CHAPTER 1
INTRODUCTION

1.1 GENERAL BACKGROUND

Health is a dynamic process which needs to be continuously monitored. Health sectors have been facing various hospital admission problems due to higher rate of patient admission to hospital. To this aim, a system is proposed for human health care. The system provides regular monitoring of patient's metabolic parameters and disease detection using the parametric values obtained. Due to increase in number of sudden deaths caused by chronic heart failure or high blood pressure, it is necessary to provide continuous health monitoring service at home. The prime goal was to develop a reliable patient monitoring system so that the healthcare professionals can monitor the patients, who are either hospitalized or executing their normal daily life activities. Recently, the patient monitoring systems is one of the major advancements because of its improved technology. In our system we are measuring patient's parameters (ECG, temperature, heart rate, pulse, etc) different available sensors. This sensor collected data i.e. biometric information is given to node mcu and then it is transferred to server.

Today, the IoT has become one of the most promising communication paradigms, and one in which all the smart objects in our daily life become part of the Internet owing to their communication and computing capabilities. This opportunity brings with its new security challenges for IoT applications. Every smart object (or sensor) in the IoT represents a potential risk in terms of system vulnerability. That is, each intelligent object may become a vulnerable entry point for any malicious attack. Two security issues, i.e. (1) physical protection for smart objects, and (2) how to maintain data confidentiality, integrity and privacy during data collection among smart objects, have thus emerged. Given the novelty and innovative nature of IoT technologies, there seems to be a general expectation for a new and revolutionary security solution tailored specifically to IoT-based objects. This is because traditional security protection mechanisms may not be suitable for smart objects. For example, firewalls containing network management control protocols are able to manage high-level traffic through the Internet. However, this application-level solution is not suitable for endpoint devices in IoT applications because these devices usually possess a specific, defined mission with limited resources available to accomplish it. Therefore, the refinement of traditional security solutions

to fit the specific security requirements of IoT-based smart objects is one of the most promising ways of securing IoT-based application systems.

In the present-day scenario, we find a large no of elderly people staying alone in flats or at isolated places. Recent research indicates that about 80% of aged people above the age of 65 are suffering from at least one life style or chronic disease. This causes many elderly people difficulties in taking care of themselves. Hence it is apparent to provide a decent quality of timely healthcare services to the elderly who are affected. The rapid advancement of IT and communication is making it possible to provide innovative modern healthcare solution instantly. Now IOT enables to extend the concept to the internet and make it more efficient and feasible. IOT allows seamless interactions around different types of devices such as medical sensors, monitoring cameras, home appliances and so on. In healthcare system IOT involves many kinds of cheap sensors that enables aged people to enjoy modern healthcare services anywhere any time and thus improving quality of the life of aged people. To give a brief about my proposed project, it consists of wrist band worn by patient on wrist with temperature sensor and NODE MCU. Temperature sensor LM-35 is embedded in the wrist band itself. whereas oxygen level, heart beat and pulse rate are measured by sensors clipped on to a fingertip and connected to the node mcu by a wire. C++ embedded code will then be uploaded to node mcu using android application. There after the data base is fed to the cloud server from where it is further transmitted to the doctor, family, friends and emergency who take appropriate action to save the life of the patient.

In the future development of technology IoT has a profound influence. In addition, with the development low power embedded technology, sensor technology is widely used. System provides real time health monitoring as well as disease prediction over the internet. It can work base on synthetic as well as real time training data. Accuracy of prediction is good than other learning approaches. System also having a capability to provide the alert when any criticalness 24*7. For Future studies to implement a such systems with parallel processing with high dimensional data using Hadoop or cloud environment.

