Wireless Body Area Network using Cryptography

Brunda U S, K Sandhya, Madhurya Kulkarni G V, Navya N, Pradeep H S

Abstract: ***Network security has been great concern with recent technical advancement in wireless communication. And for that, a secured system is to be developed to provide data security over wireless transmission. This paper presents wireless body area network (WBAN) with cryptographic AES algorithm which monitors patient biomedical parameters based on sensors, Arduino and ZigBee. WBAN provides real-time measurements of patients health based on biomedical sensor. AES cryptographic algorithm is implemented for secure communication over wireless network by encryption and decryption of physiological parameters. Implementation of algorithm using Arduino has been communicated by ZigBee network to provide security to the encrypted data (cipher text) on medium cost devices. This ensures security of data for medical rehabilitation and monitoring of patients. The main purpose of this paper is to help a physician to treat patients during emergency by monitoring patients round the clock (24*7). This paper is helpful for elderly and disabled people with no assistance to measure and send the results to the doctor immediately.***

Keywords: Sensors, Biomedical Parameters, Cryptography, ZigBee, WBAN, Data Security.

I. 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]. With increment in populace, present logical sources can't satisfy predetermination human services requests of patients. Assets are limited and it's impractical for the greater part of the patients to deal with their wellbeing for a long-term period by staying in a medical clinic because of money related guidelines, work, and different reasons. Consequently, to give the status of their wellbeing, this must be observed. The characteristics of the WBAN radio propagation are dynamic due to the motions of the human body. The objective of the proposed system is:

- To adopt the ZigBee technology and protocols which satisfy the requisites 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 like: Hospital, Physician) using AES algorithm.

The system aims at helping the medical practitioner to understand the patients' issues within a period of time securely. As a result, wireless tracking scientific structure will become a part of cell healthcare facilities with real-time tracking in the future. In this context, WBAN supporting healthcare applications can over valuable contributions to improve patient healthcare, including diagnosis and/or therapeutic monitoring. In a small span of time, WBAN technology has taken its rest steps in the medical rehabilitation and monitoring of patients. This paper is organized as follows: previously published related works are discussed in section II. The proposed design of the model is presented in section III. Section IV discusses the design implementation. Section V discusses the results of the work. In section VI work is concluded.

II. RELATED WORK

WBAN architecture can be implemented by using several wireless communication algorithms as: Wi-Fi, Bluetooth, ZigBee, and WiMax etc. Since 2003, Al-Riyami and Peterson first proposed a new public key cryptography named certificateless public key cryptography. Since then, certificateless encryption is used in many cryptography fields. In 2014, Jingwei Liu et al. proposed a certificateless cryptography based remote anonymous authentication protocol which efficiently saves the computation resource. In 2014, Debiao He et al. proposed a cloud assistant based certificateless auditing scheme for WBANs that can provide protection of data integrity. In 2015, Hu Xiong et al. [1] present a certificateless encryption scheme and certificateless signature scheme, then they build a revocable certificateless anonymous and remote authentication scheme based on the basic of CLE and CLS for WBANs. The advantages of certificateless scheme are solving the key escrow problem, but it may automatically cause computation and resource limited issues in WBANs. In the [3] system, it proposes a security and efficiency authentication protocol for WBANs. The IEEE 802.15.4 standard for low power ZigBee protocol indicates a transmission power output of 0 dBm (1 mW). Continuous operation at the maximum data rate of 250 kb/s generally consumes a normal Lithium ion battery in a matter of hours. It is evident that new

Revised Manuscript Received on May 08, 2020.

