An IoT-Based Body Area Network in Medical Care System: Related Challenges and Issues

Shaik Jhani Bhasha, Sunita P

Abstract*: *The Internet of Things (IoT) is the collection of open intelligent devices. The fast development of IoT and the huge expansion of mobile technology are unveiling fresh growth opportunities in several areas, including education, transport, and farming and, in particular, healthcare. Introduction of IoT via medical applications has several advantages including cost savings by dropping hospital costs, health care costs, and transportation costs, costs of human resources and costs of insurance. Recently, the academic world has produced major progress in research and security development for IoT-based applications, particularly on IoT-based healthcare devices. It contributes to an additional benefit of enhanced healthcare quality. However, the increased use of IoT facilities in e-health applications, particularly in the insurance field, has resulted in increased security and privacy issues. Medical applications are prone to data violations and widening security problems due to the increase in access points to sensitive data through electronic medical records and the increasing popularity of wearable technology. So there is a need of an efficient lightweight, secure verification system, providing important security levels against various attacks, such as attacks by impersonation, a man in the middle attack and unidentified key-sharing attacks for IoT foundation E-health. This article presents a survey of problems, difficulties, and challenges a short analysis of multiple problems and problems suggested by different authors using different techniques and methods.

Index Terms*: *Authentication, Light weight, IoT, medical care system, Wireless body area network

I. INTRODUCTION

In recent days, the growth of wireless communications, portable medical devices brought about tremendous changes for business, industry, science, and engineering. As shown in figure 1 provide complete details of the integration of sensors connected to the patient who resides inside or outside the hospital can be monitored and their data can be sent with the assistance of wireless body area network. By connecting all the sensors, computers, through low-power body area network wireless by taking help of internet improves the efficiency of the system. To improve further services in the medical organizations, the IoT caters important role to ensure of gathering the human medical data that can be used to know the patient condition to all the family members, friends and doctors as well who are staying at remote places through wireless from anywhere across the globe with the help of internet [1–4]. As mentioned earlier the primary work of modern healthcare organizations to collect body sensors data periodically from the patients to be monitored and sends their data through wirelessly for further investigation personnel, enabling professional doctors and medical staffs checking rigorously for health issues of patients in instantaneous and providing patients with appropriate medical care and medical treatment.

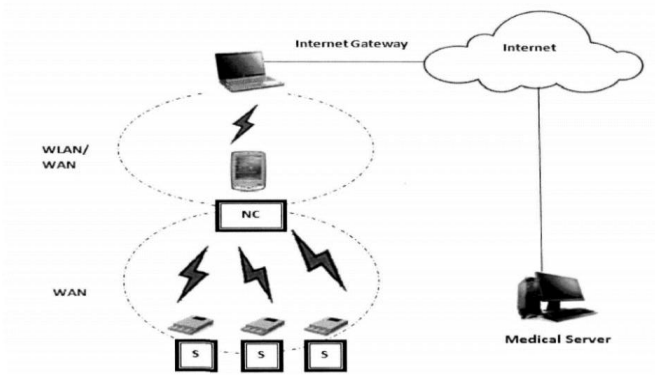

Figure 1. Overview of a WBAN

Figure 2 shows the latest developments in healthcare [5]. A significant trend is a facility for cost-effective relationships through seamless and secure communication between individual clients, hospitals and educational institutions. Modern wireless-driven healthcare networks are anticipated to help chronic diseases, early diagnosis, real-time surveillance, and medical emergencies.

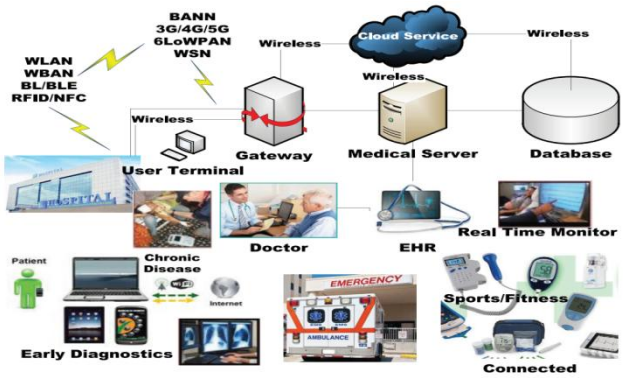

Figure 2. Overview model of Healthcare trends

Gateways, health servers, and databases play an important role in generating health records and providing approved investors with on-demand healthcare facilities. An important trend associated with IoT responsible for the creation of innovative and efficient resources used in medical association and its applications, to maintain more secure protocols and for future applications.