1.2 ABOUT THE PROJECT

In the modern health care environment, the usage of IoT technologies brings convenience of physicians and patients, since they are applied to various medical areas. The body sensor network (BSN) technology is one of the core technologies of IoT developments in healthcare system, where a patient can be monitored using a collection of tiny-powered and lightweight wireless sensor nodes. However, the development of this new technology in healthcare applications without considering security makes patient privacy vulnerable. At first, we highlight the major security requirements in BSN-based modern healthcare system. Subsequently, we propose a secure IoT-based healthcare system using BSN, called BSN-Care, which can efficiently accomplish those requirements. The body sensor network (BSN) technology is one of the most imperative technologies used in IoT-based modern healthcare system. It is basically a collection of low-power and lightweight wireless sensor nodes that are used to monitor the human body functions and surrounding environment. Since BSN nodes are used to collect sensitive (life-critical) information and may operate in hostile environments, accordingly, they require strict security mechanisms to prevent malicious interaction with the system. it basically employs low power, lightweight sensor nodes which monitor temperature, heart rate, pulse and oxygen level. Since sensors are required to collect sensitive information of the patient, proper care is taken to ensure proper security measures. Blynk server ensures timely passing of patient correct medical status to the concerned Doctor, emergency and family and friends on real time.

1.3 OBJECTIVE AND SCOPE

IOT based modern healthcare system is primarily intended to take care of the health aspects of older people staying alone. The system is envisaged to real time monitoring of the health parameters of dependent patients and provide timely and quality healthcare to them. This will help them abundantly in ageing gracefully with all possible and timely healthcare which is affordable and fully secured. When fully implemented IOT based BSN-CARE will revolutionize the healthcare all over the world.

Objective of the project is to make affordable, fully secure and timely healthcare to the elderly. The system make use of the body sensor networks which with the help of various body sensors measures the health parameters of the patient on real time. Node mcu worn by patient consolidates the readings and pass it on to blynk server an android application and then through mobile network. The information is passed to the cloud server of the medical team on real time. The medical team then take appropriate action to save the patient.

1.4LIMITATIONS

- Due to lockdown and closing of shops and traffic, greater effort had to be put in to obtain components.
- Due to lockdown, we lost lot of valuable classes and guidance by the experienced lectures at the institution.
- On line classes cannot fully compensate for class room instructions and demonstration by experts.
- Wearable IOT devices have greater demand in the market these days due to availability of affordable internet everywhere.

CHAPTER 2

LITERATURE SURVEY

2.1 STUDY OF SIMILAR WORK

A. THE CURRENT STATE OF THE ART OF IOT SECURITY

In recent years, both industry and academia have devoted considerable attention to the development of IoT applications and related security measures. In 2013, Yao et al. [7] presented a lightweight multicast authentication scheme for small-scale IoT applications. They exploited the specific characteristics of the fast accumulator proposed by Nyberg [8], i.e. the absorbency property and the one-way and quasi-communicative property, to construct a lightweight multicast authentication mechanism. To test their scheme's practicability, the authors evaluated seven principal criteria required by multicast authentications for resource constrained applications in the course of a performance analysis. The proposed scheme was claimed to be more efficient and effective than other systems it was compared to. The following year, Bello and Zeadally [9] investigated the possibility of self-collaborated device-to-device communications without any centralized control. Two challenges, namely the computation cost of smart objects and network heterogeneity, were identified. After that, the authors analysed the state of-the-art of communication mechanisms in licensed and unlicensed spectra and routing techniques which are able to support intelligent inter-devices communications. In the course of their analysis, four unresolved issues were identified: 1) maximizing the use of available network resources; 2) route management optimization; 3) inter-device-based cooperation for load balancing; and 4) security properties such as privacy, authentication, integrity and resistance to new types of attack. Later, Cai et al. [10] adopted 802.11 based sensors to construct an IoT-based device management system with a centralized control mechanism. The principal technique was based on the IETF Constrained Application Protocol (CoAP). To evaluate the scheme's feasibility and

effectiveness, the authors implemented an experimental system consisting of an 802.11 enabled sensor, a self-designed management server and an IoT application. The experimental results showed that their proposed system is practicable. However, one limitation exists as the system scalability cannot be guaranteed.

