SIDDAGANGA INSTITUTE OF TECHNOLOGY, TUMAKURU-572103

(An Autonomous Institute under Visvesvaraya Technological University, Belagavi)

Project Report on

"Authenticity and Revocability for Wireless Body Area Network"

submitted in partial fulfillment of the requirement for the award of the degree of

BACHELOR OF ENGINEERING

in

ELECTRONICS & COMMUNICATION ENGINEERING

Submitted by

Brunda U S (1SI16EC016)

K Sandhya (1SI16EC031)

Madhurya Kulkarni G V (1SI16EC043)

Navya N (1SI16EC054)

under the guidance of

MR. PRADEEP H S

Assistant Professor

Department of E&CE

SIT, Tumakuru-03

DEPARTMENT OF ELECTRONICS & COMMUNICATION ENGINEERING

2019-20

SIDDAGANGA INSTITUTE OF TECHNOLOGY, TUMAKURU-572103

(An Autonomous Institute under Visvesvaraya Technological University, Belagavi)

DEPARTMENT OF ELECTRONICS & COMMUNICATION ENGINEERING

CERTIFICATE

Certified that the project work entitled "AUTHENTICITY AND REVOCABILITY FOR WIRELESS BODY AREA NETWORK" is a bonafide work carried out by Brunda U S (1SI16EC016), K Sandhya (1SI16EC031), Madhurya Kulkarni G V (1SI16EC043) and Navya N (1SI16EC054) in partial fulfillment for the award of degree of Bachelor of Engineering in Electronics & Communication Engineering from Siddaganga Institute of Technology, an autonomous institute under Visvesvaraya Technological University, Belagavi during the academic year 2019-20. It is certified that all corrections/suggestions indicated for internal assessment have been incorporated in the report deposited in the department library. The Project report has been approved as it satisfies the academic requirements in respect of project work prescribed for the Bachelor of Engineering degree.

Mr. Pradeep H S	Head of the Department	Principal
Assistant Professor	Dept. of E&CE	SIT,Tumakuru-03
Dept. of E&CE	SIT,Tumakuru-03	
SIT,Tumakuru-03		

External viva:

Names of the Examiners **Signature with date**

1.

2.

ACKNOWLEDGEMENT

We offer our humble pranams at the lotus feet of **His** Holiness, **Dr. Sree Sree Sivakumara Swamigalu**, Founder President and **His** Holiness, **Sree Sree Siddalinga Swamigalu**, President, Sree Siddaganga Education Society, Sree Siddaganga Math for bestowing upon their blessings.

We deem it as a privilege to thank **Dr. M N Channabasappa**, Director, SIT, Tumakuru, **Dr. Shivakumaraiah**, CEO, SIT, Tumakuru, and **Dr. K P Shivananda**, Principal, SIT, Tumakuru for fostering an excellent academic environment in this institution, which made this endeavor fruitful.

We would like to express our sincere gratitude to **Dr. R Kumaraswamy**, Professor and Head, Department of E&CE, SIT, Tumakuru for his encouragement and valuable suggestions.

We thank our guide **Mr. Pradeep H S**, Assistant Professor, Department of Electronics & Communincation Engineering, SIT, Tumakuru for the valuable guidance, advice and encouragement.

Brunda U S	(1SI16EC016)
K Sandhya	(1SI16EC031)
Madhurya Kulkarni G V	(1SI16EC043)
Navya N	(1SI16EC054)

Course Outcomes

CO 1 : Identify and formulate the problem through literature survey and knowledge of contemporary engineering technology.

CO 2 : Apply engineering knowledge to arrive at optimal design solutions for solving engineering problems in compliance with the prescribed safety norms/standards taking into consideration environmental concerns.

CO 3 : Select suitable engineering tools, platform, sub-system for solving identified engineering problem.

CO 4 : Implement the proposed solution on the selected platform, considering societal, health issues. Validate the design, analyse and interpret the results using modern tools.

CO 5 : Comprehend and prepare document as per the standard, present effectively the work following professional ethics, interact with target group.

CO 6 : Contribute to the team as a member, lead the diverse team.

CO 7 : Demonstrate engineering and management principles, perform the budget analysis through utilization of the resources (finance, power, area, bandwidth, weight, size, etc)

CO-PO Mapping

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO-1	3	3										2	3	
CO-2			3									2		3
CO-3			3											3
CO-4				3	3	2	2					2		3
CO-5								3		3		2		2
CO-6									3					3
CO-7											2		2	
Average	3	3	3	3	3	2	2	3	3	3	2	2	3	3

Attainment level: - 1: Slight (low) 2: Moderate (medium) 3: Substantial (high)

POs: PO1: Engineering Knowledge, PO2: Problem analysis, PO3: Design/Development of solutions, PO4: Conduct investigations of complex problems, PO5: Modern tool usage, PO6: Engineer and society, PO7: Environment and sustainability, PO8: Ethics, PO9: Individual and team work, PO10: Communication, PO11: Project management and finance, PO12: Lifelong learning

Abstract

With recent technical advancement in wireless communication, network security have been of great concern. To address this concern, a secured system is to be developed to provide data security over wireless transmission.

The proposed project aims at developing Wireless Body Area Network (WBAN) using cryptographic AES algorithm which monitors patient biomedical parameters based on sensors, Arduino and ZigBee.

WBAN provides real-time measurements of patients' health data supported biomedical sensors. the knowledge gathered within the common habitat of the patient, offers progressively valuable data, taking into consideration an increasingly precise and a few of the time much quicker conclusion. AES algorithm is implemented for secure communication over wireless network by encryption and decryption of physiological parameters. ZigBee module provides communication wirelessly between client and application providers i.e., hospital and physician by configuring the devices. Implementation of algorithm using Arduino has been communicated by ZigBee network to provide security to the encrypted data (ciphertext) on medium cost devices. This ensures security of data for medical rehabilitation and monitoring of patients.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

Wearable wellbeing observing frameworks incorporated into telemedicine frameworks are novel data innovation that will have the option to screen the strange wellbeing conditions and avoidances of its genuine results. The health of the patient can be monitored using the proposed project at the distant location.

1.1 Motivation

With increase in population, present logical sources cannot satisfy predetermination human services and health issues of patients. Assets are limited and it's impractical for the greater part of the patients to deal with their well-being for a long-term period by staying in a medical clinic because of busy work life and money related guidelines. Consequently to give the status of their well-being, the attributes of the WBAN radio propagation are dynamic to the movements of the physical body. As a result, wireless tracking methodical structure will become a neighborhood of cell healthcare facilities with real-time tracking within the future. during this context, WBAN supporting healthcare applications can over valuable contributions to enhance patient healthcare, including diagnosis and therapeutic monitoring. In a short span of time, WBAN technology has taken its recent steps in the medical rehabilitation and monitoring of patients.

1.2 Objective of the project

The objective of the project is to adopt the ZigBee technology and protocols which satisfy the prerequisites of WBANs for healthcare application, to provide security to the data obtained by sensor nodes are encrypted at transmitter and decrypted at the receiver (i.e. Application providers (APs) like: Hospital, Physician) using AES algorithm. The project aims at helping the APs to understand the patients' issues within a period of time securely.

1.3 Organisation of the report

The report is divided into seven chapters. The motivation and objective of the project is described in chapter 1. Chapter 2 comprises of literature survey. Chapter 3 contains block diagram of the proposed project. Chapter 4 depicts about the hardware description where functionality of the hardware components used are discussed. Chapter 5 explains about required software tools and proposed algorithm. The experimental results are presented in Chapter 6. Chapter 7 briefs conclusion and future work.

Chapter 2

Literature Survey

This chapter provides a detailed description about the literature survey conducted on wearable sensors, cryptographic algorithm.

1. **Existing health monitoring systems**

   (a) "Sensor System and Health Monitoring", Jiuping Xu, Lei Xu, in Integrated System Health Management, 2017
   Assembles a sensor optimization choice model to pick the minimal most informative, cost-effective sensor subset, and build up a energy-efficient decentralized detection scheme supported the sensor particular system [1].

   (b) "Security and Privacy in Remote Healthcare", Pijush Kanti Dutta Pramanik, Anand Nayyar, in Telemedicine Technologies, 2019
   The remote wellbeing observing systems require the continual, uninterrupted checking of wellbeing qualities of patients employing a disseminated system of sensors. These sensors and in this way the individual passage or organizer are potential sources of security and privacy vulnerabilities.

