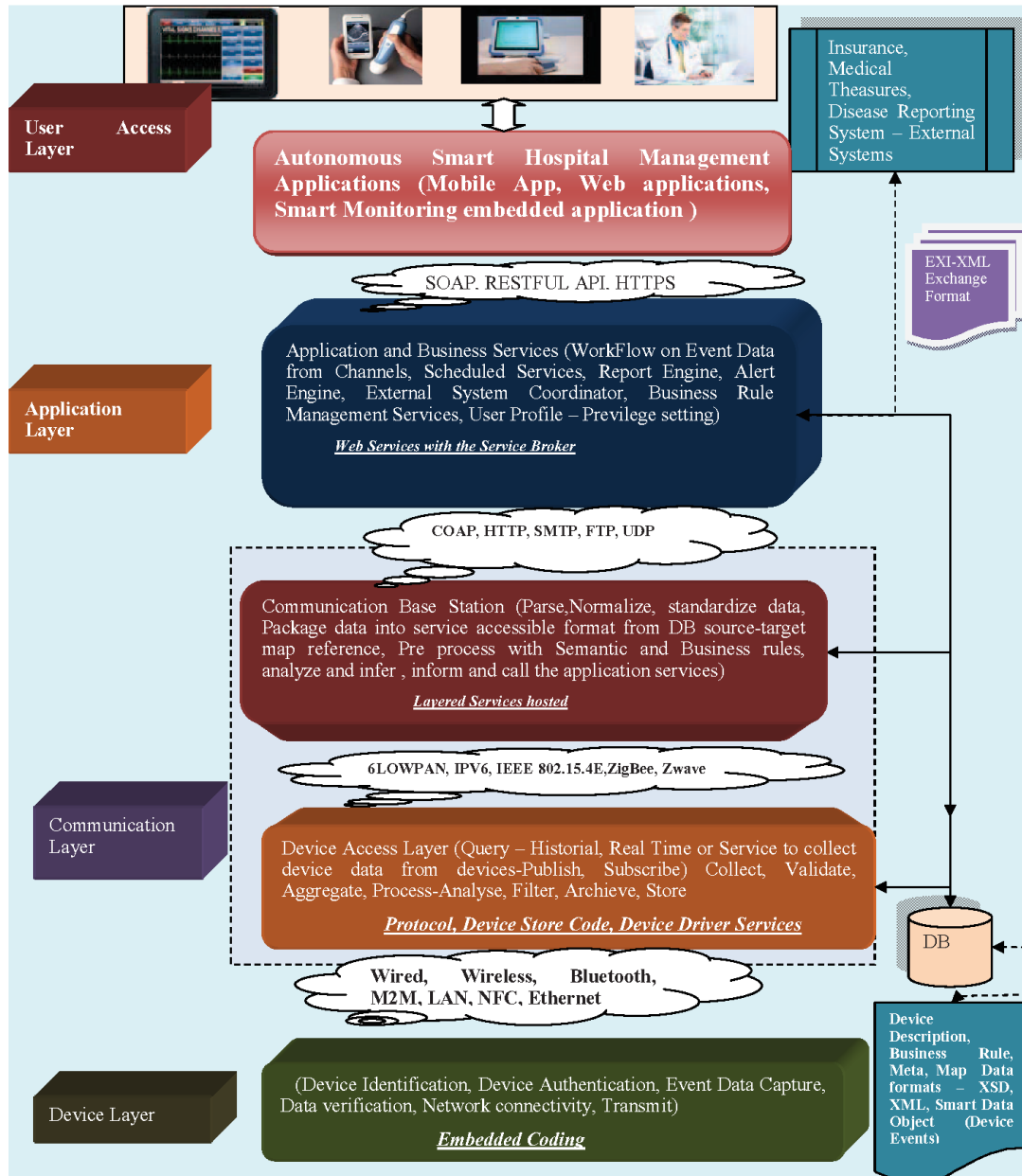


Figure 3.5: Model of Hospital management system (HMS)

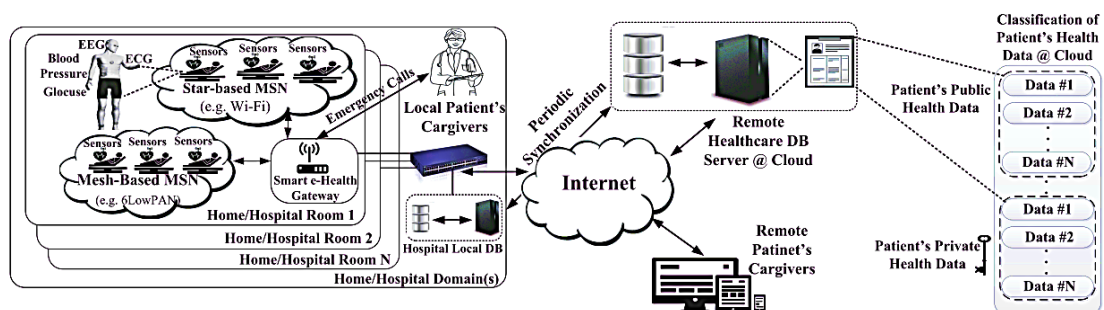


Figure 3.6: Secure e-Health monitoring framework architecture

A. Data Acquisition

Securing of details A number of wearable sensors are used, such as ECG, epidermal temperature, inhale/exhale rate, EMG muscle activity and jog. The functionality of the sensors with that, even though an aggregation site or transmission system in the right of centre personal data, that would be usually a skilled telephone in the patent's aspect, is discovered.

B. Data Transmission components

The elements of the information transmission framework are designed to transmit records of the comprehension in an ideal world in remotely similar real time, from either the patient's house (or from another area) with the Information Center of the Health Care Organization (HCO). A shorter range radios such as Zigbee or Bluetooth radio with the purpose of exchanging sensor information for the storage system is usually delivered for tactile operations.