In 2014, Keoh et al. [5] presented an overview of the security solutions for IoT ecosystems proposed by the Internet Engineering Task Force (IETF), in which CoAP and, in particular, Datagram Transport Layer Security (DTLS) are examined. Based on their performance evaluation, these authors developed a refined and lightweight DTLS capable of providing robust security functionality for IoT objects. Even so, the authors identified some unresolved issues for future work, i.e. device bootstrapping, key management, authorization, privacy and message fragmentation issues in IoT networks. Next, in 2015, Kawamoto et al. [11] demonstrated an effective data collection scheme for location-based authentication in IoT networks. In order to improve the authentication accuracy, parameters related to network control are adjusted dynamically based on the real-time requirements from the system and the surrounding network environment. In addition, optimization of authentication accuracy was investigated. The authors finally suggested that future work could focus on intelligently controlling the data distribution from inhomogeneous IoT devices. In the same year, Cirani et al. [12] introduced an authorization framework which is integrated with HTTP/CoAP services and is even able to invoke an external OAuth (Open Authorization) based service. In the proposed framework, an external client may access a remote service from a network broker (with constrained smart objects) via HTTP/CoAP. Robust communication among entities such as an external client, a network broker and smart objects was thus designed and implemented. VOLUME 4, 2016 10289 K.-H. Yeh: Secure IoT-Based Healthcare System with Body Sensor Networks Performance evaluations were performed to examine the feasibility of the proposed framework, with results showing that the proposed approach will increase the amount of energy consumed to ensure compatibility with IEEE 802.15.4. In addition, the issues of memory footprint and dynamic configuration make the OAuth logic-based scheme infeasible for use with common smart objects.

In 2015, Ning et al. [13] proposed an aggregated proof based hierarchical authentication scheme for layered U2IoT architecture to pursue security protection among ubiquitous things. In the proposed scheme, security properties such as entity anonymity, mutual authentication and hierarchical access control are achieved via the following techniques:

user authorization, aggregated-proof based verifications, homomorphism functions and Chebyshev chaotic maps. Later, Hernández-Ramos et al. [14] developed a series of lightweight authentication and authorization procedures which are compliant with the Architectural Reference Model (ARM) from the EU FP7 IoT-A project, for use on constrained smart objects. The proposed schemes are able to be combined with other standard technologies and form security plans for the life cycle of IoT devices. Recently, Gope and Hwang introduced two authentication schemes, i.e. BSN-Care [1] and USM-IoT [2], for IoT-based networks. These two authentication schemes are designed to fit the security requirements for body sensor networks and distributed wireless sensor networks, respectively. Accordingly, from the standpoint of authentication analysis, the underlying architectures can respectively be characterized as being client-server and client-server-server. In 2015, Gope and Hwang [2] first presented an authentication protocol for distributed wireless sensor networks. Their proposal not only is compatible with client-server-server (i.e. the sensor-gateway-server) architecture, but also satisfies important security properties such as mutual authentication, sensor anonymity and un-traceability, system scalability, and resistance to impersonation attack, replay attack and cloning attack. The authors thus claimed the proposed protocol is secure as well as efficient. In 2016, Gope and Hwang [1] further proposed an authentication mechanism for a distributed IoT-based healthcare system. The proposed protocol is based on body sensor networks (BSNs), which consist of lightweight and healthcare oriented smart objects. Lightweight crypto-modules, such as a one-way hash function random number of generation function and bitwise exclusive-OR operation, are adopted to simultaneously pursue system efficiency and security robustness. The authors then investigated the security density and protocol efficiency via BAN logics analysis and computation cost comparison.

B. SECURITY REQUIREMENTS FOR IOT-BASED HEALTHCARE SYSTEMS

In the following, we present the major security requirements for IoT-based communication systems.