2. **Wearable devices**

   (a) "Wearable sensors for athletes", Minyoung Suh, in Electronic Textiles, 2015
   Constant ongoing observing is conceivable when the sensor is worn on the physical body by methods for dress or accessories. Different sorts of e-textiles are adopted to define textile sensors. These electronics can convey the well-being information to a assigned individual or foundation – emergency clinics or training staff – from a separation through wireless communication [4].

(b) "Driving e-healthcare Beyond Telemedicine to Remote Health Monitoring", Pijush Kanti Dutta Pramanik, Gaurav Pareek, in Telemedicine Technologies, 2019

A remote patient monitoring server is furnished with the necessary vital requirement and programming required for complex examination on the gathered information and produce alerts as indicated by the result of the analysis [5]. The wearable gadgets and measuring equipment at the patient's end aid accurate and effective collection. Data collection serves as the reason for additional activating collection, handling, and perception of information for the clinical professional or the patient [9].

3. **Purpose of Encryption**

The term Encryption refers to strategies of making information mixed up or undecipherable by anybody aside from the authorized recipient within the event that the message is blocked by another person. It is utilised to offer three basic services:

(a) Authentication

(b) Data integrity

(c) Data confidentiality

Advanced Encryption Standard (AES)

The resistance of AES towards differential and linear crypt-analysis comes from a better "avalanche effect" and specially crafted [6]. AES is the replacement of Data Encryption Standard (DES) as standard symmetric encryption algorithm. AES utilizes keys of 128, 192 or 256 bits, although, 128 bit keys provide adequate quality today. It utilizes 128 bit blocks, and is productive in both programming and equipment usage [7].

Chapter 3

Design Methodology

WBAN architecture establishes communication between the client of WBAN and application providers i.e., hospital and physician as shown in Figure 3.1. WBAN includes wearable sensors, biosensors or a portable medical device.

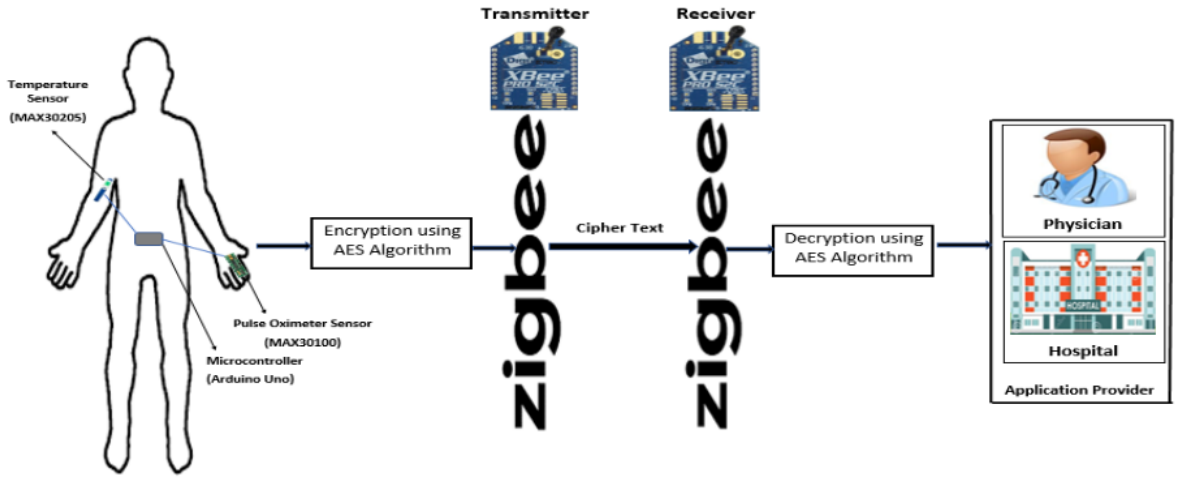


Figure 3.1: WBAN Architecture

The sensors utilized in the system are Temperature Sensor and Pulse-Oximeter Sensor which are considered based on the normal issues of people. Sensor modules are interfaced with the Arduino (ATMega328) microcontroller to collect the sensor data; it is encrypted with a secret key and the data transmission is done through ZigBee technology. Arduino IDE is utilized to program the microcontroller for interfacing of digital sensors and ZigBee modules; to configure the parameters of ZigBee, XCTU software is used. Advanced Encryption Standard (AES) algorithm is utilized for encryption and decryption of sensor data [8]. The key generation is liable for the enrolment of clients and Application providers, key is unique and preserved securely. By making use of this technique , patients' health condition are often monitored from foreign places and also provides security thereto . The proposed scheme uses the revocation and authentication approach for the identity-based encryption which avoids the third party to access the medical details.

Chapter 4

Hardware Description

This chapter explains the hardware implementation. The detailed description of the hardware components used in the system is given below

4.1 On Body Sensors

These sensors are non-invasive sensors which will be legitimately positioned on the skin of the patient or direct contact with the body. Within the project, Temperature and Pulse-Oximeter sensors are considered to monitor internal heat level, pulse and oxygen saturation level of the patient for ongoing checking of patient well-being status by advisor doctor.

4.1.1 Temperature Sensor

The sensor shown in Figure 4.1 is utilized to monitor patient body temperature is Maxim Integrated MAX30205 which precisely measures temperature and provides over-temperature caution or interrupt or shutdown yield. The digital sensor has a precision of 0.1°C over the scope of 37°C to 39°C with resolution of 16 bits (0.00390625°C).

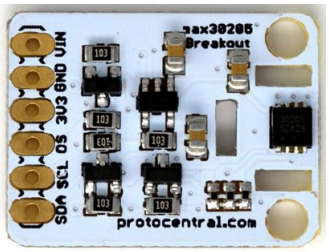


Figure 4.1: MAX30205 Temperature Sensor

Communication is through an I2C-compatible, 2-wire sequential interface. The I2C sequential interface will read the temperature information and configure the behavior of the open-channel over-temperature shutdown yield. One-Shot and Shutdown modes help with lessening power use. MAX30205 converts temperature measurements to digital form using a high-resolution, sigma-delta, analog-to-digital converter (ADC). The sensor has a 2.7 V to 3.3 V supply voltage run, low 600μA flexibly current, and a lockup-ensured

I2C-compatible interface that makes it perfect for clinical applications [10]. It consists of 6 pins in total, out of which 4 pins are used. Sequential Data line (SDA) is a bidirectional pin which transfers the data. The data transfer happens with respect to the unidirectional Serial Clock line (SCL) pin which reads the content of the temperature register through the serial data line.

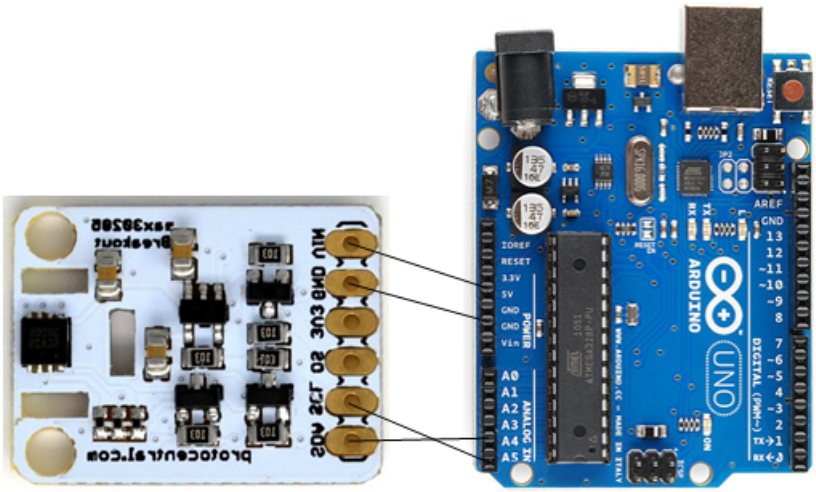


Figure 4.2: Interfacing MAX30205 Temperature Sensor with Arduino

In the proposed design, MAX30205 Temperature sensor attached to the patient body arm is interfaced with Arduino microcontroller as appeared in Figure 4.2 which sends continuously temperature data through ZigBee in terms of Fahrenheit (°F). The device works over the 0°C to +50°C temperature range i.e., 32°F to 122°F.

4.1.2 Pulse Oximeter Sensor

Maxim Integrated MAX30100 Sensor shown in Figure 4.3 is used to monitor the count of heartbeat and blood oxygen concentration of a patient. To identify beat oximetry and heart rate signals, it consolidates two LED's, a photodetector, optimized optics and low noise analog signal processing.

