7th National Conference on
"Role of Engineers in Nation Building" organized by VIVA Institute of Technology, Mumbai
(1st and 2nd March 2019)
International Journal of Engineering Research & Science (IJOER)
ISBN: [978-93-5321-411-1] ISSN: [2395-6992] [Vol-5, Issue-3, March- 2019]

Human Body Sensor Network (BSN): An IOT Application

Aniket Tare[1], Prof. Neha Lodhe[2]

Department of MCA, University of Mumbai, Mumbai, India.

Abstract— *In this paper, we explore the use of IOT based application for Healthcare System. Human health is conscious for normal as well as abnormal conditions; hence, we need to store data somewhere, which will be easily access from anywhere, so the IOT helps the data to be upload on the cloud. Human body dynamics are sense using wearable device sensor. This system will consist of compact IOT devices and the Sensor network (BSN) to drop out some limitations of existing healthcare system. Main purpose of this paper is to generate the quick and automatic report for the patient suffering from particular disease. Security of the network is the big deal and challenging.*

Keywords— Cloud Computing, E-Healthcare System, Human Body Sensor, IOT Devices.

I. INTRODUCTION

Sensors are the elements of the small electronic devices that are capable to capture the data from the specific domain. The primary domain is the "Healthcare" domain, which the data from the human body is collected and store for the future reference. Smart wearable devices are the lightweight, Small-size and the Low powered devices, which are easily wearable on the human body for the Intelligence Monitoring System. Body Sensor Area Network (BSN) uses the low powered devices, which can be connect living and non-living things to from the network which can be capable for communication between them. IEEE 802.15 standard provides the network integration capability around human body which can serve the variety of applications including medical, consumer applications for personal entertaining and other.

1.1 Nature Of The Problem

Smart wearable devices connected to the human body by various nodes or devices which forms Personal Area Network (PAN). It provides the Bluetooth connection between nodes, based on IEEE 802.15.1 standards, exchanging data between nodes and has the minimum coverage area of 10m. Collected data is passed to other node which can store the data (Cloud storage), transmission take place as the radio frequency bands which is another stander of IEEE. Considering the vulnerable nature of the wireless transmission it creates the security issues and threats, like eavesdropping, modification and misused of the data.

1.2 Previous Work

The study was made on the sport athletic runner with different skills, investigate and review the kinematic changes in the results from the root. Another study of the network synchronization is done on the heartbeat rhythm instead of traditional periodic beacons that is the radio frequency signals. We need the best location of the human body to carried out the transmission of the data from device to node retain the connectivity with the receiving unit on the chest. The accelerometer sensor captures the unit data from the various human body parts which are moving while running and doing some activity. These sensors are worn on the arms, legs, foots. An approximate algorithm used to carry out swing time calculation to generate the result and reports. This study shows effect on the human body, actual performance of the all nodes and devices, network connectivity as well as data rates of the link performance.

1.3 Purpose

The main purpose of the Body Sensor Network (BSN) is to transmit data from the wearable devices to the internet for the future reference also generating reports of the patients in healthcare domain. Sensors of the device is constantly monitoring the health condition of the patient via different nodes attached to the body, there will be small bio-chips in the body of the patient. Some fixed sensors can detect the various psychological variations in the patient health status. Wireless Transmission Unit transmits the

International Journal of Engineering Research & Science (IJOER)
ISBN: [978-93-5321-411-1] ISSN: [2395-6992] [Vol-5, Issue-3, March- 2019]

information to the doctors throughout the world. If an emergency is noticed, doctors immediately update the status of the patient from the device (Personal Computer).

II. WIRELESS SENSOR NETWORK

Wireless network is the computer network which connect different computers via wireless link. Wireless telecommunication network controls radio frequency communication channels. This can be done into physical level of the OSI Model. Cellular phone networks, wireless sensor networks, wireless local area networks (WLANs), satellite communication networks, and terrestrial microwave networks are the different formats of wireless networks. Wireless Sensor Network uses the large number of sensors that can constantly monitor and sense the remote areas. Data collected and sense by the sensors can be transmitted via base station receiver to the remote node. In the past decade Wireless Sensor Network grows rapidly due to the advances in the sensors and the communication technologies. Large numbers of sensors are monitoring the environment, having different nodes which can be take part as collection or the receiving nodes. WSN features can be used in various applications such as Weather Forecasting, Surveillance Missions, Emergency Response services and the Health monitoring.