A SESSION KEY IS REQUIRED FOR SECURE COMMUNICATION

In the past decades, the research community has thoroughly investigated the design of dynamic identity-based authentication schemes owing to their advantages in terms of user convenience and protocol efficiency. Lightweight computation modules, such as one-way hash functions and bitwise exclusive-or operation, are usually exploited in the design of secure transmission for each protocol run. Because communication entities' identities are anonymous and unpredictable as a result of the hash function and exclusive-or operation, it can be claimed that this category of authentication provides user anonymity. However, in traditional dynamic identity-based authentication mechanisms, a robust session key must be eventually agreed for secure communication among entities. A simple authentication and login activity without session key generation is not enough to guarantee any kind of security. Even if it may be claimed that SSL/TLS or other security techniques can be used to achieve robust security after the authentication, the computation cost involved will make such an approach inefficient. Based on the above reason, we argue that the session key agreement is an essential property for entity authentication and secure communication.

INAPPROPRIATE USAGE OF THE BITWISE EXCLUSIVE-OR MODULE MUST BE AVOIDED

Cryptanalysis for security modules is critical for protocol robustness. While the one-way hash function maintains qualified security, the exclusive-or operation may be the attacker's target. It is obvious that the exclusive-or operation can only resist against ''cipher-text only'' attacks, which represents the lowest security level in terms of cryptanalysis activity. Other security guarantees, such as resistance to known plain-text attacks, chosen plain-text attacks, chosen cipher-text attacks, and chosen text attacks launched by a malicious adversary are not supported. Hence, we have to carefully consider the utilization of the exclusive-or operation during the design of each protocol run. More specifically, all publicly transmitted text must be in an unpredictable cipher form and the exclusive-or computation cannot be performed simply and directly on the cipher. It is suggested that all exclusive-or operations must be embedded within the computation of a one-way hash function. For example, the form of ''M $\oplus$

key'' may be more vulnerable than the form of ''H(M ⊕key)'' or ''H(M) ⊕ key'', where key is a secret and M is a message.

GPS INFORMATION IS SUGGESTED TO RESIST AGAINST SPOOFING ATTACK

The IoT-based communication architecture builds on traditional wireless sensor networks and at the same time embeds body area networks consisting of body bio-sensors. Individual privacy is a key issue to consider owing to the involvement of personal bio-data and sensitive health-related information. Meanwhile, the correctness of application operation incurred by sensor movement must also be considered 10290 VOLUME 4, 2016 K.-H. Yeh: Secure IoT-Based Healthcare System With Body Sensor Networks carefully, including individual identification, network switching, reputation maintenance, anonymity and un-traceability, and resistance to spoofing attacks invoked by a malicious cluster head made up of parts of IoT networks. All these requirements can be supported via the anonymous authentication technique with a unique legitimate identification in which GPS information is involved. That is, with identification of an individual's location, immunity against spoofing attacks can be guaranteed.

THE NEED FOR RESISTANCE TO MAN-IN-THE-MIDDLE ATTACK

Resistance to man-in-the-middle attack is one of the most important security considerations after authentication. A malicious attacker may interrupt transmitted authentication messages and spoof the legal communicating entities into believing that he/she is the other legitimate side via counterfeited and illegal messages by spoofing. That is, the attacker may pretend that he/she is the legitimate user who is communicating with the server. Spoofing can also be used when the attacker faces the real legitimate user. The attacker may pretend to be the legitimate server to communicate with the legal user. An efficient solution for resisting man-in-the-middle attacks is to embed the identities of all communicating entities into the protocol message for entity authentication. For instance, H (IDi ||IDi+1|| . . .) is a possible form of protocol message which can

be utilized to perform entity authentication and simultaneously conquer man-in the-middle attacks.

MULTIPLE SECURITY AND PRIVACY PROPERTIES MUST BE GUARANTEED AT THE SAME TIME

The protection of data security and entity privacy is the most important aspects for IoT-based healthcare systems. As the communication of the BSN is mostly wireless (and insecure) in nature, various attacks may be launched at it as a vulnerability entry, resulting in serious system damage to the entire system. Therefore, in the following, we describe the key security and privacy properties which must be guaranteed in an IoT-based healthcare system. First, mutual authentication among communication entities is required to protect against malicious data access and entity spoofing. Second, the system has to achieve anonymity and untraceability for the biosensors in IoT-based healthcare systems to guard against the disclosure of an individual's personal health status or private information. Third, the resistance against forgery attack and replay attack during system operations must be embedded into the IoT-based healthcare system.