Figure 4.3: MAX30100 Pulse Oximeter Sensor

It works from 1.8 V and 3.3 V power supplies and may be shut down through software with negligible reserve current, allowing the facility supply to stay connected in the least times. MAX30100 sensor is attached to finger or earlobe which sends small beams of light go through the finger, estimating the measure of oxygen. It measures through changes in light assimilation in oxygenated and deoxygenated blood. The pulse rate is determined by knowing the duration between increment and decline of oxygenated blood. The device has two LEDs i.e., radiating red light and infrared light [11]. Heart rate signals can be detected by only infrared light whereas both red light and infrared light is required to measure blood oxygen levels.

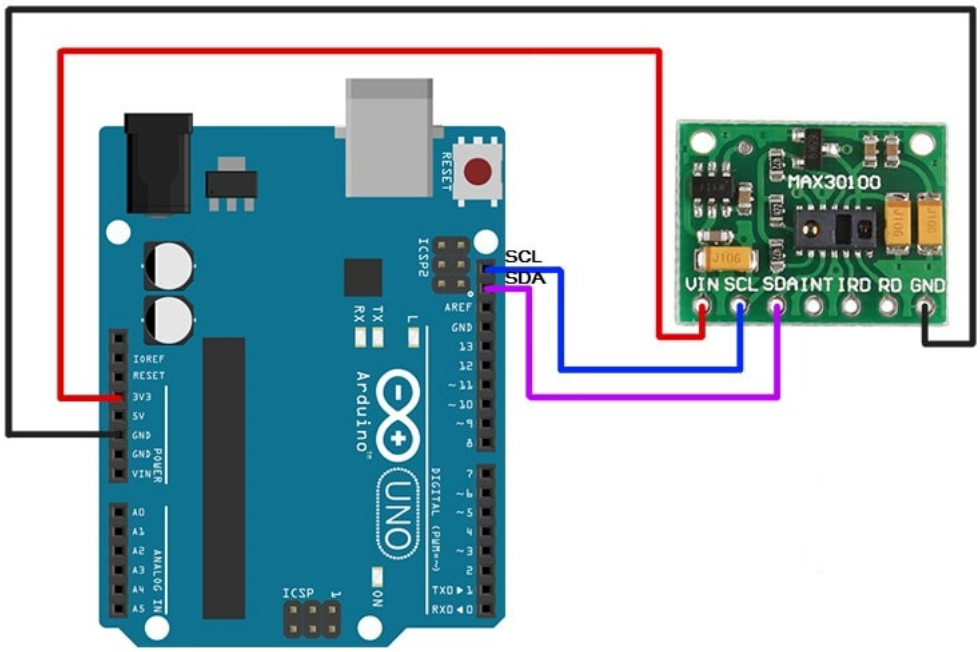


Figure 4.4: MAX30100 Pulse Oximeter Sensor

In proposed design, MAX30100 Pulse Oximeter Sensor attached to the finger of patient is interfaced with an Arduino microcontroller as depicted in Figure 4.4 which sends continuously the count of heartbeat in terms of beats per minute (bpm) and saturation level of oxygen in terms of percentage (%). The main function of MAX30100 is, oxygenated blood absorbs infrared light and deoxygenated blood absorbs red light which reads absorption levels for both light and store them in buffer that can be read via I2C serial communication. The features of MAX30100 sensor is ultra-low shutdown current i.e. 0.7μA and fast data output capability.

4.2 Arduino Microcontroller

Arduino ATMega328 shown in Figure 4.5 is an 8-bit AVR microcontroller that joins 32KB ISP streak memory with read-while-compose abilities. It has 20 digital information/yield pins (of which 6 pins can be utilised as PWM outputs and other 6 pins can be utilised as analog inputs), a 16MHz resonator, USB connection, power jack, an In-Circuit System Programming (ICSP) header and a reset button. The board feature sequential communication interface including Universal Serial Bus (USB) on some models. The device operates between 1.8 V-5.5 V. The Arduino microcontroller is programmed using a dialect of features from the C and C++ programming languages. In addition to using conventional compiler tool chains, the Arduino project provides an Integrated Development Environment (IDE) supported the processing language project.

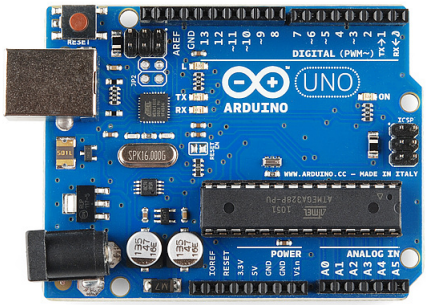


Figure 4.5: Arduino ATMega328P Microcontroller

In the proposed design, Arduino is interfaced with the digital sensors and ZigBee Module. At WBAN client, the sensor data is encrypted using Arduino and communicated wirelessly cipher text through ZigBee. At application providers, the cipher text received from ZigBee is decrypted using Arduino to get original data.

4.3 ZigBee Wireless Module

ZigBee as shown in Figure 4.6 is an IEEE 802.15.4-based detail for a set up of high-level communication protocols. The main asset of the protocol is to make wireless personal area networks, built from low powered computerised radios, for example, home automation, clinical device data collection and low power transmission capacity needs, intended for little scope projects which need remote connection.

ZigBee is a low-power, low information rate wireless ad-hoc network. The technology characterised by the ZigBee specification is proposed to be easier and more affordable than

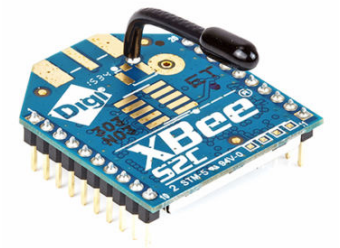


Figure 4.6: ZigBee Module

other Wireless Personal Area Networks (WPANs). ZigBee has an advantage of reliability, enduring battery life, boundless network size when contrasted with other wireless standards [12]. The frequency range supported in ZigBee mostly 2.4 GHz worldwide whose information rates vary from 20 kbit/s (868 MHz band) to 250 kbit/s (2.4 GHz band). The ZigBee modules are configured either as coordinator or router using AT commands or XCTU Software by interfacing with ATMega328 microcontroller as depicted in Figure 4.7.

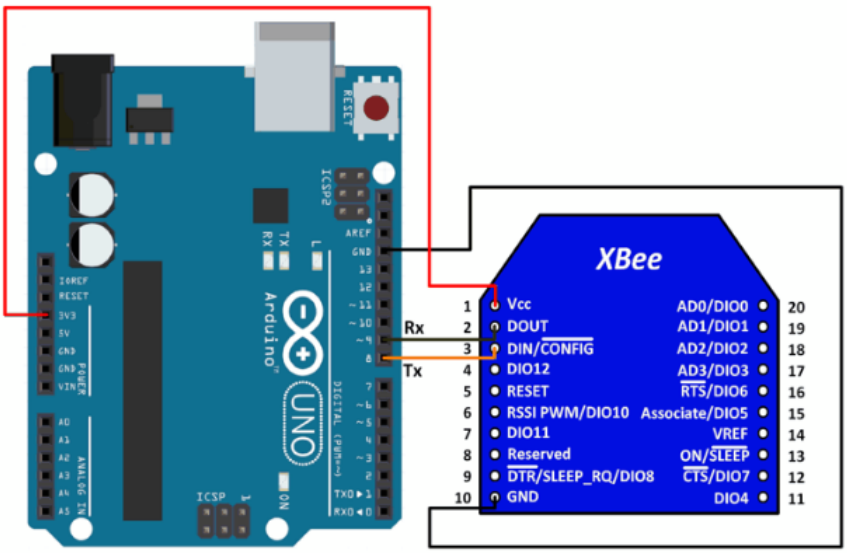


Figure 4.7: Interfacing ZigBee Module with Arduino

In the proposed project, ZigBee is used as a wireless transceiver for communicating the ciphertext using ZigBee protocols. ZigBee protocols provide the ability to transmit informative data through other ZigBee to reach the physician [13]. The ZigBee range of transmission is over 10-100 meters which can transmit information over significant distances by passing information through a mesh network of intermediate devices to succeed in more distant ones.

Chapter 5

Software Description

The chapter describes the software tools that are used in the project and proposed AES algorithm for sensor data secure communication.

5.1 Arduino IDE

The Arduino IDE is a software which is utilised to program the Arduino microcontroller. It contains a word processor for composing code, a message territory, a text console, a toolbar with buttons for regular functions and a series of menus. It interfaces with Arduino to upload programs. Programs composed using Arduino IDE as depicted in Figure 5.1 are called Sketches and these sketches are saved with file extension (.info).