Revised Manuscript Received on November 05, 2019.

Shaik Jhani Bhasha, Research Scholar in GITAM Deemed to be University, Bengaluru, and working as Assistant Professor, Dept. of ECE, GITAM Deemed to be University, Hyderabad, India.

Dr. Sunita P, Assistant Professor, Department of ECE, GITAM Deemed to be University, Bengaluru, India.

In fact, strategies and instructions were created in numerous nations and organizations worldwide to deploy IoT technology in the medical sector. This paper examines the developments in IoT health studies and identifies numerous queries that need to be resolved in order to adapt IoT healthcare systems. This paper provides an insight into the security and privacy problems of IoT health alternatives by conducting an IoT-based study of the IoT facilities and applications.

II. OVERVIEW OF E-HEALTHCARE SYSTEMS GROUND WORKS

A typical eHealthcare system [6] architecture comprises four layers as illustrated in Figure 3. More details are provided in each layer of this architecture. A set of sensor devices running on a wireless network are integrated into the BAN layer (layer 1). In this layer, sensor nodes are designed to arrange on the patient body so-called as on-body sensors, similarly some sensors under the patient skin so-called in-body sensors.

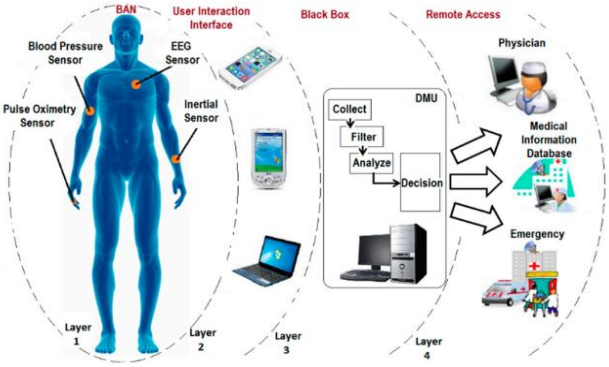

Figure 3. Typical 4-layer model for Healthcare

These sensors are constantly capturing and relaying vital parameters. However, information can involve low-level on-tag handling before delivery, based on the functionality and computation abilities of nodes. Initially, the gathered information can be either relayed to a central body coordinator or transferred straight to the top layers for further processing. In off-body communication, the necessary energy for transmission by a sensor node is primarily based on several variables like body path loss (BPL), received noise figure (RNF) and a signal-to-noise ratio (SNR).

III. RELATED WORKS

The developing of the IoT towards on-body low power brought about tremendous changes for healthcare industry, science and engineering. In this section, we address the influence of IoT on wireless body area network in domestic applications. The simplified model with low-power consuming intra-body communication with highly feasible scheme is shown in Figure 4. This model associated with the more secure protocols makes reliable and high speed intra-body communication. IBC-based sensor systems pass the health data to a central coordinating unit through the body. This central coordination unit is responsible for creating connection among patient body appliances and a base station (BS). This makes it possible to move the gathered information to a base station using one of the existing low-power communication protocols.

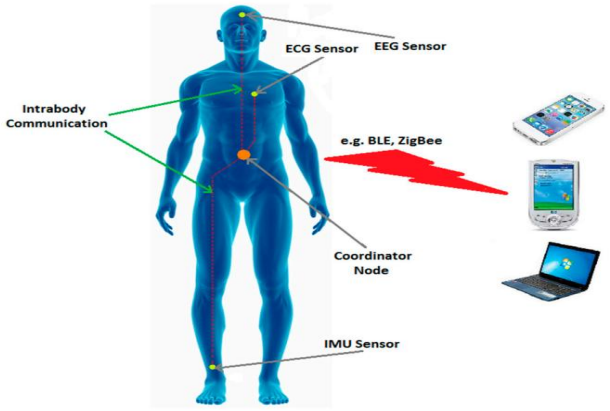

Figure 4. Intra-body communications united Intra-body communications shared with existing low-power protocols

In [7], the authors discussed the main inspiration behind the innovation is to reduce the workload in doctor's facilities and provide competent health services. For this purpose, different body sensors are used for physical monitoring of the patient's physical parameters such as electro-cardiograms, heart rate, blood pressure, and body temperature, and the continuous monitoring of their condition using the wireless sensor network (WSN) in conjunction with Internet of Things (IoT). The data on health parameters are also sent via the wireless technology module such as the Zigbee module (S2 module) and Internet cloud computing to medical personnel.