2.1.1 EXISTING SYSTEM

At present a patient has to travel to the nearest hospital for treatment. To see a doctor, he has to their wait for his turn. Doctor on examination of basic medical parameters prescribe medicines or ask for further investigation at the lab. After that patient if required will be admitted for inpatient treatment or will be disposed of as an outpatient with necessary medicines. This process is time and effort consuming and is expensive. Moreover, in case of a medical emergency it will take time to reach a doctor/hospital. In many such emergencies a patient by the time he reaches the hospital is dead. There are many such case of "brought dead" in our present scenario. Modern healthcare system with the advent of IOT is able to provide BSN CARE and thus saving many lives. It is boon to old people staying alone and at isolated places.

2.1.2 DRAWBACKS OF EXISTING SYSTEM

- Existing System is inefficient.
- It is very tedious and time consuming.
- Lack of safe and security.
- Complexity.
- More human efforts.
- Implementation Issues.
- High Expenses.

CHAPTER 3

OVERALL DESCRIPTION

3.1 PROPOSED SYSTEM

- **IOT BASED BSN-CARE**

The proposed system is intended to assist old people staying alone with quality and timely healthcare. The patient health status can to seen by the designated healthcare on real time which enable them to take timely action.

I have used the following components in my project:

(a) Wrist band
(b) Node mcu
(c) Temperature sensor
(d) Heart beat pulse sensor amped

(a) **Wrist Band**: Is worn by patient on the wrist. Node mcu and temperature sensors are embedded on to it.
(b) **Node mcu**: Is a nano chip on the wrist band to which other sensors are also connected sensors feed their output to the nano chip which convert them to digital signal and is fed to the cloud server application. ESP 8266 node mcu is used in my project.
(c) **Temperature sensor**: I have used LM35 to -92-3 board mount temperature sensor. It measures the temperature of the patient on any given time and feed it in to the node mcu. In case of up normal temperature, it gives an alarm to the patient to the careful.
(d) Heart beat pulse sensor Amped: This sensor is clipped on to a finger of the patient and connected to the node mcu with the help of wire. This sensor measured the heart beat

pulse rate and is fed to the node mcu as electrical signals (digital) through the connected wire.

(e) **Open Source Android App (Blynk)-:** Blynk is an open source android app which is designed and developed in order to control the hardware via internet of things (IOT). This digitally displays sensor data, it can accumulate and visualize the data. Plus, it can also do other parameters such as:

(f) **Blynk App**: This app gives us to create amazing interfaces for a project using multiple widgets which is an in-build app.

(g) **Blynk server**: It acts as an interface between the smartphone and hardware which is responsible for the communication. We can also use blynk cloud or compile our private blynk server. It's an open source that can control any number of devices plus can also be launched on Raspberry pi.

(h) **Blynk Libraries**: For all the standard hardware platforms, supports communication with the sensor and the complete progression of incoming and outgoing instructions.

(i) **Embedded C:** It is mainly used for the purpose of real time response. RTS (real time response) is designed and developed as a device which corrects based on the time of response. The advanced version of RTS follows the concept of responding with delay is fine. For instance, this includes railway platform which displays schedule system.

(j) **Arduino IDE**: Arduino IDE where IDE (Integrated Development Environment). This is basically an open source app where one can code, compile, and upload a file in an Arduino device. In fact, any Arduino modules are adapted by this software, which has in build features by default. It is available for operating systems for instance MAC, Windows, Linux, and runs on the java software. A range of Arduino modules, consist of Arduino Uno, Arduino Mega, Arduino Leonardo, Arduino Micro etc. Every module contains a microcontroller on the board which is in build by default.