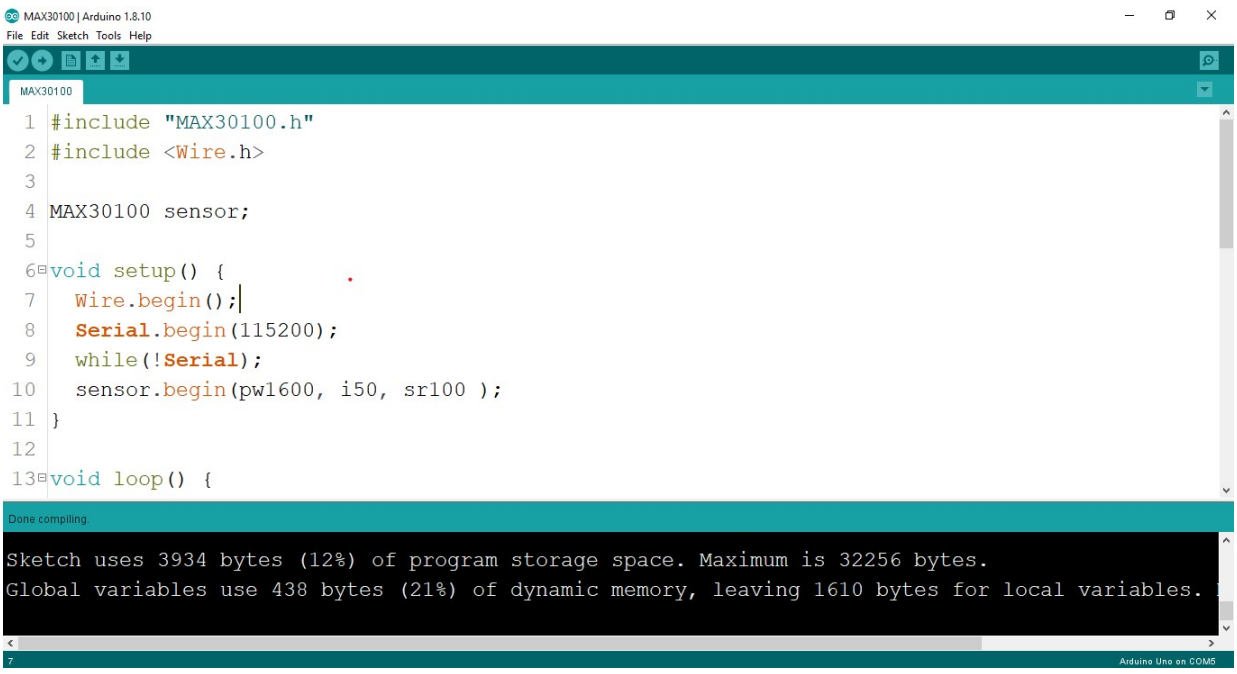


Figure 5.1: Text editor window of Arduino IDE

In the project, Arduino is programmed using Arduino IDE software for its interfacing with sensors and ZigBee module. Microcontroller sends the encrypted data at transmitter end and decryption of data is done at receiver end.

5.2 XCTU Software

ZigBee is a wireless communication module which utilizes IEEE 802.15.4 standard for low power applications of radio frequency; it acts as trans-receiver. In the project, ZigBee Modules with Arduino are configured using XCTU software as shown in Figure 5.2 to establish serial communication of data.

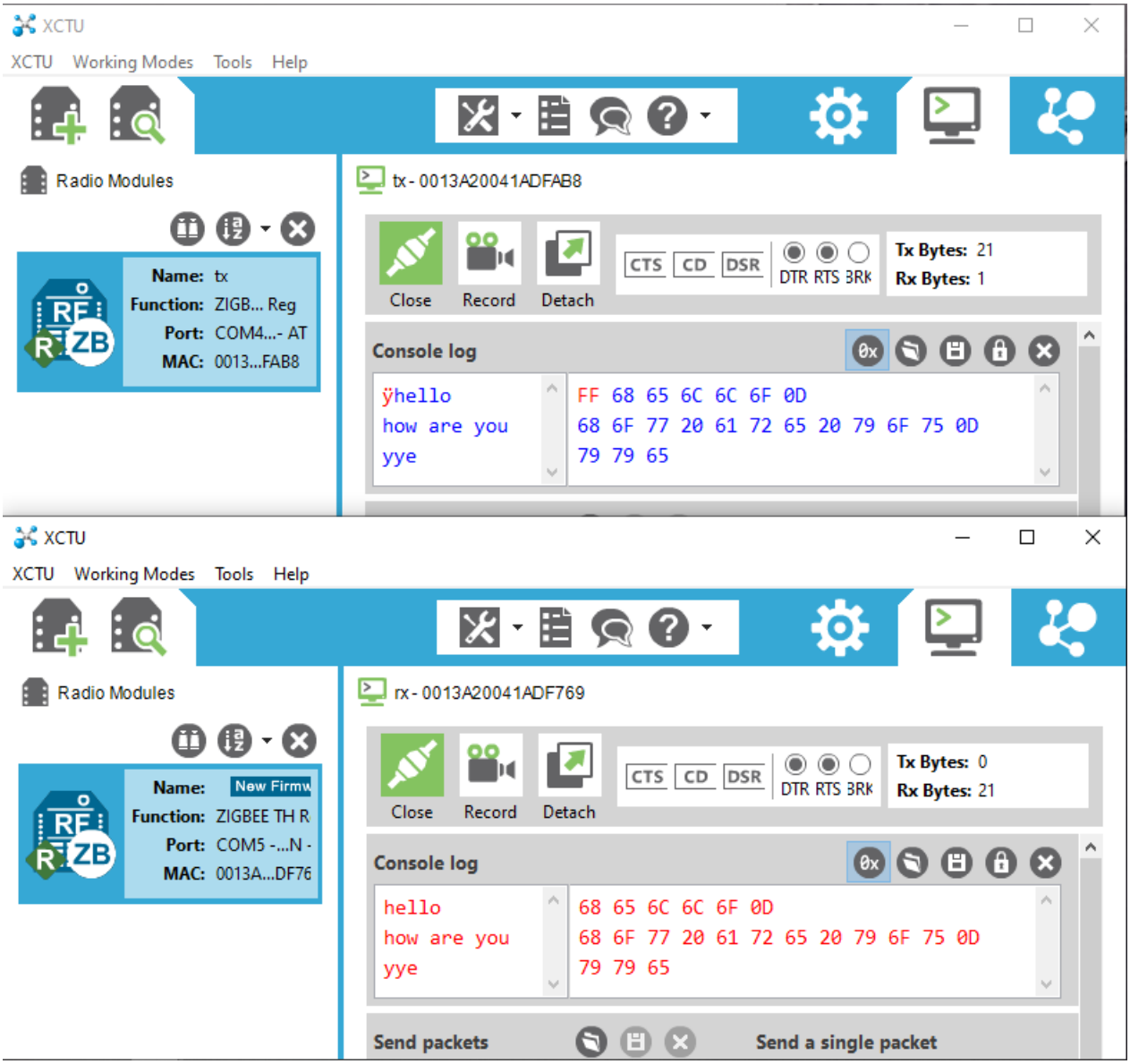


Figure 5.2: ZigBee Modules Configuration

ZigBee module can act as a Coordinator, Router or an End device, however, it should be configured using Attention commands (AT) or enter the data manually to work in desired mode. Pan ID, Source Address (MY) and Destination Address (DL) is to be given to configure ZigBee module as a Coordinator or Router [14]. ID stay same for both the modules

just MY and DL information exchange for example MY for the receiver ZigBee becomes DL of the transmitter ZigBee (coordinator) and DL for the receiver ZigBee becomes MY of the transmitter ZigBee as shown in table 5.1.

Table 5.1: Configuration of parameters

	ATDL	ATMY	ATID
XBee 1 coordinator	1234	5678	2244
XBee 2 end device	5678	1234	2244

5.3 AES Algorithm

Cryptography is a procedure for securing the secrecy of communication. In the system, Advanced Encryption Standard (AES) cryptographic algorithm is utilised to secure the data. AES has an advantage of implementing in both hardware and software to secure sensor data. It is a symmetric block cipher (as shown in Figure 5.3) which uses a key size of 128/192/256 bits in order to encrypt and decrypt the data in blocks of 128 bits. AES has built-in exibility of key length, which permits a level of 'future-proofing' against progress within the capacity to perform through key searches. It is an iterative algorithm based on 'substitution-permutation network'.