In [8], the authors present a novel system for real-time personal health monitoring: WISE (Wearable IoT cloud-based health surveillance system). In help of real-time health surveillance, WISE is adopting the BASN (bodily region sensor network) model. Several wearable sensors, including heartbeat, body temperature, and blood pressure sensors, have been incorporated. Second, most wearable health monitoring systems require a smartphone, which affects the normal daily use of a smartphone, as data transmission, visualization, and transmission gateways. While in WISE, data from the BASN are transmitted directly to the cloud and a lightweight wearable LCD can be integrated as an alternative for quick viewing of the data in real-time.

Because of the IoT and privacy features, the addressing of the major issues in the present intelligent health care scheme. The prototype scheme was then intended and finished depending on a lightweight, private holomorphic matrix and a DES encryption scheme. Finally, they intended and finished a prototype scheme centered on software and hardware. Also there is a web-based IoT sensor system for the monitoring of the biological data of the elderly and other private information relating to electronic box, electronic registration, stamp and time-stamp processes, and asymmetric encryption technology. The suggested system could provide more versatile and precise medical delivery and reduce expenditure. For cloud-assisted WBAN system use expanded chaotic maps for a secure verification system. The system secure agreement grounded on the well-known algorithm Diffie-Hellman scheme that provides the scheme respondents with secure methods or routes for registration. Before transmission, evaluated health items gathered from body WBAN sensors would be encrypted.

Table 1 Summary of IoT based healthcare availability techniques

S.No.	Authors	Findings	Merits	Algorithm/Technology used
1.	Authors in, [13]	Accommodated standard authentication and key agreement scheme that consumes low power that serves IoT services.	Maintaining user secrecy, with stand to user synchronization issue easily.	Uses the XOR operations, hash operations, and only four elliptic multiplications.
2	Authors in, [14]	In order to rectify the security, an algorithm is proposed named as "ESHCMA: Enhanced Secure Health Care Monitoring Algorithm using One-Time Password in Wireless Body Area Network.	Maintains user integrity by generating password. It gives high security with less key length compared to existing algorithms.	Elliptic Curve Cryptography (ECC) key generation technique.
3	Authors in, [15]	It proposes a sensor (or sensor tags) based communication architecture for future IoT based healthcare service systems.	Medicine error prevention and patient safety can thus be guaranteed.	It introduces a coexistence scheme for proving the correctness of the coexisting medical items for which the ultra-low-cost IoT based sensors, such as passive RF tags, are utilized.
4	Authors in, [16]	It proposes a secure lightweight authentication scheme for the wireless body area networks. With this scheme, forward secrecy can be guaranteed without using asymmetric encryption.	Lower security risk, computational cost	It uses the efficient Lightweight Mutual Authentication and Key Agreement Scheme to verify the security and analyze informal security.
5	Authors in, [17]	To maintain and ensure high secure against several attacks uses mutual authentication approach. Another purpose of providing security to body area sensors with lightweight protocols.	Capable of providing and maintenance of efficacy in case of WSN and Mobile gadgets, it also provides better anonymity of the WBAN users.	Auto recovery and self-healing methods are designed against several active and passive attacks.

Table 2 Summary of Authentication efficiency techniques

S.No.	Authors	Findings	Merits	Algorithm/Technology used
1.	Authors in, [18]	Constructed a mechanism that assists patient who are in in emergency without need of medical consultants.	Reduce the time period of the verification in case of emergency.	An identity-based fast authentication scheme is proposed.
2	Authors in, [19]	Uses Protocol between controller node and sensor nodes in different situations.	It supports more computation speed and less communication overhead.	BAN logic formal verification tool has been employed in aid design of 3PAKE protocol for authentication and security verification.
3	Authors in, [20]	The carried out work detects quickly input constraints during the initial stage of user login process, also cancel lost card for future use.	Less overhead, maintains higher efficiency and more speed for medical care systems.	Integration of secure identity and chaotic maps that relies majorly on key authentication process
4	Authors in, [21]	For the sake of providing privacy to user against password threats and data leakage attacks, the scheme uses data encryption for IoT based healthcare systems.	Efficient reduction in case data redundancy in implemented protocol stack design.	It uses User Authentication and User Anonymity Scheme with Provably Security.
5	Authors in, [22]	The user authentication system presented is extremely useful method for providing access with more secure manner.	Selectivity is combined with group authentication in IoT environments.	It uses Selective Group Authentication Scheme