C. Cloud Processing

Storage, Data analysis and Visualization being the core components of a Cloud Processing system which is being specifically fabricated to store the patient's bio-health information as well assisting health experts by providing diagnostic information (Hani et al., 2014).

- i. Analytics provide the system with the sensor data along with significant records that are becoming widespread and can help with diagnoses and prognoses for a number of health conditions and diseases.
- ii. Presenting the same captured data becomes a crucial task in such systems or else in its absence the voluminous data is just a junk for every user of the system. Visualization methods enables the system to provide the data in an understandable form, ready to digest by the health experts to formulate a diagnosis.

3.4 Data Acquisition and Sensing

Wearable devices that incorporate simpler than anticipated sensors that can calculate numerous physiological parameters, limited preprocess equipment and contact steps, are capable of obtaining biomedical details for the delivery of the observed data. Table 3.1 summarizes numerous

biomarkers which can be calculated using existing or wearable sensors that will soon be available. The suitability for the treatment of 4 types of illness is further shown in the below listed table.

The requirement for wearability is the actual necessity of the sensor devices. The sensors should be powerful, compact and should not prevent the development and mobility of a patient. So much, because they must operate on rechargeable batteries in the lightweight package, the resilience must be strong. Despite being able to refresh or buy a replacement for ease and to insure data-integrity at power-up or battery maintenance cycles, the intensified non-stop circumstances without recharge or substitute are overly enticing.

Table 3.1: Biomarkers that can evaluate existing or upcoming wearable sensors

Bio-marker	CVD	COPD	PD/HD	Diabetes
Gait (posture)	Yes	Yes	Yes	No
ECG	Yes	Yes	Yes	Yes
Respiratory rate	Yes	Yes	Yes	No
Skin temperature	Yes	Yes	Yes	Yes
Surface EMG	Yes	Yes	Yes	No
Sweating	No	No	Yes	No
Blood pressure	Yes	Yes	Yes	Yes
Body movements	Yes	No	Yes	No
Blood Glucose	No	No	No	Yes
Heart Sound	Yes	Yes	No	No
Oxygenation	Yes	Yes	No	No

Title volume	Yes	Yes	Yes	No
---------------------	-----	-----	-----	----

A handshake starts with a letter of ClientHello that integrates the association's protection criteria which is then used to determine the mystery key for the pre-master. Extra ClientHelloVerify cookie is included in flight 3. The communication begins with ServerHello and includes the planned cypher suite for the actual handshake and the unusual value of the sharp gateway used afterwards among the handshake to measure aces mystery key. Figure 3.7 comprises several DTLS handshake messages. The concomitant chip packages rely on the end user's supported system suites.

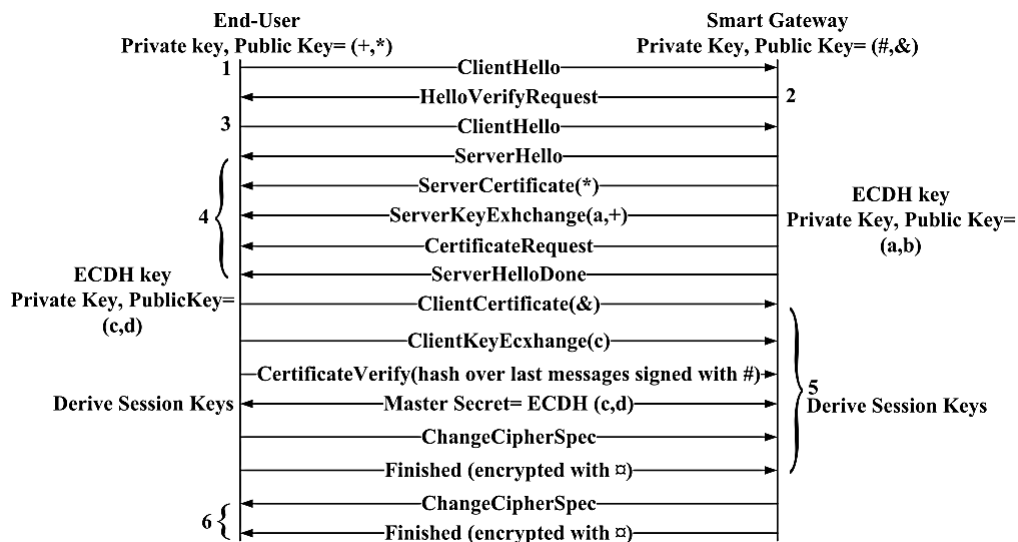


Figure 3.7: DTLS handshake

Should the shrewd website and end users not comply with the same chipset, the handshake shall be cancelled with a warning notification HandshakeFailure. The message below in flight 4 is a long certificate notification comprising the credential chain of the gateway. The first credential within the chain contains a secure key for the experienced gateway that is used as a 1.0.1.j under OpenSSL. With Https, TLS and other cryptographic resources including symmetric key, distributed key, and hash calculations, OpenSSL is open source. It is widely used for the creation and monitoring of keys and certificates. Upon the acceptance of the stamp, the end-user may delete the sensitive open key.

As a mutual handshake the CertificateRequest is sent and comprises of the lists of valid certificates been associated with the smart gateway. Further, along with specific cipher suites the ServerKeyExchange message is sent that requires more parameters so as to compute master secret key. While this being a notable feature, the Cipher suite been implemented in this work is TLS ECDHE ECDSA WITH AES 128 CCM 8 SHA 256 which signifies the use of elliptic cryptography particularly Elliptic Curve Diffie-Hellman (ECDH) and Elliptic Curve Digital Signature Algorithm (ECDSA). Furthermore, for encryption we've used AES-based CCM with an IV of 8. And hence the fabricated cipher suite enables the ServerKeyExchange message to contain the Smart Gateway's ECDH public key and associated elliptic curve details.