Example Scenario for Wireless Sensor Networks

Fig. 1

III. INTERNET OF THINGS

IoT is the system interrelated computing devices, objects, mechanical or digital machines, animals and peoples having unique identifier (UID) that can interact with other for transfer the data over the network without the need of human-to-human or human-to-machine interaction. IoT services are the beyond the Machine-to-Machine interaction that can utilize the better advantages of the internet. An IoT applications has verity of areas like smart cities, traffic congestion, waste management, structural health, security, emergency services, logistics, retails, industrial control, and health care etc. The perspective of IoT devices in medical domain gives better solutions of the problems. It gives the health monitoring system that contains the medical devices, sensors and the diagnostics imaging devices. A massive amount of the data is collected by a sensor, blood ~~pressure (BP)~~ pressure (BP), Electrocardiogram (ECG). Along with that, the IoT can properly identify optimum times for replenishing supplies for various devices for their easy, continuous and better operation. Additionally, the efficient arrangement of restricted resources can be decided by the IoT by ensuring their best use and can serve more patients. Based on analysis and aggregation, care givers can supervise patient's condition from any location and respond accordingly and quickly.

IV. BODY AREA NETWORK

Autonomously connected various medical sensors and actuators located on, in, around or/and near the human body constituent WBAN to monitor physiological signals. The IEEE 802.15.6 BAN Standard aims to enable low-power communication to be dependable and practical for in-body/on body nodes to assist a variety of medical and non-medical applications. With the time passes, the number of people coexisting in BAN is increasing rapidly with the anticipated growth in the number of BAN users. This scenario of coexistence of more people is a concern for the near future, where reliable communications is vital in especially healthcare scenarios. When there is a coexistence of multiple closely-located BANs, the potential 397 inter-network

International Journal of Engineering Research & Science (IJOER)
ISBN: [978-93-5321-411-1] ISSN: [2395-6992] [Vol-5, Issue-3, March- 2019]

communication and cooperation across BANs leads to the implementation of wireless body-to-body networks (BBNs). System of sensors is placed on or near the surface of the patient's body or embedded statically into tissue to collect particular physiological information. The captured signals can be used for various medical as well as non-medical applications. Each sensor node will transmit the collected information to an external node via wireless technique. This external node can use traditional networks to further transmit the data. Thus, sensor nodes used in a BAN must have wireless capability, should be reliable with less complexity and low power operation.

V. IOT & BAN INTEGRATION

The constant development of WBAN technology experienced a major breakthrough in the year 1995, around the idea of using wireless personal area network (WPAN) technologies to implement communications on, near, and around the human body. About six years later, a new term "BAN" was introduced to refer systems where communication is entirely within, on, and in the very close region of a human body. Advancements in wireless communication, Micro Electro Mechanical Systems (MEMS) technology and integrated circuits has enabled low-power, intelligent, miniaturized, invasive/non-invasive micro and nanotechnology sensor nodes that are strategically placed in or around the human body to be used in various applications, such as personal health monitoring. With other wireless technologies like WSNs, radio frequency identification (RFID) technology, Bluetooth, Bluetooth Low Energy (previously called WI Bree), Zigbee, wireless personal area network (WPAN), video surveillance systems, wireless local area networks (WLAN), internet, and cellular networks, BAN is also able to interface. It comprises of three tiers communications: Intra-BAN communications, Inter-BAN communications and beyond BAN communications. Intra-BAN communications indicate communications among wireless body sensors and the master node of the WBAN. Inter-BAN communications encompass communications between the master node and personal electronic devices such as smart phones, tablets, notebooks, computers, home service robots etc. The beyond-BAN tier connects the personal device to the Internet. The end unit is either data processing unit for IoT or a health care facilitator WBAN network. So, both the networks can be an integrated smart and intelligent network for future wireless sensor network. With the time passes, the number of people and things coexisting in BAN and IoT is increasing rapidly with the anticipated growth in the number users. This scenario of coexistence of more people and things is a concern for the near future, where reliable communications is vital in especially healthcare scenarios. When there is a coexistence, the 398 potential inter-network communication and cooperation across BAN and IoT leads to the implementation of wireless body-to body networks (BBNs) or things to things networks. To overcome the issues of coexistence and enhance general performance is the main aim in future. A cost-effective solution for the process of remote monitoring of a group of patients or things, for instance, can be provided by this type of integrated network by relaying sensor data in case of out of range network infrastructure.