With this, the user can access the medical services from the cloud in a more secure manner that enhances the patient caretaking that changes lives to promote real-time analyzes through ongoing remote monitoring for stream-oriented health products. In [9] the writers suggested a sharp IOT structure for medical facilities. They designed to provide medical facilities anywhere using a remote sensor that can reduce distinct obstacles and improves access to restaurant administrations. It is also used to save a life in vital healthcare and emergencies within metropolitan regions and urban networks. The company's basic favorable position is the use of distant body sensor innovation that reduces the risk of wired technology.

The primary system unit is the Wearable Body Area Sensor Network (WBASN), the Automated Intelligent Central Node (AICN), and Sink, the Cloud-based Central Server (CICS), respectively. In [10]. WBASN is made up of two closed source electronic panels, the mobile cover Arduino Leonardo and Arduino Yun and three medical sensors are attached to the patient. The devices collect their suitable data and communicate that information via a wireless hotspot interaction mechanism to the Automated Intelligent Central Node (AICN). The devices include heart rate sensor, heat sensor, and Galvanic Skin Response detector use the AICN cellular hotspot protocol. The mobile phone is a route to the middleware dump and the mobile working software agent gathers information from the sensors and gives the user account to the cloud-based Central Server (CICS), a Web-based 3G-network application. The proposed scheme is useful in the previous identification of diseases, the continuous monitoring of human health and improved portable planning between clients and healthcare consultants.

In [11] the authors use the health surveillance scheme structure that can be implemented not only to android applications but also to other portable environments. The scheme utilizes the biomedical data in BSN to monitor healthcare as well suggested implementation case study is conducted in the field of athletics (football matches). This scheme consists of wearable machines, biosensors, and cloud for processing and portable environments to extract monitoring information. The communication between the wearable and the different sensors takes place via Bluetooth and, for a broad range of communications, between wearables and remote devices, WLAN Standard 802.11 is used in the next generation. The paper describes in detail how the information is transmitted and the structure for correct data transmission in the medical implementation.

In [12], the authors proposed a health-care system using the Body Sensor Network, a lot of bio-sensors are connected to the central core unit LPU (the local processing unit) that operates as an intermediate between the BSN and the BSN central server data are sent securely through OCB-authenticated mode.

IoT Threat Model

IoT health equipment and networks, due to the enhanced attack region, are susceptible to security attacks. In the first case, the extension of networks, cloud networks, and cloud facilities is included. The second situation involves more communication between IoT, networking, cloud, and applications. The final one involves hardware and software constraints in the device.

IV. IoT HEALTHCARE SYSTEM

In addition, this paper presents a survey of issues, challenges, provides a brief study of different challenges and issues that are proposed by various authors by using especially different security techniques and methods.

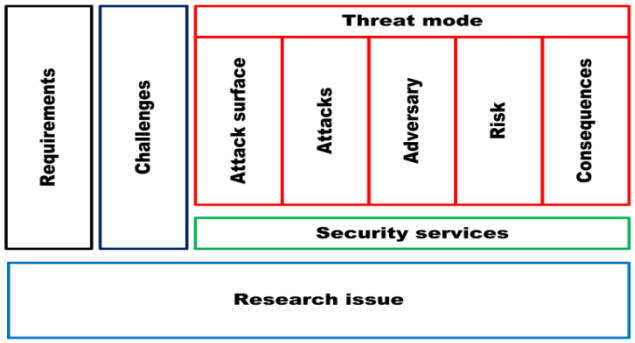

Figure 5. Security issues in IoT-based health care

Table 3 Summary of challenges with parameters towards IoT

Challenges	Energy Efficiency	Reliability	QOS	Availability	Security& privacy	Resource utilization	Fault tolerance	Replication	Bandwidth	Cost	Performance	Throughput	Overhead	Integrity	Flexibility	Authentication	Repudiation	Confidentiality	Time	Scalability
Availability	✓		✓				✓	✓	✓	✓			✓							
Energy Efficiency			✓				✓		✓		✓									