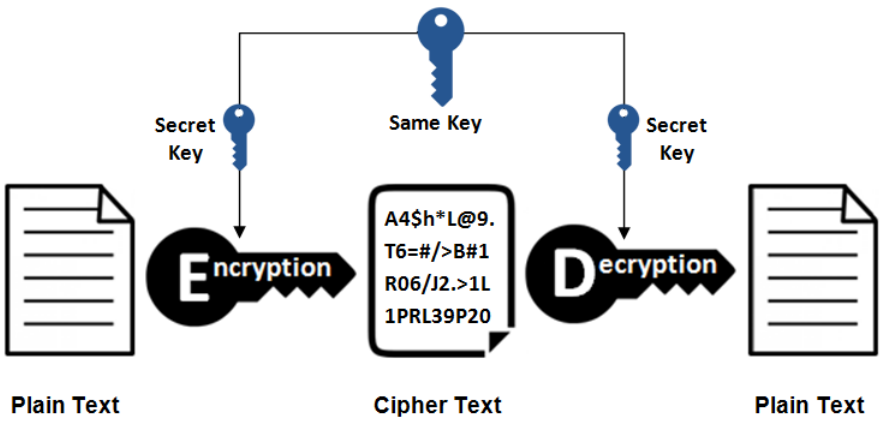


Figure 5.3: Symmetric Key Encryption

AES considers the 128 bits of a plaintext block as 16 bytes which is converted to an unusual format of representing data i.e., ciphertext using a single 128-bit key in Arduino [6]. The ciphertext is transmitted to the receiver through ZigBee. Using the same single 128-bit key, the ciphertext is decrypted to plaintext in Arduino using AES. Incorporating the security with this algorithm prevents the third-party access that may lead to societal issues and troubles the population.

Comparison between different algorithms:

- Data Encryption Algorithm (DES)

  It is one of the most widely accepted, publicly available cryptographic systems today. It was developed by IBM in the 1970s. It uses a 56-bit key to encrypt the 64 bit block size data. It processes 64-bit inputs into 64-bit cipher-text and algorithm performs 16 iterations.

- Blowfish

  It is a symmetric-key block cipher, designed in 1993 by Bruce Schneier and included in a large number of cipher suites and encryption products. Blowfish provides a good encryption rate in software and no effective cryptanalysis of it has been found to date. However, the AES now receives more attention.

Table 5.2: Comparison between different algorithms

Features	DES	Blowfish	AES
Created By	IBM in 1975	Bruce Schneier in 1993	Vincent Rijmen, Joan Daemen in 2000
Key length	56 bits	32-448 bits	128, 192 or256 bits
Round(s)	16	16	10 - 128 nit key,12 - 192 bit key, 14 - 256 bit key
Block size	64 bits	64 bits	128 bits
Acceleration type	Better in hardware than in software	Does not have hardware acceleration	Hardware & software acceleration is faster
Speed	Slow (in ms)	Very slow (in s)	Fast (in us)
Security	Not secure Enough	Moderate	Excellent Security

Blowfish algorithm is vulnerable to attacks because of its small block size. DES algorithm is vulnerable to Brute Forced,Linear and differential cryptanalysis attack and AES

algorithm is much faster based on the consumption of time for encryption and decryption processes as shown in Table 5.2.

5.4 System Flowchart

The implementation of the proposed system comprises a temperature sensor, pulse oximeter sensor, arduino and xBee modules. The design provides a continuous wirelessly monitoring system by physician of patient health within their place. The implementation of the design is carried out at client end and server end wirelessly as shown in Figure 5.4.

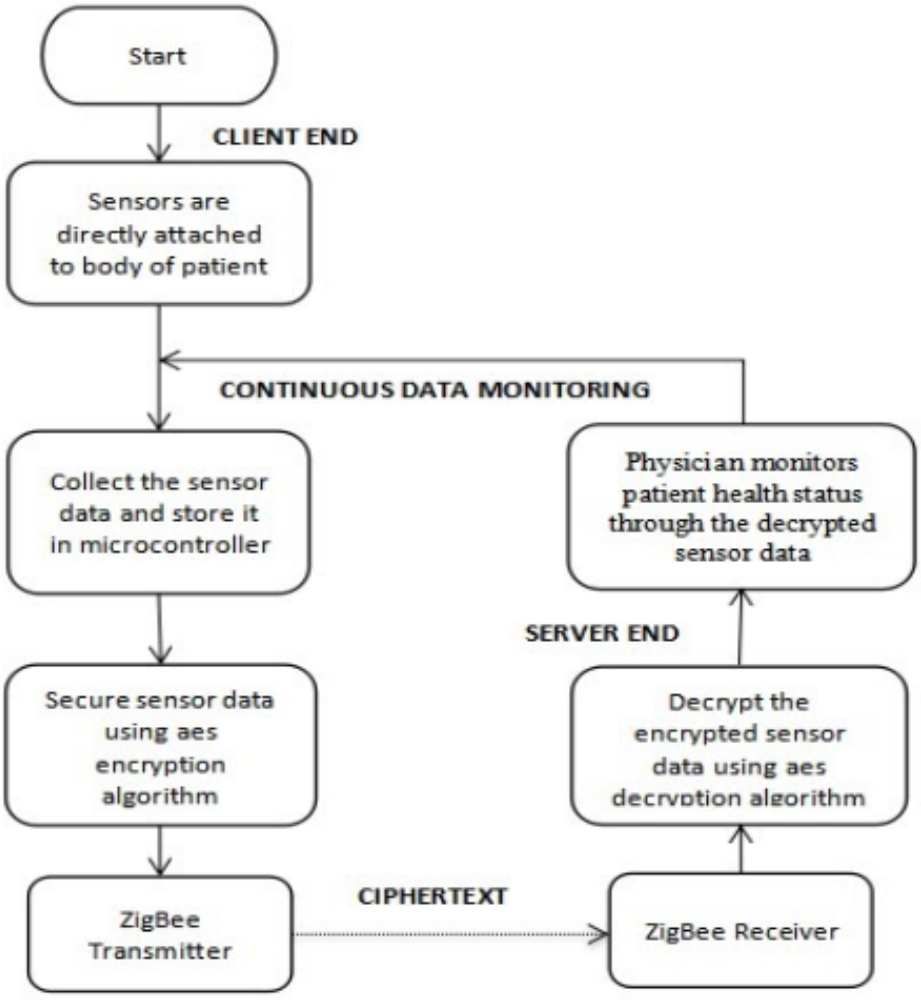


Figure 5.4: Design Flow of System

At the client end: The Temperature and Pulse-Oximeter sensors are directly attached to the skin of the patient body. The data from the sensors are collected by the Arduino ATMega328 microcontroller. The data stored in Arduino is encrypted into unusual for-

mal (ciphertext) using AES encryption algorithm to provide security of data. The ZigBee transmits the ciphertext wirelessly to the receiver side ZigBee which is configured using AT commands.

At the server end: The receiver ZigBee holds the transmitted ciphertext which is decrypted using AES decryption algorithm in Arduino. The decrypted data (original data) is monitored by physicians about patients' health status.

Chapter 6

Results

Authenticity and Revocability for Wireless Body Area Network is a continuously health monitoring system of a patient which sends the health status of the patient to the physician at regular intervals of time. Figure 6.1 shows the system module at transmitter side which consists of Arduino ATMega328 Microcontroller, MAX30205 Temperature Sensor, MAX30100 Pulse Oximeter Sensor, ZigBee Module. The transmitter module measures the vital parameter (i.e., temperature, pulse rate, oxygen saturation) with the help of sensors and encrypting the vital parameters using Arduino is sent through ZigBee to provide constant checking of patients' health by providing secure transmission of data.

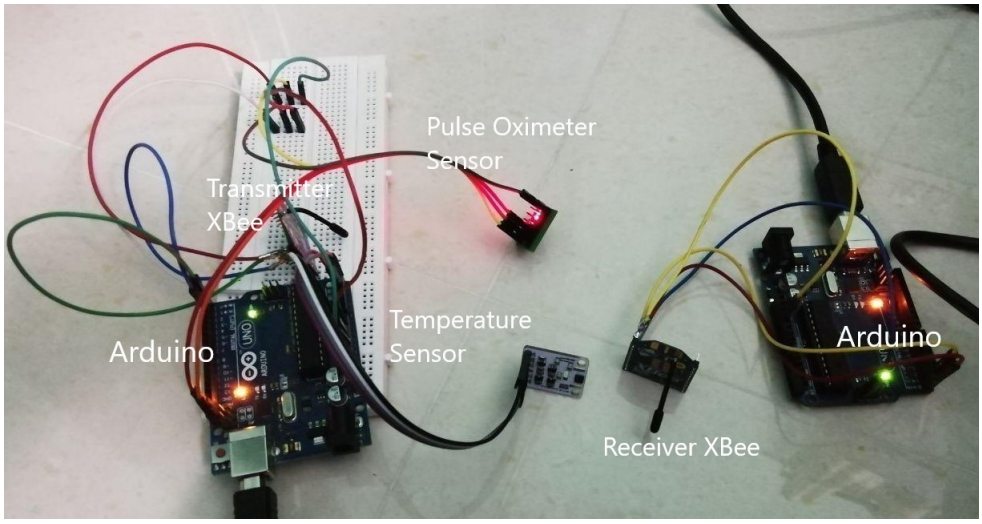


Figure 6.1: Client Side Module

Figure 6.2 depicts the system module at receiver side which consists of ZigBee Module Arduino ATMega328 Microcontroller. The ciphertext is received to the Arduino from ZigBee module and the decryption of the ciphertext is done, which displays the parameter values on the monitor of physician. Physician monitors the received data at regular time interval for being aware of the patients' health condition.