Flight 4 messages end with the ServerHelloDone message announcement. After this flight 5 message is initiated using the end-user's certificate just in order to get authenticated under certain circumstances. Using extracted features from the ClientKeyExchange master key is computed. In our case, we transfer the ECDH public key of the smart gateway. While with the use of CertificateVerify message, end-user verifies its identity and authenticates with its private key which corresponds to the public key contained in the certificate.

Thus, transmission occurs with mutual authentication. Prior to the transmission the remote device sends a ChangeCipherSpec message to gateway in order to inform about the start of transmission, and notifying the cipher suites and secret key based encryption of the incoming message. To establish a secure handshake, both the peers needs to be aware of the fact that neither of the flight messages are been hampered with, for that the encrypted hash over all flight messages are been embedded to the Finished messages. Response is been generated by the smart gateway with its own ChangeCipherSpec and Finished messages.

After getting on with the Finished message transmission and successful verification, our primary data containing actual information takes place over the same established connection. As shown in Figure 3.7, during this phase too the authentication process keep on happening between the remote end-point and the system gateway. With the DTLS handshake which is certificate based the gateway authenticates (Auth-req.1) the remote device using certificates.

As seen in modern web browsers, the gateways too has a pool of verified or trust certificates. The authentication between smart gateway (Auth-req.2) and the remote end-point is to be done using certificates and that too within the certificate-based DTLS handshake or by creating a password

from a specific application, as soon as the handshake ends. Our aim was primarily is to restrict the verification process at the sensing device level itself, which is been worn by the user.

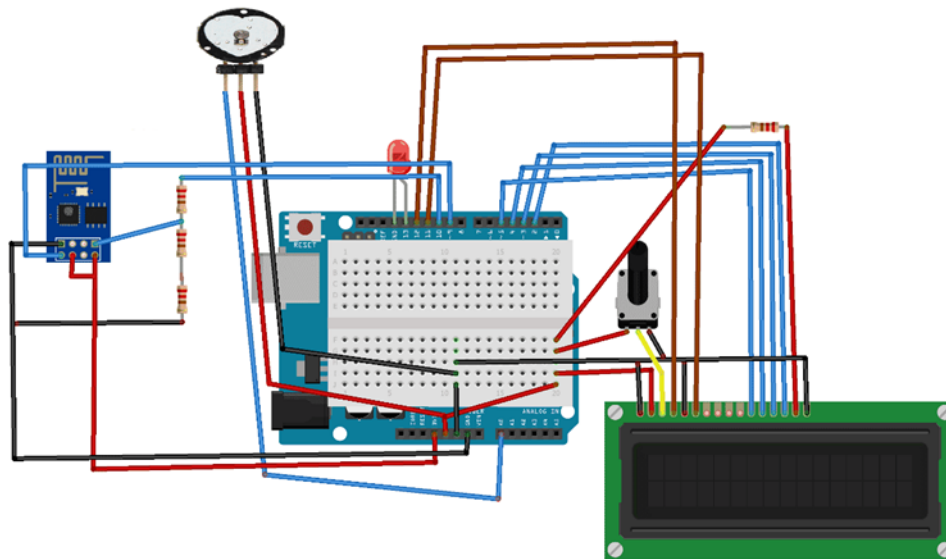


Figure 3.8: Circuitry of the model

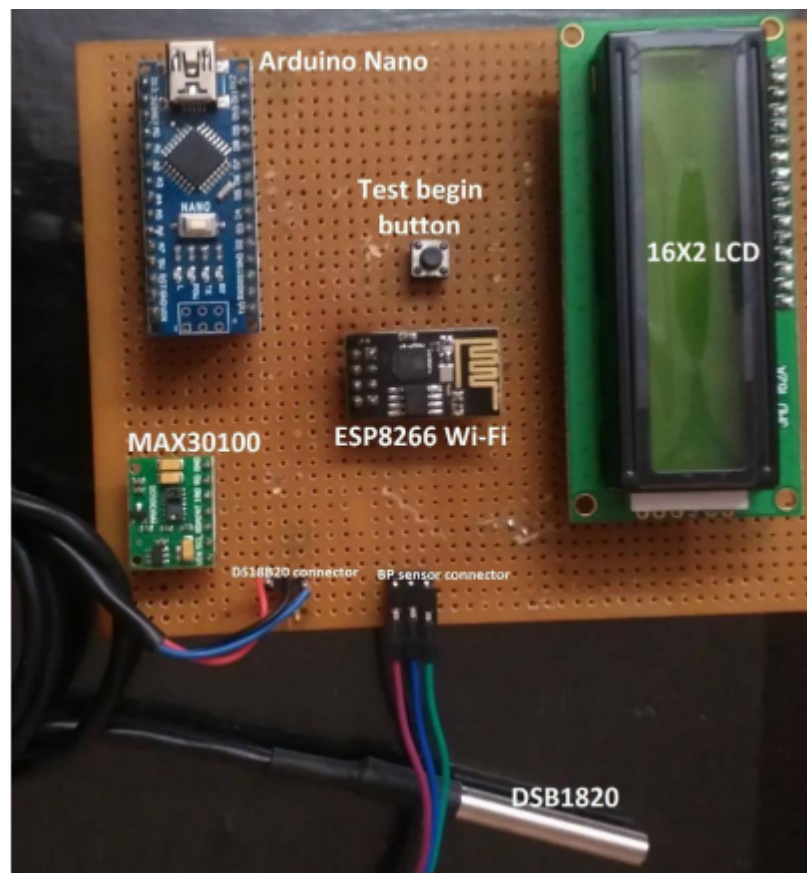


Figure 3.9: Experimental Setup

The network being used here maintains a interface allowing data transfer between invasive/implanted sensors and base station. Secondly the same network allows a coordinator to communicate with the sensor as well. Now, our BSN-Care (shown in Figure 3.8 and Figure 3.9) is a BSN architecture which comprises of wearable and implantable sensors. Bio-sensors such as Electrocardiogram (ECG), Blood Pressure (BP) etc. is being associated with each sensor node.