3.2 FEATURES OF PROPOSED SYSTEM

- Cost Effective
- Efficient
- Can Implement Easily
- Safe and Secure
- Easy to maintain
- Can easily add advanced technologies
- User Friendly
- Light Weight
- Ease of Use

3.3 ADVANTAGES OF PROPOSED SYSTEM

- The proposed IOT based BSN CARE health system is cost effective as its components are available at affordable prices.
- The system is very efficient as the information on human health is obtained on real time at the health care provider.
- A solar power system is provided for powering all the sensors.
- An ESP8266 WIFI module is used for connecting to the internet
- In this project, a system for 24*7 human health monitoring is designed and implemented.
- The system can be implemented easily due to availability of wearable IOT devices and mobile network.
- It is safe and secure as adequate security measures are incorporated.
- It is easy to maintain, user friendly and light weight.
- Analysis and prediction of chronic disorders in primary stage through the data mining techniques for better decision by doctors.
- Future expansion is possible as advanced technologies can easily be added.

3.4 REQUIREMENT SPECIFICATION

System analyst tasks to a variety of persons to gather details about the business process and their opinions of why things happen as they do and their ideas for changing the process. These can be done through questionnaires, details investigation, observation, collection of samples etc. As the details are collected, the analyst studies the requirements data to identify the features the new system should have, including both the information the system produces and operational features such as processing controls, response times, and input output methods.

Requirement specification simply means, "Figuring out what to make before you make it". It determines what people need before you start developing a product for them. Requirement definition is the activity of translating the information gathered in to a document that defines a set of requirements. These should accurately reflect what consumer wants. It is an abstract description of the services that the system should provide and the constraints under the system must operate. This document must be written for that the end user and the stake holder can understand it.

The notations used for requirements definition should be based on natural languages, forms and simple intuitive diagrams. The requirements fall into two categories: functional requirements and non-functional requirements.

The requirements of specification of the proposed system are as follows:

- NODE MCU(ESP8266)
- Embedded C
- Internet of Things (IOT)
- Open Source Android App (Blynk)
- Thingspeak
- Temperature sensor
- ECG
- Power Supply
- Heart beat pulse sensor Amped
- Wrist band
- Arduino IDE

3.5 FEASIBILITY ANALYSIS

The initial investigation points to be question whether the project is feasible. The feasibility study concerns with the considerations made to verify whether the system fit to be developed in all terms. Once the idea to develop software is put forward, the question that rises first will pertain to be the feasibility aspects. Feasibility study is a test of proposed system regarding its efficiency, impact on the organization, ability to meet the need of users and effective use of resources.

Thus, when a new project is proposed, it normally goes through a feasibility study before it is approved for development. A feasibility study is conducted to select the best system that meets the system performance requirements. This entitles an identification description, an evaluation of candidate system and the selection of the best system for the job.

During system analysis, a feasibility study of the proposed system was carried out to see whether it was beneficial to the organization. Three key considerations that are involved in the feasibility study. They are,

- Technical Feasibility
- Economic Feasibility
- Behaviour Feasibility
- Operational Feasibility

3.5.1 TECHNICAL FEASIBILITY

Technical Feasibility centres on the existing computer system hardware, software, etc. and to some extent how it can support the proposed addition. This involves financial considerations to accommodate technical enhancements. Technical support is also a reason for the success of the project. The techniques needed for the system should be available and it must be reasonable to use. Technical Feasibility is mainly concerned with the study of function, performance, and constraints that may affect the ability to achieve the

system. By conducting an efficient technical feasibility, we need to ensure that the project works to solve the existing problem area.

Since the project is designed using Embedded C as programming language. It is very efficient and user friendly. Here we are using NODE MCU to feed the program and the readings from various sensors are send to the mobile phones using Bluetooth data monitoring app which easy to use and maintain.

3.5.2 ECONOMIC FEASIBILITY

The role of interface design is to reconcile the differences that prevail among the software engineer's design model, the designed system meets the end user requirement with economical way at minimal cost within the affordable price by encouraging more of proposed system. Economic feasibility is concerned with comparing the development cost with the income/benefit derived from the developed system. In this we need to derive how this project will help the management to take effective decisions.

Economic Feasibility is mainly concerned with the cost incurred in the implementation of the project. Since this project is developed using Embedded C which is more commonly available and even the cost involved in the installation process is not high.