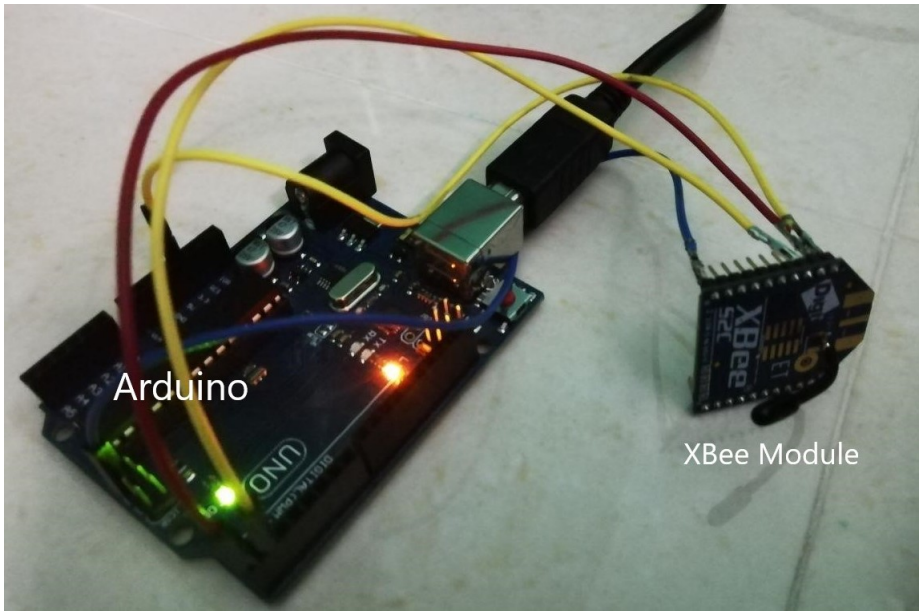


Figure 6.2: Server Side Module

At client side, the input data string includes patients' details like patient name, age and gender along with sensor data as shown in Table 6.1. The concatenated data string is converted to character array using the string length of data. The character array further encrypted into secured format (ciphertext) as shown in Figure 6.3 using inbuilt 'aes128encryption' function by considering message, message length, aes key, size of aes key, initialization vector (IV) as input to the function.

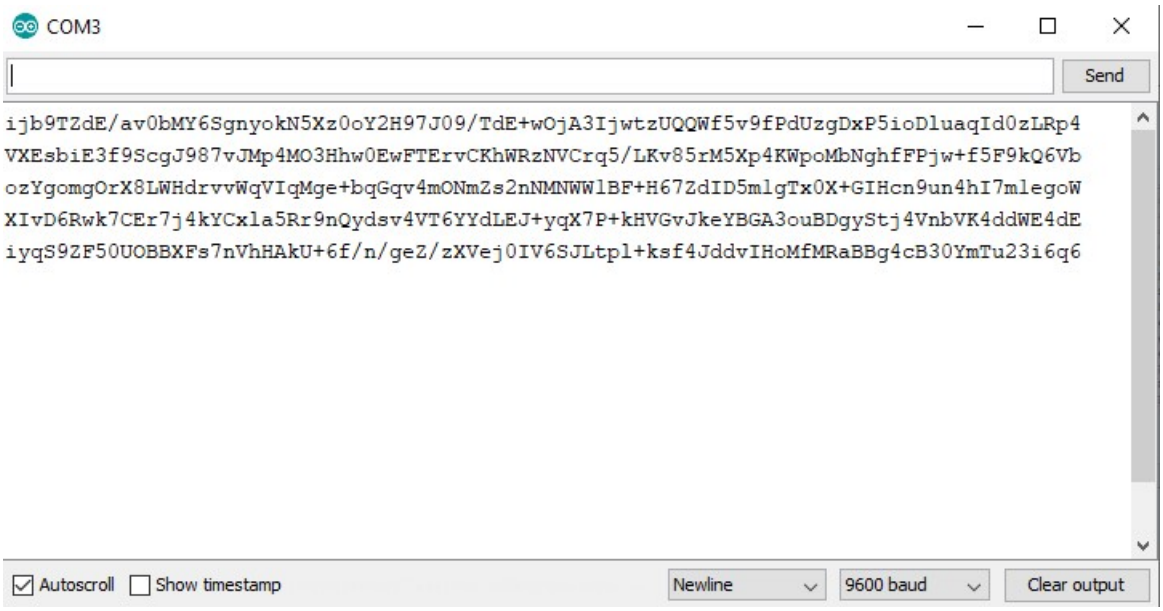


Figure 6.3: Ciphertext displayed on Serial monitor at transmitter

At server side, the ciphertext is converted to character array using the length of received ciphertext. The ciphertext character array is further decrypted into original format as shown in Figure 6.4 using inbuilt 'aes128decryption' function by considering message, message length, aes key, size of aes key, initialization vector as input to the function.

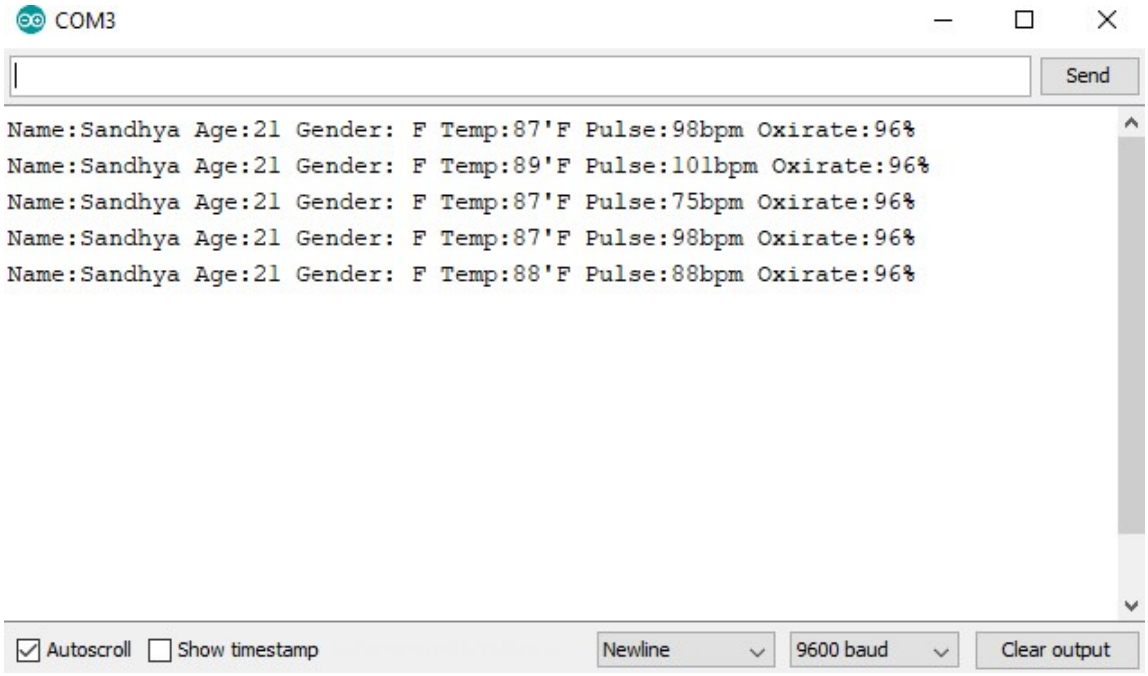


Figure 6.4: Sensor Data displayed on Serial monitor at receiver

Table 6.1 shows the difference between the reading obtained from sensor and the reading taken in health center with fluctuation nearly 5 to 7 percent. The analysis is carried out for different people using module and standard modules for temperature, beat rate and saturation level of oxygen in SIT Health center. The analysis depicts that, the readings obtained have an accuracy of 90 to 92 percent.