The sensors continuously keep on monitoring vitals and forward them to the coordinator also known as the Local Processing Unit (LPU), which can be a smartphone too. The LPU is responsible to route the data collected from the sensors to the main server, using wireless medium i.e. mobile networks. Apart from this, in case any adversary is detected, immediate alert is being sent to the patient itself.

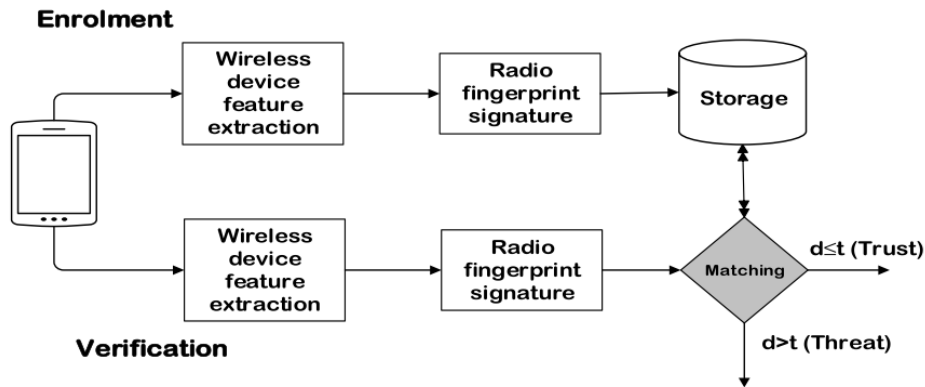


Figure 3.10: Authentication through radio fingerprint for PDA device

3.5 Device to Network Authentication

The phases associated during authentication are enrolment and verification. To create a radio fingerprint of smartphone for validation the features are extracted for enrolment purpose. Same gets stored at a secured location for future mapping and comparison. The secured location could be a wireless access point. Further, when a device requests for the access of medical server, first the stored radio fingerprint is verified against the requested one at the wireless AP or at the operator end. On a successful match the connection will be established but the request will be blocked in case of a wrong match. In our proposal we assumed that only successful matches will be allowed to pass through traffic. Mobile network till date does not provide any such service.

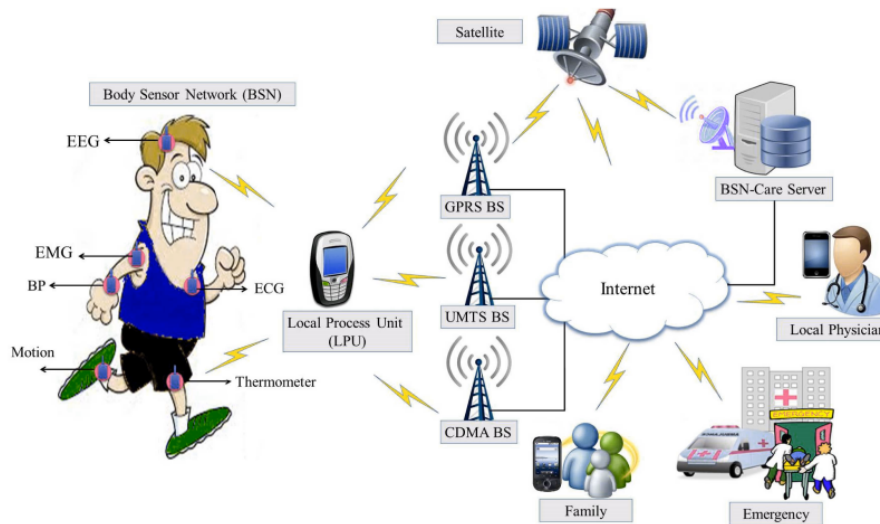


Figure 3.11: Schema of BSN care network

At the server when data is received from LPU, same gets stored in database for further analysis and trend judgement. In case any abnormalities are observed further processing may include communication with family, local physician assigned, or nearby emergency unit. Here we've assumed that the patient is wearing the sensor and its connected to the LPU, failing this the process could be delayed.

3.6 Implementation

The experiment and its implementation was carried out through MATLAB's ThingSpeak website after login it provides various options for channel creation and device connectivity. This is later followed by code implementation for data visualizations (see Figure 3.12 through Figure 3.14).

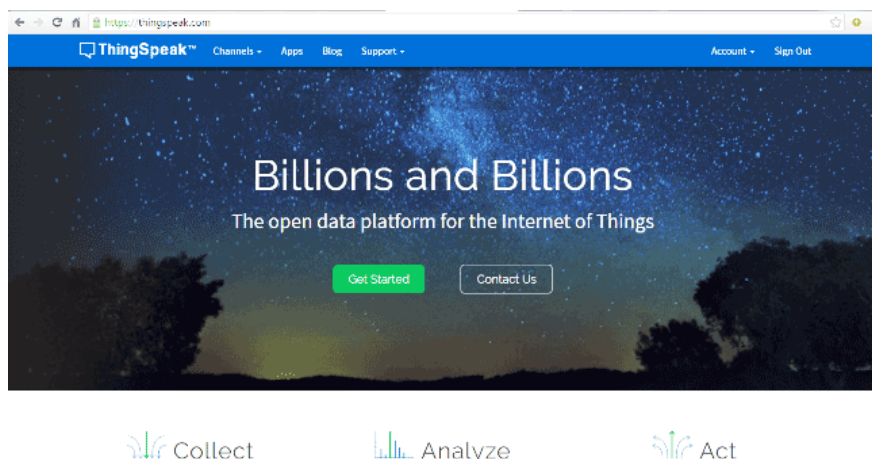
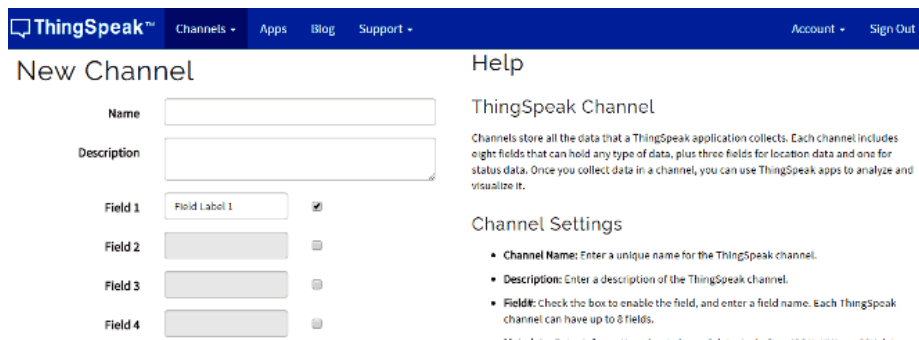