* Correspondence Author

Brunda U S, Electronics and Communication Engineering, SIT, Tumakuru, Karnataka. Email: bestus0508@gmail.com

K Sandhya, Electronics and Communication Engineering, SIT, Tumakuru, Karnataka. Email: ksandhya1298@gmail.com

Madhurya Kulkarni G V, Electronics and Communication Engineering, SIT, Tumakuru, Karnataka. Email: madhuryakulkarni@gmail.com

Navya N, Electronics and Communication Engineering, SIT, Tumakuru, Karnataka. Email: navya.26699@gmail.com

Pradeep H S, Assistant Professor, Electronics and Communication Engineering, SIT, Tumakuru, Karnataka. Email: pradep.hs@gmail.com

approaches to ultra-low power wireless technology are required for improving next generation WBAN technology [4].

III. PROPOSED DESIGN METHODOLOGY

WBAN architecture establishes communication between the WBAN client and application providers i.e., hospital and physician as shown in Fig.1. WBAN includes wearable sensors, biosensors or a portable medical device [5].

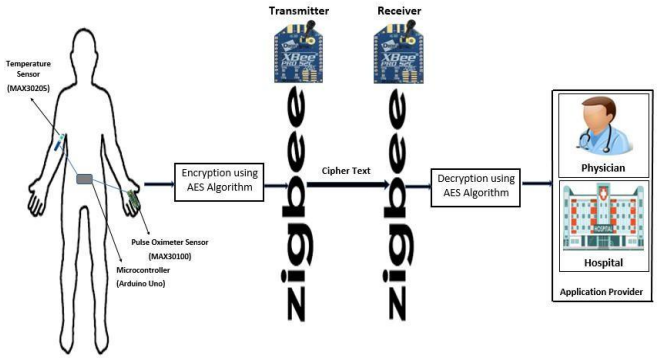

Fig.1: Block diagram of the proposed system

A. *On Body Sensors*

These sensors are non-invasive sensors that can be directly placed on the skin of the patient or direct contact with the body [6]. In the project, Temperature and Pulse Oximeter Sensors are considered in order to gather body temperature, pulse rate and oxygen saturation of the patient for real-time monitoring of patient health status by consultant physician.

Temperature Sensor (MAX30205):
The digital temperature sensor (as shown in Fig.2) has an accuracy of 0.1ºC over the range of 37ºC to 39ºC with resolution of 16 bits (0.00390625ºC). One-Shot and Shutdown Modes helps to reduce power usage. MAX30205 converts temperature measurements to digital form using a high- resolution, sigma-delta, analog-to-digital converter (ADC). The sensor with a lockup-protected I2C-compatible interface that makes it ideal for medical applications.

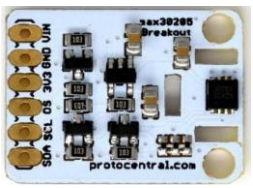

Fig.2: MAX30205 Temperature Sensor

In the proposed design, MAX30205 Temperature sensor attached to the patient body arm is interfaced with microcontroller which sends continuously temperature data through ZigBee in terms of ºF. Serial Data line (SDA) is a bidirectional pin transfers the data, which happens with respect to unidirectional Serial Clock line (SCL) pin reading the content of the temperature register through SDA.

Pulse Oximeter Sensor:
Maxim Integrated MAX30100 Sensor (as shown in Fig.3) is used to monitor pulse rate and oxygen concentration of a patient. To detect pulse oximetry and heart rate signals, it combines two LEDs, a photodetector, optimized optics and low noise analog signal processing. It operates from 1.8V to 3.3V power supply. The MAX30100 sensor is attached to the finger which sends small beams of light pass through the finger, measuring the amount of oxygen. It measures through changes in light absorption in oxygenated and deoxygenated blood. The pulse rate is determined by knowing the duration between increase and decrease of oxygenated blood. The device has two LEDs i.e., emitting red light and infrared light. Heart rate signals can be detected by only infrared light whereas both red and infrared light is required to measure blood oxygen levels.

Fig.3: MAX30100 Pulse Oximeter Sensor

In the proposed design, MAX30100 Pulse Oximeter sensor attached to the finger of patient is interfaced with an Arduino microcontroller which sends continuously pulse rate in terms of beats per minute (bpm) and oxygen saturation in terms of percentage (%). The main function of MAX30100 is, it reads absorption levels for both light and store them in buffer that can be read via I2C serial communication [7].