Load Balancing		✓				✓				✓	✓	✓	✓						✓	✓
QOS	✓	✓		✓	✓					✓	✓		✓	✓					✓	
Resource Allocation						✓			✓	✓	✓				✓				✓	
Security &Privacy										✓	✓			✓	✓	✓	✓	✓	✓	✓

To facilitate the full acceptance of the IoT in the healthcare domain, it is critical to identify and analyze distinct features of IoT security and privacy, including security requirements, vulnerabilities, threat models, and countermeasures, from the healthcare perspective as in Figure 5. The prerequisites of IoT in the field of medical care for security are similar to the commercial availability of communication protocols. So it is mandatory to concentrate on the parameters to be considered with their present challenges as listed in the Table 3. As shown in the figure 6 discriminating rate of 2-anonymity for various *K*-anonymity for investigation of how the dataset is distributed related to discriminating rate for analyzing the level of security in case of attacks.

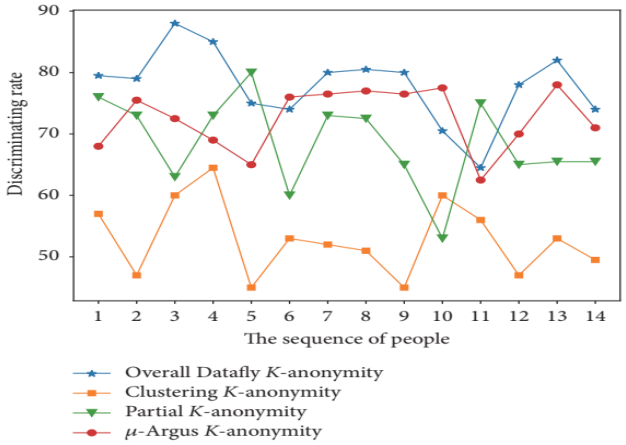

Figure 6. The discriminating rate of 2-anonymity

It is evident that the discrimination level of 2-anonymity clustering is comparatively low. We can thus say that the 2-anonymity clustering would be the secure technique among the four techniques regarded.

V. CONCLUSION

From the literature investigated, it has been found that WBANs are an outstanding tool to remotely monitor patient information and tremendously appropriate for both medical and e-healthcare. The techniques that allow these WBANs are cutting edge, as they generally apply to WSNs. Safety including privacy, security and energy efficiency are the main issues for WBANs, and these regions offer a wide range of study options. Many works focus on the security element of WBANs and a lot of work has been undertaken to enhance accuracy. However, not much has been performed to fix the security and maintenance issues. Energy effectiveness has not been regarded and its suitability for WBANs is uncertain in the suggestions that address both the issues. In this paper, we therefore tackle all of the issues mentioned above, bringing into account the background in which these schemes are implemented. Although medical background is important, the scheme suggested so called lightweight, secure verification in this paper is relevant to any WBAN used for any intent.

REFERENCES

1. Chiou, S.Y.; Ying, Z.; Liu, J. Improvement of a privacy authentication scheme Based on cloud for medical environment. J. Med. Syst. 2016, 40, 101.
2. He, D.; Kumar, N.; Chen, J. Robust anonymous authentication protocol for healthcare applications using wireless medical sensor networks. Multimed. Syst. 2015, 21, 49–60.
3. Xin Liu,Ruisheng Zhang, Qidong Liu; A Temporal Credential-Based Mutual Authentication with Multiple-Password Scheme for Wireless Sensor Networks, special issue Climate Change And Health, January 2017.
4. Li, C.T.; Lee, C.C.; Weng, C.Y. A secure cloud-assisted wireless body area network in mobile emergency medical care system. J. Med. Syst. 2016, 40, 117.
5. K. Vasanth and J. Sbert. Creating solutions for health through technology innovation. Texas Instruments. [Online]. Available: http://www.ti.com/lit/wp/sszy006/sszy006.pdf, accessed Dec. 7, 2014.
6. University of Bristol. SPHERE 2015. Available online: http://www.irc-sphere.ac.uk/about
7. M. H. Riaz, U. Rashid, M. Ali L. Li, "Internet of Things Based Wireless Patient Body Area Monitoring Network", 2017 IEEE International Conference on Internet of Things (iThings), : 970-973.
8. Jie Wan , Munassar A. A. H. Al-awlaqi, MingSong Li, Michael O'Grady, Xiang Gu, Jin Wang and Ning Cao, "Wearable IoT enabled real-time health monitoring system", EURASIP Journal on Wireless Communications and Networking, Dec 2018.
9. FarahNasri, Adel atif Mtibaa." Smart Mobile Healthcare System Based on WBSN And 5G," International Journal of Advanced Computer Science and Applications, Vol. 8, No. 10, 2017.
10. OlutayoBoyinbode." A Cloud-Based Body Area Sensor Network Mobile Healthcare System," International Journal of Advanced Research in Computer Science and Software Engineering Volume 7, Issue 5, May 2017.
11. Higinio Mora ID, David Gil ID, Rafael Muñoz Terol D, Jorge Azorín, D AndjulianSzymanski." An IoT-Based Computational Framework for Healthcare Monitoring In Mobile Environments, "Sensors 2017.
12. Kavitha.Y, Lavanya.M, Mounika.A, Sasirekha.KN.VignaVinod Kumar." A Secure IoT-Based Modern Healthcare system Using Body Sensor Network," International Journal Of Innovative Research In Science, Engineering And Technology, Volume 6, Special Issue 3, March 2017.