Figure 3.12: ThingSpeak™ web page



ThingSpeak™ Channels Apps Blog Support Account Sign Out

New Channel

Name

Description

Field 1 ☒

Field 2 ☐

Field 3 ☐

Field 4 ☐

Help

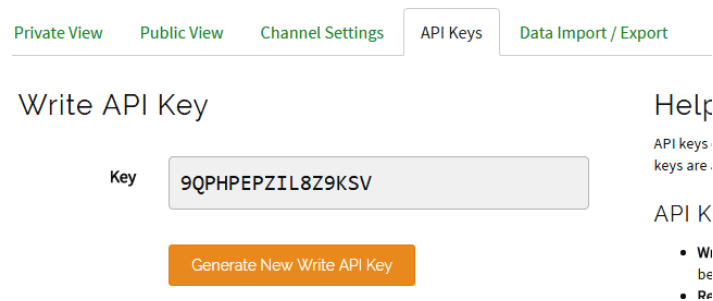
ThingSpeak Channel

Channels store all the data that a ThingSpeak application collects. Each channel includes eight fields that can hold any type of data, plus three fields for location data and one for status data. Once you collect data in a channel, you can use ThingSpeak apps to analyze and visualize it.

Channel Settings

- **Channel Name:** Enter a unique name for the ThingSpeak channel.
- **Description:** Enter a description of the ThingSpeak channel.
- **Field#:** Check the box to enable the field, and enter a field name. Each ThingSpeak channel can have up to 8 fields.

Figure 3.13: Creating channel on ThingSpeak site



Private View Public View Channel Settings API Keys Data Import / Export

Write API Key

Key

[Generate New Write API Key](#)

Help

API keys

API keys are used to authenticate devices.

API K

- Wi be

Figure 3.14: Device connectivity through API key

Chapter 4

EXPERIMENTAL RESULTS

From the workflow the pulse sensor is been attached to the patient then it senses the pulse rate and records it and then referring to the association rules it looks for the other symptoms with the high or low pulse rate for example if patient has high pulse rate then it checks for symptom like body temperature, then by using this system we get direct predictions like chances of high blood pressure, heart and lung diseases, stress or any other related disease (Figure 4.1). While executing, we ought to establish our own channels and corresponding field representation too.



Figure 4.1: Sample output

The occasion triggers the call of alert administrations arranged according to the work process. For instance, the caution ought to be sent just to the "Basic Care" benefit bought in specialists of the unit and not to all. On the off chance that the alert move isn't made, the healing centre administration framework ought to have the acceleration lattice as a major aspect of the work flow. In the doctor's facility administration framework, the occasion driven process stream is clarified in the accompanying Figures with the occasion esteem.

The data gets represented in the form of a graph and which shows the variation as per different timelines. Field 1 comprises of heart rate, while field 2 contains the average value for readings in a week. Health parameter and date are been represented respectively by Y and X-axis. Figure 4.2 through Figure 4.4 shows the recorded plots against time and date and provides specific data when we hover cursor above those plotted values.