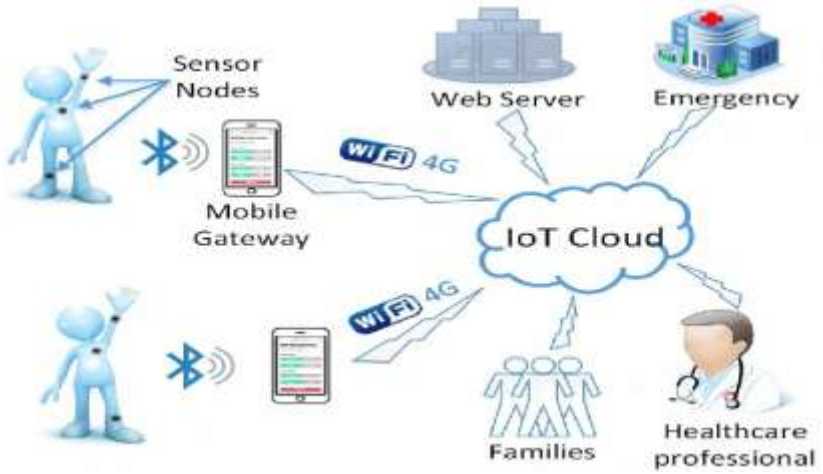

Fig. 2

International Journal of Engineering Research & Science (IJOER)
ISBN: [978-93-5321-411-1] ISSN: [2395-6992] [Vol-5, Issue-3, March- 2019]

VI. SECURITY ATTACKS IN WBAN

The development of WBANs is hindered by various security threats due to the vulnerable nature of wireless channel. Some of the major attacks in WBANs are as follows:

4.1 Eavesdropping:

The features of wireless channels in WBANs are open. Hence the radio communication between the nodes in the WBANs can be intercepted by the attackers freely and easily. This allows the attackers to eavesdrop packets from node to node. It also helps the attackers to obtain sensitive and valuable information.

4.2 Data Modification:

The eavesdropped information is partly or fully removed or replaced by the attackers. The modified information is sent back to the original receiver to achieve some illegal purpose.

4.3 Impersonation Attack:

The attacker eavesdrops the legal BAN Network Controller (BNC's) or the BAN nodes (BN's) private identity information. He uses the legal identity information to cheat BN's or BNC.

4.4 Replaying:

A part of the valid information can be eavesdropped by the attacker and is send back to the original receiver after some time to achieve the same purpose in different case. e. Denial of Service: When the traffic is beyond the capacity of the systems, the Denial of Service (DoS) attack occurs. The effect of both intentional act of malicious and compromised nodes and unintentional excessive peak network utilization is associated with it. A DoS attack can be easily initiated by the attackers using the infected BNs, when the authenticated BNs are compromised.

VII. SECURITY REQUIREMENTS IN WBAN

In general, the characteristics of an application are needed to build robust security mechanism, which defend the system from possible security threats. The fundamental security requirements in WBAN are described below.

4.5 Data Confidentiality:

To protect the data from a disclosure, the system requires data confidentiality. During communication, there is a possibility of overhearing and eavesdropping the sensitive information by the adversary. Encrypting the data with a secret key and sharing the secret key through a secure channel is one of the ways to acquire confidentiality.

4.6 Data Authentication:

Applications including both medical and non-medical application necessitates data authentication. Each BN and BNC has to verify whether the data is transmitted by the trusted sensor or by the adversary. Symmetric technique can be used in a WBAN to achieve data authentication. This technique shares the secret key to compute Message Authentication Code (MAC) for all data.

4.7 Data Integrity:

Data integrity is necessary as an adversary can alter the data that is transmitted over an insecure channel. Absence of data integrity technique paves a way to the adversary to modify the information before it reaches the BNC. Data integrity is attained through data authentication protocols, which ensures that the received data is not changed by the adversary.