13. Yuwen Chen, Lourdes López, José-Fernán Martínez, and Pedro Castillejo, "A Lightweight Privacy Protection User Authentication and Key Agreement Scheme Tailored for the Internet of Things Environment: LightPriAuth", Journal of Sensors, September 2018.
14. V.Sethupathi and E.George Dharma Prakash Raj, "ESHCMA: Enhanced Secure Health Care Monitoring Algorithm using One-Time Password in Wireless Body Area Networks", International journal of Computer Science & Network Solutions Jun.2016-Volume 4.No.6.
15. Jia-Li Hou and Kuo-Hui Yeh, "Novel Authentication Schemes for IoT Based Healthcare Systems", International Journal of Distributed Sensor Networks, August 2015.
16. Zisang Xu , Cheng Xu1, Wei Liang, Jianbo Xu, and Haixian Chen, "A Lightweight Mutual Authentication and Key Agreement Scheme for Medical Internet of Things", IEEE Transactions, volume 7, 2019.
17. Chien-Ming Chen, Bing Xiang, Tsu-Yang Wu, and King-Hang Wang' "An Anonymous Mutual Authenticated Key Agreement Scheme for Wearable Sensors in Wireless Body Area Networks", Appl. Sci. 2018, 8, 1074.
18. Chen Wang, Wenying Zheng, Sai Ji, Qi Liu, and Anxi Wang, "Identity-Based Fast Authentication Scheme for Smart Mobile Devices in Body Area Networks", Wireless Communications and Mobile Computing, August 2018.
19. Jingwei Liu, Qian Li, Rui Yan and Rong Sun, "Efficient authenticated key exchange protocols for wireless body area networks", EURASIP Journal on Wireless Communications and Networking (2015) 2015:188.
20. C.-T. Li, C.-C. Lee, C.-Y. Weng, and S.-J. Chen, "A secure dynamic identity and chaotic maps based user authentication and key agreement scheme for e-healthcare systems," Journal of Medical Systems, vol. 40, no. 11, article 233, 10 pages, 2016.
21. C. Li, T. Wu, C. Chen, C. Lee, and C. Chen, "An efficient user authentication and user anonymity scheme with provably security for IoT-based medical care system," Sensors, vol. 17, no. 7, 1482, 18 pages, 2017.
22. Y. Park and Y. Park, "A selective group authentication scheme for IoT-based medical information system," Journal of Medical Systems, vol. 41, no. 4, article 48, 8 pages, 2017.

AUTHORS PROFILE

Shaik Jhani Bhasha is presently working as Assistant Professor in the department of Electronics and communication Engineering, GITAM Deemed To be University, Hyderabad Campus. He has 19 years of teaching experience. He is presently doing his research in the field of medical IoT. His areas of interests include Embedded Systems, mobile ad-hoc networks and IoT.

Dr. Sunita Panda is presently working as Assistant Professor in the department of Electronics and communication Engineering, GITAM Deemed To be University, Bengaluru Campus. She has published many research papers in national and international journals, having 15years of experience in the field of teaching, research. Her area of interest include soft computing, Channel equalization, Digital Signal processing, antennas, IoT etc.