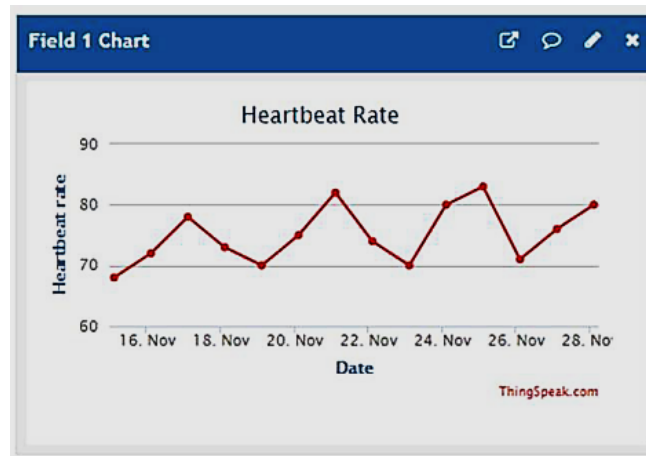


Figure 4.2: Heart-rate and date values

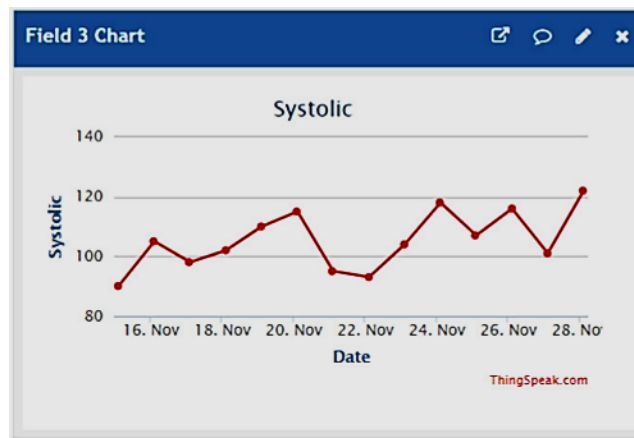


Figure 4.3: Systolic pressure

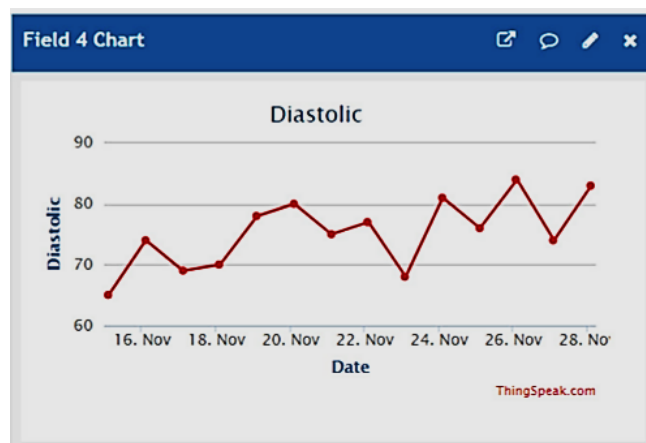


Figure 4.4: Diastolic Pressure

Field 3 and 4 represents systolic and diastolic values respectively (Figure 4.3 and Figure 4.4). In the same way, blood pressure levels were captured and been saved for a span of two weeks. Figure 4.4 shows the representation of captured blood pressure levels(diastolic).

4.1 Action Responses

Table 4.2: Parameters for response action

Captured BP Data	Corrective Measure	Response
BP \leq 120	No Action	Null
BP>130	Inform Family Members	FR:T/F
BP>160 and FR:F	Inform Local Physician	PR:T/F
BP >160, FR:F and PR:F	Inform Emergency	ER:T/F
FR:Family Response; PR:Physician Response; ER:Emergency Response		

Above Table (Table 4.1) denotes the corrective measure been to be taken based on the data received from BP sensor, where we can see that if the blood pressure is less than or equal to 120 then the server need not have to perform any action. In extreme case, if the blood pressure level rises beyond 130 point, an information broadcast will be sent to the relevant family member. Further in case the reading crosses 145-mark, system will generate an alarm and will intimate the emergency to assigned physician in case no response is received by the alerted family member. Whilst the system crosses 160, without getting responses from intimated persons till that time, nearest health centre will be contacted for emergency handling furnishing the location of the user. Figure 4.5 shows alert messages sent to the target individual.

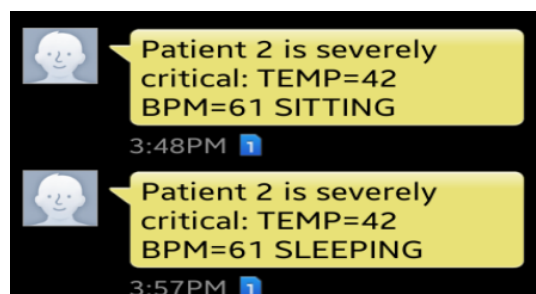


Figure 4.5: Alert messages sent to the phone

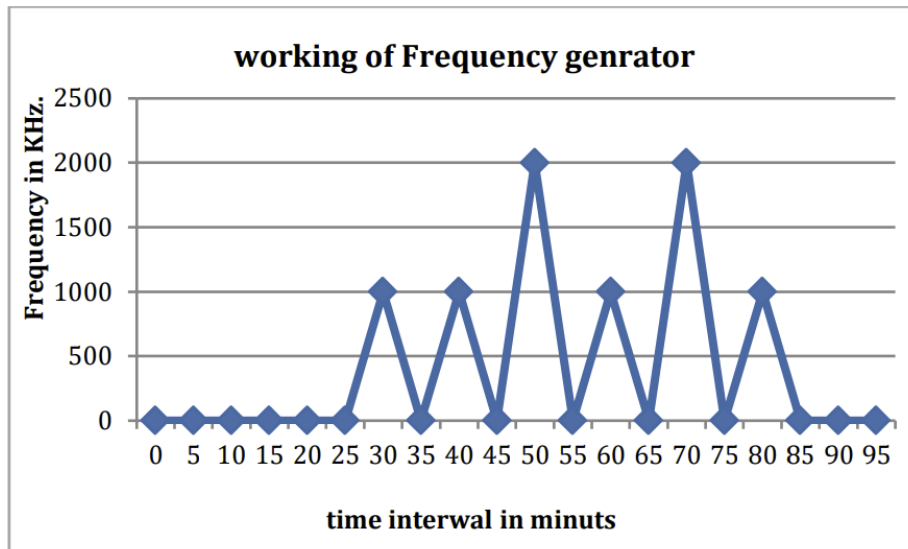


Figure 4.6: Frequency generation

A Frequency generator activated when the difference of the comparator is more or less than the reference limit of the parameters. When the difference values of the comparators for the parameters had crossed lower or upper limit then microcontroller did not activate the frequency generator (Figure 4.6). It waited for the next value; if next values also perform the same character then microcontroller activated the frequency generator for the generation of 1 MHz. frequency to activate pizzo-electric buzzer alarm.

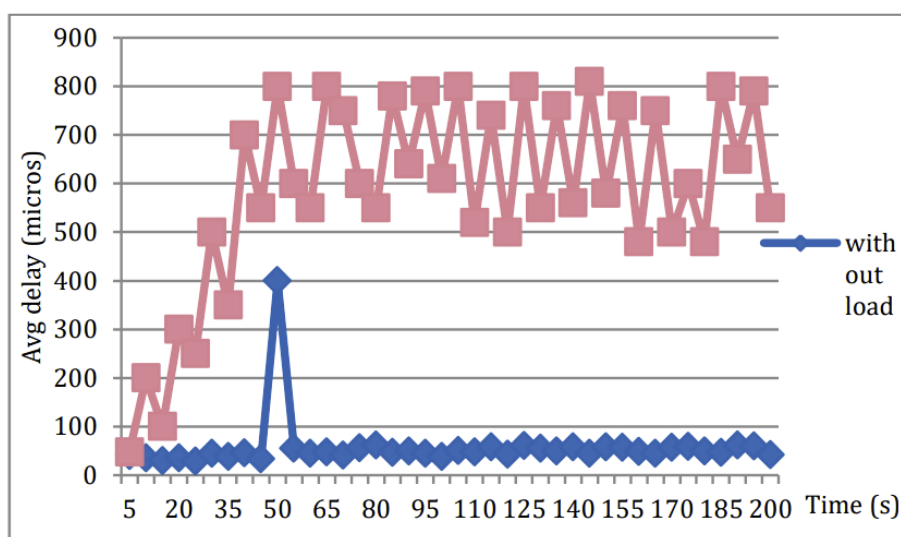


Figure 4.7: Throughput comparison

Figure 4.7 shows that the proposed IoT based healthcare system gives better throughput compared to existing method and speed of transmission will be high in this method. Due to implementation IoT and Intelligent E-health gateway process it has increased the speed of data transfer due to data compression and fusion process.