B. *Arduino Microcontroller*

Arduino ATmega328 (as shown in Fig.4) is an 8-bit AVR microcontroller that combines 32KB ISP flash memory with read-while-write capabilities. It has 20 digital input/output pins (of which 6 can be used as PWM outputs and 6 can used as analog inputs), a 16MHz resonator, USB connection, power jack, an In Circuit System Programming (ICSP) header and a reset button [8]. The device operates between 1.8V-5.5V. The Arduino microcontroller is programmed using a dialect of features from the programming languages C and C++ which provides an integrated development environment (IDE) based on the processing language project.

Fig.4: Arduino ATmega328 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.

ZigBee Wireless Network

ZigBee is an IEEE 802.15.4-based specification for a suite of high-level communication protocols. ZigBee (as shown in Fig.5) is a low data rate wireless ad hoc network. ZigBee has an advantage of reliability, long lasting battery life, unlimited network size when compared to other wireless standards. The frequency range supported in ZigBee mostly 2.4 GHz worldwide whose data 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 Arduino ATmega328 microcontroller.

Fig.5: ZigBee Module

In the proposed system, 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 [9]. The ZigBee range of transmission is over 10-100 meters which can transmit data over long distances by passing data through a mesh network of intermediate devices to reach more distant ones.

C. *Cryptographic Algorithm*

Cryptography is a technique for securing the secrecy of communication. In the system, Advanced Encryption Standard (AES) cryptographic algorithm is used to secure the data. As Data Encryption Standard (DES) started becoming vulnerable to brute force attacks, AES came into existence. AES has an advantage of implementing in both hardware and software to secure sensor data. It is the only cipher which is publicly accessible and is approved by National Security Agency (NSA) when it was used in an approved cryptographic module.

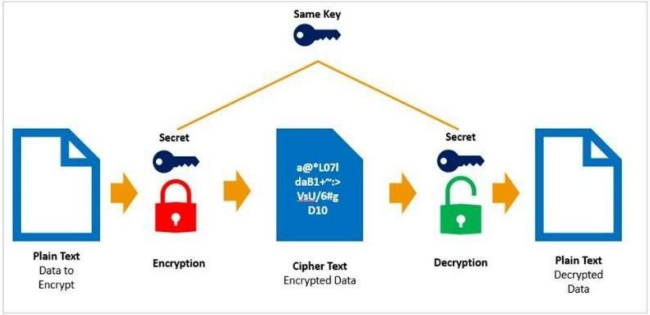

Fig.6: Symmetric Encryption

It is a symmetric block cipher (as shown in Fig.6) which uses a key size of 128/192/256 bits in order to encrypt and decrypt the data in blocks of 128 bits. This algorithm defines a many number of transformations where number of rounds is determined by the key length, i.e., 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, 14 rounds for 256-bit keys. While comparing 256-bit key and 128-bit key, the 256-bit key is more difficult for brute force attacks, but when power is an issue and where delay is considered, 128-bit keys are likely to be a better option. Because, 256-bit keys require more processing power. AES has built-in flexibility of key length, which allows a degree of 'future-proofing' against progress in the ability to perform exhaustive key searches. It is an iterative algorithm based on 'substitution-permutation network' [10] as shown in Fig.7.