Table 6.1: Performance Comparison of Sensors

Patients	Iterations	Temperature (in degree F)			Pulse rate (in bpm)			SPO2 (In %)		
		MAX30205 sensor	Thermo meter	δ	MAX30100 sensor	Pulse-oximeter	δ	MAX30100 sensor	Pulse-oximeter	δ
Patient1	Iteration1	97.2	95	2.2	87	91	4	96	93	3
	Iteration2	97	95	2	89	98	9	97	94	3
	Iteration3	97.2	96	1.2	91	95	4	95	94	1
Patient2	Iteration1	96	93	3	77	85	8	96	94	2
	Iteration2	97	93	4	79	85	6	98	95	3
	Iteration3	97	94	3	73	82	9	98	94	4
Patient3	Iteration1	97.4	94	3.4	112	95	17	97	95	2
	Iteration2	97	93	4	109	93	15	98	96	2
	Iteration3	97.2	93	4.2	103	94	9	99	96	3
Patient4	Iteration1	97.1	93	4.1	98	82	16	94	96	2
	Iteration2	97	93	4	102	84	18	95	96	1
	Iteration3	97.2	94	3.2	99	86	13	94	95	1
* δ - Deviation from measured data with sensors and standard devices										

Table 6.2 includes the patients' details in string format to be transmitted. The AES algorithm produces different ciphertext for the same data with different keys. Similarly, if the same key is used for encrypting different data yields in variety of ciphertext. This varied condition implies the uniqueness of the technique being used in the system. The input data taken for encryption can be varied in size i.e. patient name; age; address etc. will be reflected at the transformed data visuals.

Data transmitted in the encrypted form will be received at the server of application providers, these data will be decrypted using the same key and technique obeyed at client's side to get exact values as shown in Table 6.3 for the same data mentioned in the

Table 6.2: Transmitter-Side Encryption

Conditions	Plaintext or Sensor data (Data obtained from sensors)	Cryptographic key (16 bytes)	Ciphertext (Encrypted data at client side)
Same input, different keys	Temp: 85'F Rate: 78bpm Oxirate: 95%	{0xB2, 0xE7, 0x51, 0x61, 0x82, 0xEA, 0x2D, 0x6A, 0xBA, 0x7F, 0x51, 0x88, 0x90, 0xFC, 0xF4, 0xC3}	iOIkSbTBvChNphdMmns/6d5hLGICh957qopk BeJT7dGbQaXdr7z/bIgBKg1SML1w
		{ 0x2B, 0x7E, 0x15, 0x16, 0x28, 0xAE, 0xD2, 0xA6, 0xAB, 0xF7, 0x15, 0x88, 0x09, 0xCF, 0x4F, 0x3C}	dBw+H6dxRpz4sAx20bigyotl5UFcQgiuc0yDug 2KWSoAZXeFvNOv7rvVtlqaEVpJ
Different inputs, same key	Temp: 93'F Rate: 75bpm Oxirate: 93%	{0xB2, 0xE7, 0x51, 0x61, 0x82, 0xEA, 0x2D, 0x6A, 0xBA, 0x7F, 0x51, 0x88, 0x90, 0xFC, 0xF4, 0xC3}	BwyWDAxyJ8N+gChfOukqf51MXspNSlvcsu7 QY7P0wvPD0/nzpukXuPVQe+GX5gKi
	Temp: 85'F Rate: 78bpm Oxirate: 95%		iOIkSbTBvChNphdMmns/6d5hLGICh957qopk BeJT7dGbQaXdr7z/bIgBKg1SML1w

Table 6.2.

Table 6.3: Receiver-Side Decryption

Conditions	Ciphertext (Encrypted data Received by Application provider)	Cryptographic key (16 bytes)	Decrypted data (original data or plaintext)
Same input, different keys	iOIkSbTBvChNphdMmns/6d5hLGICh957qopk BeJT7dGbQaXdr7z/bIgBKg1SML1w	{0xB2, 0xE7, 0x51, 0x61, 0x82, 0xEA, 0x2D, 0x6A, 0xBA, 0x7F, 0x51, 0x88, 0x90, 0xFC, 0xF4, 0xC3}	Temp: 85'F Rate: 78bpm Oxirate: 95%
	dBw+H6dxRpz4sAx20bigyotl5UFcQgiuc0yDug 2KWSoAZXeFvNOv7rvVtlqaEVpJ	{ 0x2B, 0x7E, 0x15, 0x16, 0x28, 0xAE, 0xD2, 0xA6, 0xAB, 0xF7, 0x15, 0x88, 0x09, 0xCF, 0x4F, 0x3C}	
Different inputs, same key	BwyWDAxyJ8N+gChfOukqf51MXspNSlvcsu7 QY7P0wvPD0/nzpukXuPVQe+GX5gKi	{0xB2, 0xE7, 0x51, 0x61, 0x82, 0xEA, 0x2D, 0x6A, 0xBA, 0x7F, 0x51, 0x88, 0x90, 0xFC, 0xF4, 0xC3}	Temp: 93'F Rate: 75bpm Oxirate: 93%
	iOIkSbTBvChNphdMmns/6d5hLGICh957qopk BeJT7dGbQaXdr7z/bIgBKg1SML1w		Temp: 85'F Rate: 78bpm Oxirate: 95%

The time taken for execution are: 245 μs (uses 9224 bytes for encryption) and 127 μs (uses 6202 bytes for decryption), it indicates that AES algorithm is faster in execution.

Chapter 7

Conclusion

The project titled "Authenticity and Revocability for Wireless Body Area Network" is successfully implemented and tested. Obtained results shows that the consulting physicians/doctors having the patient health report with them before the patient presence at his/her place can be helpful in diagnosing or arranging the special medications to patients in advance by those data collected from WBAN even at distant places on time. Along with the continuous monitoring, the system includes cryptographic techniques so there will be no problem if data theft incorporates in healthcare.

7.1 Scope for future work

The idea can be additionally extended into a wearable gadget by including feature like locating the patient using GPS tracker which can be used for mobile patients. Implementation of system can be upgraded to get the proportions of communicable diseases within the population by their health variations.

Bibliography

[1] Hu Xiong, Zhiguang Qin, "Revocable and Scalable Certificateless Remote Authentication Protocol with Anonymity for Wireless Body Area Networks", IEEE Transactions on Information Forensics and Security, vol. 10, issue: 7, pp. 1442 - 1455, July 2015.

[2] Ms. S. Padma, "Ensuring Authenticity and Revocability for Wireless Body Area Network using Certificateless Cryptography", International Research Journal of Engineering and Technology (IRJET), e-ISSN: 2395 -0056, vol. 03, issue: 03, March 2016.

[3] Jian Shen, Shaohua Chang, "Certificateless Authentication Protocol for Wireless Body Area Network", International Conference on Genetic and Evolutionary Computing, ISSN: 2194-5357, October 2017.

[4] Narayana K R, Sanchari saha, "A Certificate less Encryption and Signature Scheme with Efficient Revocation for Securing Inter-Body Wireless Sensor Network", International Journal of Science Technology, vol. 2, issue: 11, May 2016.

[5] Benoit Latre, Bart Braem, Ingrid Moerman, Chris Blondia, Piet Demeester, "A survey on wireless body area networks", Wireless Networks, vol. 17, issue: 1, pp. 1-18, January 2011.

[6] Robert H. Deng, "A revocable certificateless signature scheme", phD thesis, Jiangsu Engineering Research Center on Information Security and Privacy Protection Technology, Nanjing 210023, China.

[7] Hak Soo Ju, Dae Youb Kim, Dong Hoon Lee, Jongin Lim, and Kilsoo Chun, "Efficient Revocation of Security Capability in Certificateless Public Key Cryptography", International Conference on Knowledge Based and Intelligent Information and Engineering Systems, KES 2005, September 2005.

[8] Mohammad Ghamari, Balazs Janko, R. Simon Sherratt, William Harwin, Robert Piechockic and Cinna Soltanpur, "Review A Survey on Wireless Body Area Networks for eHealthcare Systems in Residential Environments", Sensors 2016, June 2016.

[9] Razie SH, "Wireless Body Area Networks: An Overview", International Research Journal of Engineering and Technology (IRJET), vol. 04, issue: 05, May 2017.

[10] Sarita Kumar, "A research Paper on Cryptography Encryption and Compression Techniques", International Journal Of Engineering And Computer Science, ISSN:2319-7242, vol. 6, issue: 4, pp. 20915-20919, April 2017.