This project has various sensors which is available at low cost in the market. The helmet used in this project is also low cost. Also, the price of micro controller NODE MCU is affordable. The installation cost of Bluetooth data monitoring app, Arduino IDE are also free.

The system once developed must be used efficiently. Otherwise there is no meaning for developing the system. For this a careful study of the existing system and its drawbacks are needed. The user should be able to distinguish the existing one and Proposed one, so that one must be able to appreciate the characteristics of the proposed System, the manual one is not highly reliable and also is considerably fast. The proposed system is efficient, reliable and also quickly responding.

3.5.3 BEHAVIOUR FEASIBILITY

Proposed projects are beneficial only if they can be changed in to information system that will meet operation requirement of the organization. People are inherently resistant to change and computers have been known to facilitate changes. An estimate should be made of how strong reaction the user staff is likely to have towards the development of a computerized system. The behavioral feasibility depends upon whether the system performed in the expected way or not. Behavioral Feasibility study is a test of system proposal according to it workability, impact on organization, ability to meet user's need and effective use of resources. However, a feasibility study provides a useful starting point for full analysis. Our system is behaviorally feasible because of the effective use of the resources and also the system satisfies user needs and is user friendly. The different sensors used will increase the systems performance and makes is more effective. The user will be able to identify the malicious websites quickly and effectively.

3.5.3 OPERATIONAL FEASIBILITY

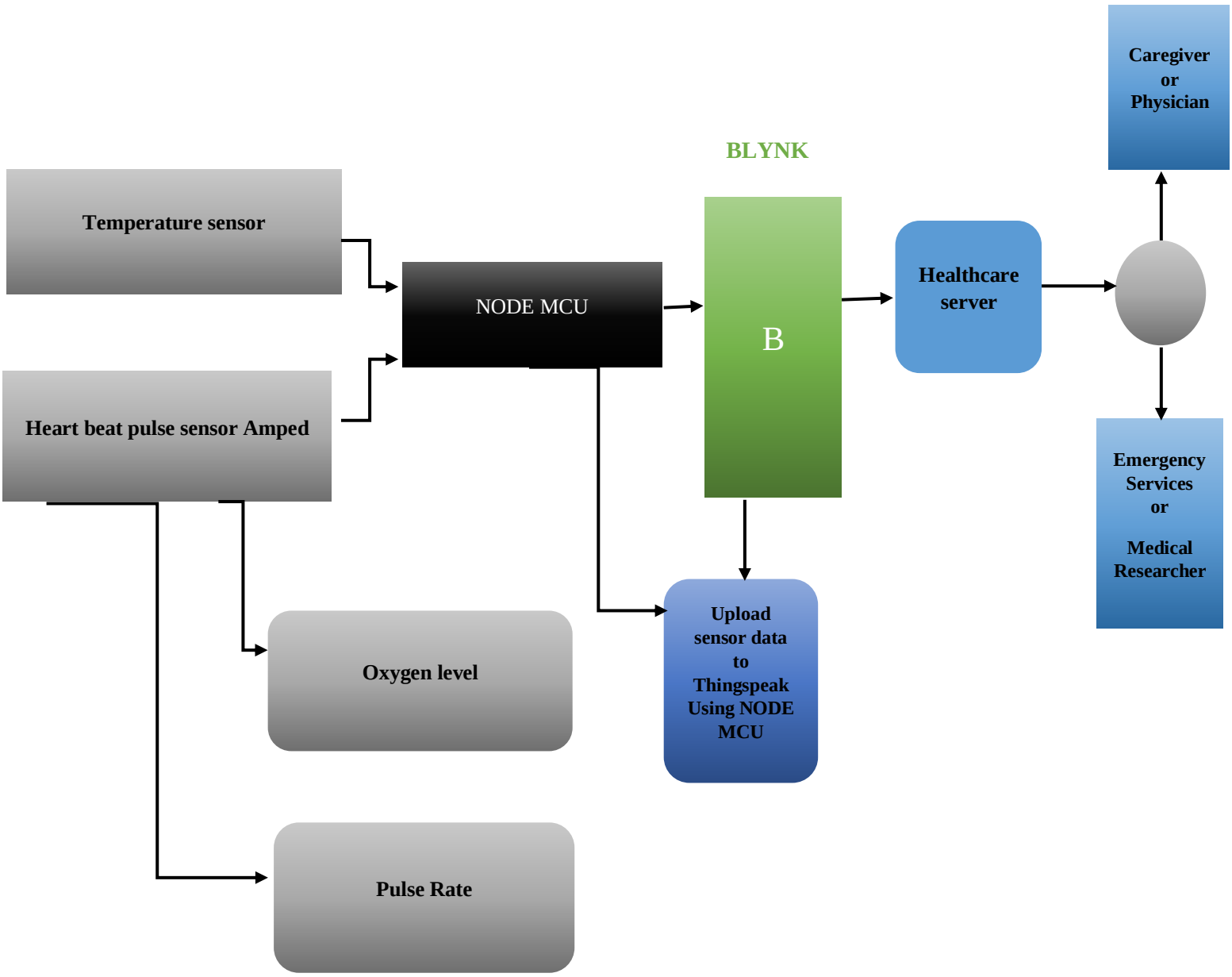
There is not much difficulty in implementing the system. The proposed system is effective, user friendly and functionally efficient. The user of the system must be unaware of the internal working of the system so that the user will not face any problems running the system. In our system we are using NODE MCU microcontroller and various sensors. We can extend or add any features to the system easily