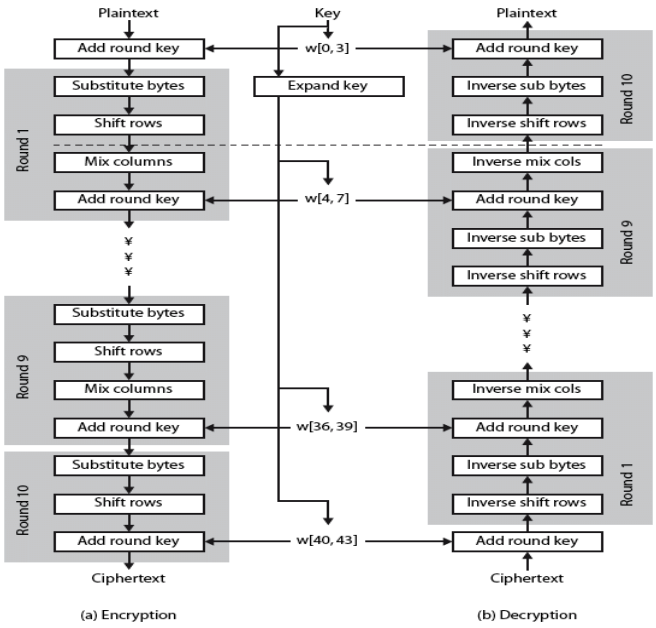

Fig.7: AES Key Generation

AES treats 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 [11]. 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 [12]. In the current scenario, the collections of health parameters are time- consuming that are reduced by theses wearable devices. It is associated with data security given to those contents using the cryptographic algorithm, which in turn helps to keep the person in isolation state by making their details confidential. Enormous development in technology allows anybody to get access to these data if they are unmasked (or in raw form), therefore by including the securing technique can enhance its vitality with enrich hospitality at the client's place itself.

IV. IMPLEMENTATION OF DESIGN

The implementation of the proposed system comprises a Temperature Sensor, Pulse

Oximeter Sensor, Arduino and ZigBee 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 Fig.8.

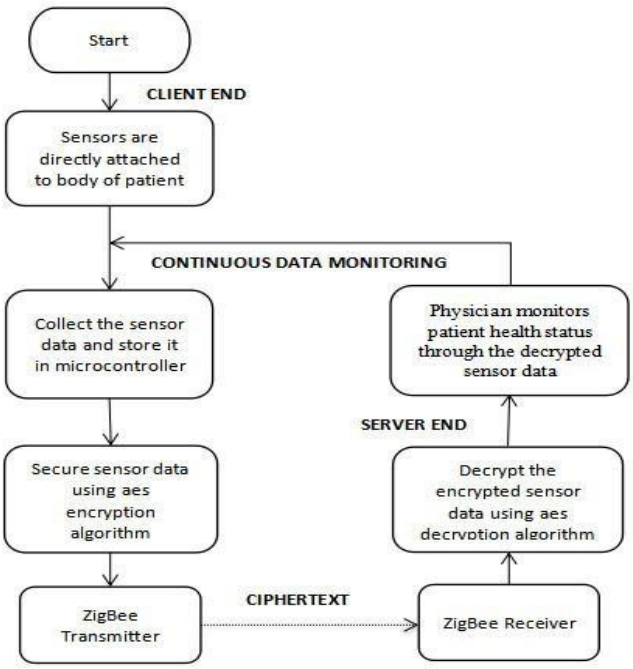

Fig.8: Design flow of the proposed system

At the clients 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 [13]. The data stored in Arduino is encrypted into unusual formal (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 servers end:

The receiver ZigBee holds the transmitted ciphertext which is decrypted using AES decryption algorithm in Arduino [14]. The decrypted data (original data) is monitored by physicians about patients' health status.

V. EXPERIMENTAL RESULTS

The results obtained by encrypting the health details using AES at WBAN client and received information is decrypted to get back the original data at the Application provider for analysis. Here the table includes the data to be transmitted, i.e. patient details in a string format. The cryptographic 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 as shown in Table 1. 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. name of the patient; address etc. will be reflected at the transformed data visuals.