Chapter 5

CONCLUSION AND FUTURE WORK

5.1 Conclusion

This thesis was focussed on the design and mechanism along with the methodology for IoT empowered independent intelligence clinic administration framework with the accompanying innovative ways, gadget recognition, information analysis & representation, inter-operability, information mapping and change, information approval and filtration, process flow setup for event driven work flows, engineering, and foundation choice points of interest.

Our proposed authentication framework comprises of three phases: it validates and verifies that the received data at remote medical server are legit and correct, also identifies alterations. The framework is in itself resource and energy efficient as it does not requires processing overhead for authentication purpose except for the initial pre-processing of biometric and radio fingerprinting templates. In case of any emergency for e.g. a heart attack or other extraordinary medical situation found while remotely examining a patient, the location can be determined using smartphone radio fingerprints.

Basic limitation of using gadgets based architecture is their limited power which needs to be addressed or can be handled by substituted batteries being managed by some sort of administrative system. As per quality experts recommendation a proper check or routine for analysing gadget working standards should be applied. Apart from the above task, other regular and redundant activities like lab management, outpatient examination, room assignment, staff management and other inter-departmental tasks are been put under future plan of this work, so as to make this system work to its full potential. Moreover, the information been generated by this system would be huge as one can imagine, for the same we'd be needing cloud system as well.

5.2 Future Work

The intelligence of clinic administration framework examined to enable the healing centre expert to interface a medicinal gadget, characterize the information display, characterize the information mapping positions, characterize the procedure or work process. There is an office to interface with

coordinate with the current and the outer framework with the best possible source-goal information mapper. There is an office of characterizing the level1 information organize, level2 information designs cling to the medicinal record groups. The healing center experts can without much of a stretch characterize the work process and process stream with the standards and approvals required. The part and validation instruments are configurable. The framework accessible itself distinguishable and also configurable. The shrewd healing facility, computerized cautions, making reports to the goal gather designed to analyse and follow up on require.

REFERENCES

- [1] Gope, P., & Hwang, T. (2015). BSN-Care: A secure IoT-based modern healthcare system using body sensor network. *IEEE Sensors Journal*, 16(5), 1368-1376.
- [2] Jain, A. K., Nandakumar, K., & Ross, A. (2016). 50 years of biometric research: Accomplishments, challenges, and opportunities. *Pattern Recognition Letters*, 79, 80-105.
- [3] Jain, A. K., Ross, A., & Pankanti, S. (2006). Biometrics: a tool for information security. *IEEE transactions on information forensics and security*, 1(2), 125-143.
- [4] Wortmann, F., & Flüchter, K. (2015). Internet of things. *Business & Information Systems Engineering*, 57(3), 221-224.
- [5] Niranjana, S., & Balamurugan, A. (2015). Intelligent E-Health Gateway Based Ubiquitous Healthcare Systems in Internet of Things. *International Journal of Scientific Engineering and Applied Science (IJSEAS)-Volume-I, Issue-9*.
- [6] Rahmani, A. M., Thanigaivelan, N. K., Gia, T. N., Granados, J., Negash, B., Liljeberg, P., & Tenhunen, H. (2015, January). Smart e-health gateway: Bringing intelligence to internet-of-things based ubiquitous healthcare systems. In *2015 12th Annual IEEE Consumer Communications and Networking Conference (CCNC)* (pp. 826-834). IEEE.
- [7] Bardyn, J. P., Melly, T., Seller, O., & Sornin, N. (2016, September). IoT: The era of LPWAN is starting now. In *ESSCIRC Conference 2016: 42nd European Solid-State Circuits Conference* (pp. 25-30). IEEE.
- [8] Gia, T. N., Thanigaivelan, N. K., Rahmani, A. M., Westerlund, T., Liljeberg, P., & Tenhunen, H. (2014, October). Customizing 6LoWPAN networks towards Internet-of-Things based ubiquitous healthcare systems. In *2014 NORCHIP* (pp. 1-6). IEEE.
- [9] Satija, U., Ramkumar, B., & Manikandan, M. S. (2017). Real-time signal quality-aware ECG telemetry system for IoT-based health care monitoring. *IEEE Internet of Things Journal*, 4(3), 815-823.
- [10] Chiuchisan, I., Costin, H. N., & Geman, O. (2014, October). Adopting the internet of things technologies in health care systems. In *2014 International Conference and Exposition on Electrical and Power Engineering (EPE)* (pp. 532-535). IEEE.