[11] Jingwei Liu, Zonghua Zhang, Xiaofeng Chen, Kyung Sup Kwak, "Certificateless Remote Anonymous Authentication Schemes for Wireless Body Area Networks", IEEE Transactions on Parallel Distributed Systems, vol. 25, pp. 332-342, February 2014.

[12] R. Filsoof, A. Bodine, B. Gill, S. Makonin and R. Nicholson, "Transmitting patient vitals over a reliable ZigBee mesh network," IEEE Canada International Humanitarian Technology Conference, Montreal, QC, pp. 1-5, June 2014.

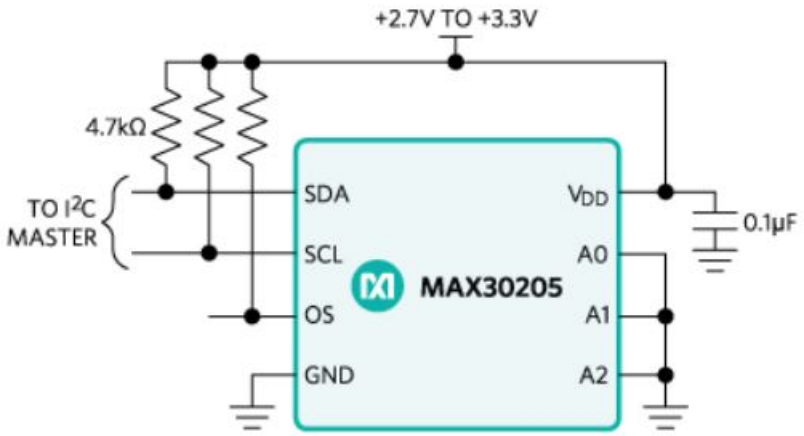
[13] Sachin S. Patil1 ,Shrenik S. Sarade2,Sagar V. Chavan, "Zigbee based sensor networks for temperature monitoring and controlling", IOSR Journal of Electronics and Communication Engineering (IOSR-JECE), ISSN: 2278-2834, ISBN: 2278-8735, PP: 66-71, March 2013.

[14] S. Y. Kanawade, Vikas Nagare, Anupam Kumar, Swapnil Dhakane, "Secured Wireless Communication Through Zigbee using Cryptography and Steganography", International Journal for Innovative Research in Science Technology, vol. 2, issue: 11, 2349-6010, April 2016.

Appendices

Appendix A

Data Sheet of MAX30205 Temperature Sensor

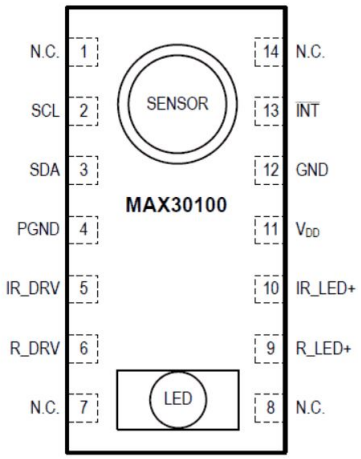


Key Features

1. High Accuracy and Low-Voltage Operation Aids Designers in Meeting Error and Power Budgets
   (a) 0.1C Accuracy (37C to 39C)
   (b) 16-Bit (0.00390625C) Temperature Resolution
   (c) 2.7V to 3.3V Supply Voltage Range
2. One-Shot and Shutdown Modes Help Reduce Power Usage
3. 600A (typ) Operating Supply Current
4. Digital Functions Make Integration Easier into Any System
   (a) Selectable Timeout Prevents Bus Lockup
   (b) Separate Open-Drain OS Output Operates as Interrupt or Comparator/Thermostat Output

Appendix B

Data Sheet of MAX30100 Pulse Oximeter Sensor

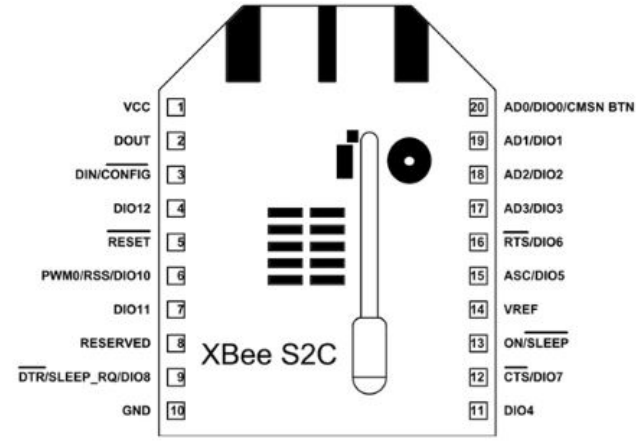


Key Features

1. The MAX30100 operates from 1.8V and 3.3V power supplies
2. Complete Pulse Oximeter and Heart-Rate Sensor Solution Simplifies Design
   (a) Integrated LEDs, Photo Sensor, and High-Performance Analog Front-End
   (b) Tiny 5.6mm x 2.8mm x 1.2mm 14-Pin Optically Enhanced System-in-Package
3. Ultra-Low-Power Operation Increases Battery Life for Wearable Devices
   (a) Programmable Sample Rate and LED Current for Power Savings
   (b) Ultra-Low Shutdown Current (0.7A, typ)
4. Advanced Functionality Improves Measurement Performance
   (a) High SNR Provides Robust Motion Artifact Resilience
   (b) Fast Data Output Capability

Appendix C

Data Sheet of XBee Module



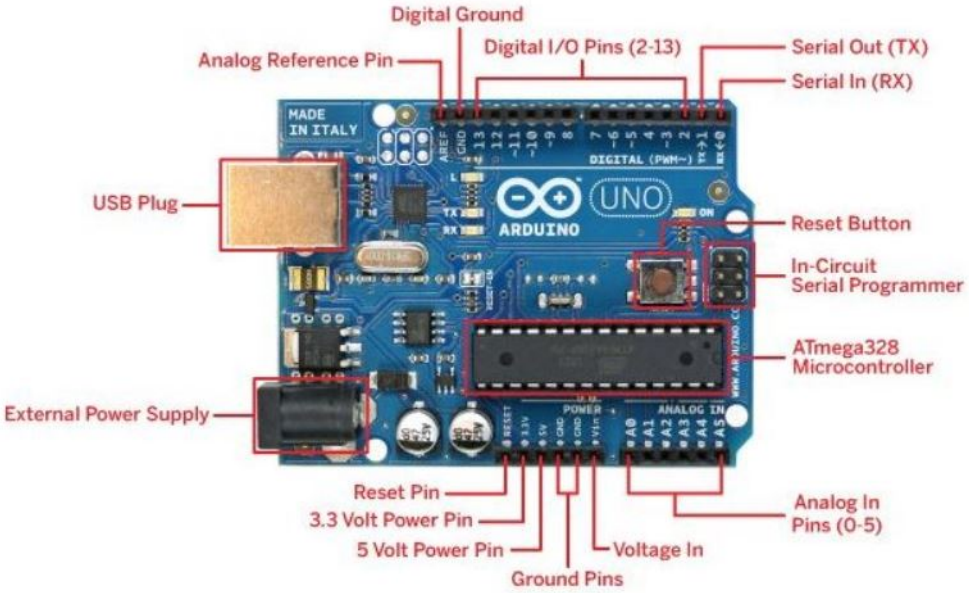
XBee S2C Module Pinout

Key Features

1. Transmission Frequency: 2.4GHz to 2.5GHz
2. Featured with UART (250 Kb/s maximum) and SPI (5 Mb/s maximum) interface
3. Outdoor RF line-of-sight Range: up to 4000ft
4. Transmit Power Output: 6.3mW (8dBm) in Boost mode,2mW (3dBm) in Normal mode
5. RF Data Rate: 250,000 bps
6. Supply Voltage Range: +2.1V to +3.6V
7. Operating Current: 33mA (at3.3V, for Normal mode) , 45mA (at 3.3V,for Boost mode)
8. Idle Current: 9mA
9. Maximum output current on all pins together: 40mA
10. Operating Temperature: -40°C to 85 C

Appendix D

Data Sheet of Arduino UNO



Key Features

1. Microcontroller: ATmega328P
2. Operating Voltage: 5V
3. Input Voltage (recommended): 7-12V
4. Inout Voltage (limit): 6-20V
5. Digital I/O Pins: 14 (of which 6 provide PWM output)
6. PWM Digital I/O Pins: 6 ,Analog Input Pins: 6
7. DC current for 3.3V Pin: 50 mA
8. Flash Memory: 32 KB (ATmega328P) of which 0.5 KB used by bootloader
9. Clock Speed: 16 MHz
10. EEPROM: 1 KB (ATmega328P)