The sensors will give accurate value according to the programs that are fed in to the micro controller. The user can easily use the system and app. There is no need to worry about the internal procedures of the system.

ABSTRACT

In the present-day environment, it was thought to be possible to provide efficient and timely healthcare to patients particularly those elders staying alone at isolated places. The present system of a patient physically moving to a healthcare provider has yielded no efficient result. Therefore, an attempt was made to make use of modern developed technologies like IOT and Body Sensor Network (BSN). In this project, therefore it was thought to make use of the already developed technologies like IOT and BSN. However, development of this technology demands careful consideration of security of patient. An attempt is therefore made to cover major security requirements. Subsequently a secure IOT based healthcare system using various body sensors already available in the market is proposed. The proposed system envisages use of various body sensors which can be worn by the patient and can be easily managed by the veteran patients. The output of the sensors used are consolidated by a local processing unit which further forward it to the healthcare server through the mobile network. I have used NODE MCU (ESP8266) worn by the patient on his wrist and a few body sensors which are commercially available in the market. The proposed system enables a patient's medical status to be monitored by the healthcare team on real time and thus a patient getting timely and quality healthcare. This system when further developed will be definitely a blessing particularly to isolated elders suffering from prolonged life style diseases. About 75 % of elders of today is suffering from one or two of the life style diseases namely diabetes, hypertension etc. The proposed BSN healthcare system come to the timely rescue of these elderly patients who are otherwise not able to make it to hospital due to poor health condition. Depending on a patient's requirement, he is made to wear various body sensors. The proposed body sensor network with the help of IOT make it possible for the designated healthcare team to get the patient health condition instantly. Components used in the proposed system are commercially available and are affordable. BSN healthcare system with the help of IOT is a very valuable instrument for healthcare and is definitely going to revolutionize the healthcare system of the world.

BLOCK DIAGRAM



BLOCK DIAGRAM OF PROPOSED BSN-CARE

Sensors output of the sensors worn by the patient namely Temperature sensor, Heart beat pulse sensor, oxygen level and pulse rate sensor are fed to the NODE MCU. These sensor data are uploaded to Thingspeak using NODE MCU. Blynk server then forward the coded data to Healthcare server. The data so received is analysed and interpreted by the healthcare server. Healthcare server then feed the data to the concerned care giver or physician. It also simultaneously feed the data to emergency services or medical researcher. Healthcare giver and emergency services take appropriate action to treat the patient and also information is passed on to family or friends. The whole action is taking place on real time and hence no valuable time is lost in providing necessary treatment to the patient.