- [11] Rahmani, A. M., Thanigaivelan, N. K., Gia, T. N., Granados, J., Negash, B., Liljeberg, P., & Tenhunen, H. (2015, January). Smart e-health gateway: Bringing intelligence to internet-of-things based ubiquitous healthcare systems. In 2015 12th Annual IEEE Consumer Communications and Networking Conference (CCNC) (pp. 826-834). IEEE.
- [12] Wayman, J. L. (2001). Fundamentals of biometric authentication technologies. *International Journal of Image and Graphics*, 1(01), 93-113.
- [13] Galbally, J., Marcel, S., & Fierrez, J. (2014). Biometric antispoofing methods: A survey in face recognition. *IEEE Access*, 2, 1530-1552.
- [14] Hiremath, S., Yang, G., & Mankodiya, K. (2014, November). Wearable Internet of Things: Concept, architectural components and promises for person-centered healthcare. In 2014 4th International Conference on Wireless Mobile Communication and Healthcare-Transforming Healthcare Through Innovations in Mobile and Wireless Technologies (MOBIHEALTH) (pp. 304-307). IEEE.
- [15] Haghi, M., Thurow, K., & Stoll, R. (2017). Wearable devices in medical internet of things: scientific research and commercially available devices. *Healthcare informatics research*, 23(1), 4-15.
- [16] Bao, S. D., Zhang, Y. T., & Shen, L. F. (2006, January). Physiological signal-based entity authentication for body area sensor networks and mobile healthcare systems. In 2005 IEEE Engineering in Medicine and Biology 27th Annual Conference (pp. 2455-2458). IEEE.
- [17] Chowdhury, M. A., Light, J., & McIver, W. (2010, December). A framework for continuous authentication in ubiquitous environments. In 2010 Sixth International conference on Wireless Communication and Sensor Networks (pp. 1-6). IEEE.
- [18] Fatemian, S. Z., & Hatzinakos, D. (2009, July). A new ECG feature extractor for biometric recognition. In 2009 16th international conference on digital signal processing (pp. 1-6). IEEE.
- [19] Horrow, S., & Sardana, A. (2012, August). Identity management framework for cloud based internet of things. In *Proceedings of the First International Conference on Security of Internet of Things* (pp. 200-203). ACM.

- [20]Sidek, K. A., Khalil, I., & Smolen, M. (2012, September). ECG biometric recognition in different physiological conditions using robust normalized QRS complexes. In 2012 Computing in Cardiology (pp. 97-100). IEEE.
- [21]Odinaka, I., Lai, P. H., Kaplan, A. D., O'Sullivan, J. A., Sirevaag, E. J., & Rohrbaugh, J. W. (2012). ECG biometric recognition: A comparative analysis. *IEEE Transactions on Information Forensics and Security*, 7(6), 1812-1824.
- [22]Poree, F., Kervio, G., & Carrault, G. (2016). ECG biometric analysis in different physiological recording conditions. *Signal, image and video processing*, 10(2), 267-276.
- [23]Srivastava, H. (2013). Personal Identification Using Iris Recognition System, a Review. *International Journal of Engineering Research and Applications (IJERA)*, 3(3), 449-453.
- [24]Silva, H., Lourenço, A., Fred, A., & Filipe, J. (2011, November). Clinical data privacy and customization via biometrics based on ECG signals. In *Symposium of the Austrian HCI and Usability Engineering Group* (pp. 121-132). Springer, Berlin, Heidelberg.
- [25]Mohan, A., Bauer, D., Blough, D. M., Ahamad, M., Bamba, B., Krishnan, R., ... & Palanisamy, B. (2009). A patient-centric, attribute-based, source-verifiable framework for health record sharing. Georgia Institute of Technology.
- [26]Dube, S., Ndlovu, S., Nyathi, T., & Sibanda, K. (2015). QR code based patient medical health records transmission: Zimbabwean case. In *Proceedings of informing science & IT education conference (InSITE)* (pp. 521-520).
- [27]Brandt, R. A. (2015). Identifying stakeholder incompatibilities mitigating the integration of US patient-controlled personal health records (Doctoral dissertation).
- [28]Mohammed, J., Lung, C. H., Ocneanu, A., Thakral, A., Jones, C., & Adler, A. (2014, September). Internet of things: Remote patient monitoring using web services and cloud computing. In 2014 IEEE International Conference on Internet of Things (iThings), and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) (pp. 256-263). IEEE.
- [29]Sunyaev, A. (2013). Evaluation of Microsoft HealthVault and Google Health personal health records. *Health and Technology*, 3(1), 3-10.

- [30] Tyagi, S., Agarwal, A., & Maheshwari, P. (2016, January). A conceptual framework for IoT-based healthcare system using cloud computing. In 2016 6th International Conference-Cloud System and Big Data Engineering (Confluence) (pp. 503-507). IEEE.
- [31] Gomez, J., Oviedo, B., & Zhuma, E. (2016). Patient monitoring system based on internet of things. *Procedia Computer Science*, 83, 90-97.
- [32] Khoi, N. M., Saguna, S., Mitra, K., & Åhlund, C. (2015, October). Irehmo: an efficient iot-based remote health monitoring system for smart regions. In 2015 17th International Conference on E-health Networking, Application & Services (HealthCom) (pp. 563-568). IEEE.
- [33] Kitson, N. A. (2011). A convergence of cultures and strategies to improve Electronic Health Record implementation within a Tanzanian clinical environment.
- [34] Babu, S., Chandini, M., Lavanya, P., Ganapathy, K., & Vaidehi, V. (2013, July). Cloud-enabled remote health monitoring system. In 2013 International Conference on Recent Trends in Information Technology (ICRTIT) (pp. 702-707). IEEE.
- [35] Dias, D., & Paulo Silva Cunha, J. (2018). Wearable health devices—vital sign monitoring, systems and technologies. *Sensors*, 18(8), 2414.
- [36] Mainetti, L., Patrono, L., Secco, A., & Sergi, I. (2016, July). An IoT-aware AAL system for elderly people. In 2016 International Multidisciplinary Conference on Computer and Energy Science (SpliTech) (pp. 1-6). IEEE.
- [37] Verma, P., & Sood, S. K. (2018). Fog assisted-IoT enabled patient health monitoring in smart homes. *IEEE Internet of Things Journal*, 5(3), 1789-1796.
- [38] Hani, A. F. M., Paputungan, I. V., Hassan, M. F., Asirvadam, V. S., & Daharus, M. (2014, June). Development of private cloud storage for medical image research data. In 2014 International Conference on Computer and Information Sciences (ICCOINS) (pp. 1-6). IEEE.