Table 1: Represents the data notation received from sensors and during transmission of encrypted data

Conditions	Plaintext or Sensor data	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}	iOlkSbTBvChNphdMmns/6d5hLGICh957qopkBeJT7dGb QaXdr7z/blgBKg1SML1w
		{ 0x2B, 0x7E, 0x15, 0x16, 0x28, 0xAE, 0xD2, 0xA6, 0xAB, 0xF7, 0x15, 0x88, 0x09, 0xCF, 0x4F, 0x3C}	dBw+H6dxRpz4sAx20bigyotl5UFcQgiuc0yDug2KWSoA ZXeFvNOv7rvVtlqaEVpJ
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+gChfOukqf51MXspNSlvcsu7QY7P0wv PD0/nzpukXuPVQe+GX5gKi
	Temp: 85'F Rate: 78bpm Oxirate: 95%		iOlkSbTBvChNphdMmns/6d5hLGICh957qopkBeJT7dGb QaXdr7z/blgBKg1SML1w

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 2 for the same data mentioned in above table.

Table 2: The data collected from the ZigBee and converted to raw data at the receiver side

Conditions	Ciphertext (Encrypted data Received by Application provider)	Cryptographic key (16 bytes)	Decrypted data (original data or plaintext)
Same input, different keys	iOlkSbTBvChNphdMmns/6d5hLGICh957qopkBeJT7dGb QaXdr7z/blgBKg1SML1w	{0xB2, 0xE7, 0x51, 0x61, 0x82, 0xEA, 0x2D, 0x6A, 0xBA, 0x7F, 0x51, 0x88, 0x90, 0xFC, 0xF4, 0xC3}	Temp: 85'F Rate: 78bpm Oxirate: 95%
	dBw+H6dxRpz4sAx20bigyotl5UFcQgiuc0yDug2KWSoAZ XeFvNOv7rvVtlqaEVpJ	{ 0x2B, 0x7E, 0x15, 0x16, 0x28, 0xAE, 0xD2, 0xA6, 0xAB, 0xF7, 0x15, 0x88, 0x09, 0xCF, 0x4F, 0x3C}	
Different inputs, same key	BwyWDAxyJ8N+gChfOukqf51MXspNSlvcsu7QY7P0wvP D0/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%
	iOlkSbTBvChNphdMmns/6d5hLGICh957qopkBeJT7dGb QaXdr7z/blgBKg1SML1w		Temp: 85'F Rate: 78bpm Oxirate: 95%

VI. CONCLUSION

In this project a WBAN system has been developed to provide clinical health care and medical assistance in rural and remote areas using the ZigBee technology and cryptography. The system will enable the patients at remote places to extend their well-being with handy instruments. Eventually, consulting physicians having the 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 collected data even at distant places on time. Along with the continuous monitoring, the system includes cryptographic techniques so there will be no problem data theft incorporates in healthcare.

REFERENCES

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 Certificateless 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. H. Deng3, “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: 2278-8735, 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, 23499-6010, April 2016.

AUTHORS PROFILE

Brunda U S, studying 8th sem, Electronics and Communication Engineering in Siddaganga Institute of Technology, Tumakuru. She has done Home automation project on IoT. She developed a GUI using pyqt5, done project on firebase database and worked on Machine learning and Image processing concepts.

.

K Sandhya, studying 8th sem, Electronics and Communication Engineering in Siddaganga Institute of Technology, Tumakuru. She has done Waste Management project based on Embedded Systems and Tracking System of Luggage based on IoT using firebase database.

Madhurya Kulkarni G V, studying 8th sem, Electronics and Communication Engineering in Siddaganga Institute of Technology, Tumakuru. She has done Home automation project based on IoT and Smart Wardrobe Management System project based on IoT

Navya N, studying 8th sem, Electronics and Communication Engineering in Siddaganga Institute of Technology, Tumakuru. She has done Home automation project based on IoT and developed some API’s in Golang and .net which integrates with database (mongo db). She also worked on Swagger project.

Pradeep H S, is working as Assistant Professor in the Department of ECE in Siddaganga Institute of Technology, Tumakuru. He has more than 12 years of teaching experience. His area of research is Antennas & Microwave Engineering.