4.8 Data Freshness:

The data freshness technique is essential to assure data confidentiality and integrity. The adversary may confound the BNC by taking data during transmission and retransmit them later. Data freshness guarantees the newness of data. In our words, it checks the arrangement of data frames. Strong freshness and weak freshness are the two types of data freshness.

International Journal of Engineering Research & Science (IJOER)
ISBN: [978-93-5321-411-1] ISSN: [2395-6992] [Vol-5, Issue-3, March- 2019]

4.9 Secure Management:

As BNC, distribute keys to BNs to achieve encryption and decryption techniques, it demands secure management. The BNC adds and removes the BNs in a secure manner in the case of association and disassociation.

4.10 Availability:

It guarantees that the patient's information is accessible to the doctor. This accessibility can be destroyed by the adversary by disabling an ECG mode. This may lead to critical situation such as loss of life. During the loss of availability, a technique is required to maintain the operation of the BNs and switch the operation to another BN in addition to the basic security requirements like confidentiality, integrity protection and authentication certain other goals should be met. It includes:

Efficiency: An important aspect of a BSN's design is energy-efficiency due to the limited capabilities of sensors. The continuous monitoring requirements of a BSN can be hindered by the frequent energy depletion even though the sensors are rechargeable. Hence energy-efficient secure communication is needed for BSN.

Usability: The security solutions for BSN have to be useable. The usable security solutions are defined which are activated on employment in plug-n-play manner with minimal initialization procedures.

VIII. CONCLUSION

WBAN is an emerging and promising technology that will change people's healthcare experiences revolutionarily. It brings out a replacement set of challenges in terms of sensor deployment and density, energy potency, security and privacy and wireless technology. In this paper, we've reviewed the present development on Wireless Body Area Network and that we targeted in security problems faced by this technology. During this paper, we discussed the security attacks and requirements in WBAN. We presented the existing security mechanisms in WBAN. In this paper, we also presented the difference between WBAN and WSN. Thus, we tend to believe that WBAN needs a robust security system and a part of its authentication. A secured authentication system is extraordinarily required in numerous applications WBAN technology notably in medical and military.

REFERENCES

[1] Jingwei Liu, Kyung Sup Kwak, "Hybrid Security Mechanisms for Wireless Body Area Networks", pp.98- 103,2010.
[2] Latré, Benoît, Bart Braem, Ingrid Moerman, Chris Blondia, and Piet Demeester. "A survey on wireless body area networks," Wireless Networks, vol. 17, 2010, pp. 1-18, doi: 10.1007/s11276-010-0252-4
[3] M. A. Hanson, H. C. Powell Jr., A. T. Barth, K. Ringgenberg, B. H. Calhoun, J. H. Aylor and J. Lach , "Body area sensor networks: challenges and opportunities", IEEE Computer,vol42., Issue.1,pp.58-65,2009.
[4] Harrison B.L., Consolvo S., Choudhury T. Using Multi-Modal Sensing for Human Activity Modeling in the Real World. In: Nakashima H., Aghajan H., Carlos Augusto J., editors. Handbook of Ambient Intelligence and Smart Environments. 1st ed. Volume 4. Springer; New York, NY, USA: 2009.
[5] Aziz O., Lo B., King R., Darzi A., Yang G.Z. Pervasive Body Sensor Network: An Approach to Monitoring the Post-Operative Surgical Patient. Proceedings of the International Workshop on Wearable and Implantable Body Sensor Networks; Cambridge, MA, USA. 3–5 April 2006;
[6] Conroy L., Ó'Conaire C., Coyle S., Healy G., Kelly P., O'Connor N., Caulfield B., Connaghan D., Smeaton A., Nixon P. TennisSense: A Multi-Sensory Approach to Performance Analysis in Tennis. Proceedings of the 27th International Society of Biomechanics in Sports Conference 2009; Limerick, Ireland. 17–21 August 2009.
[7] Pansiot J., Lo B., Yang G.Z. Swimming Stroke Kinematic Analysis with BSN. Proceedings of the 2010 International Conference on Body Sensor Networks (BSN); Biopolis, Singapore. 7–9 June 2010;
[8] Burchfield R., Venkatesan S. A Framework for Golf Training Using Low-Cost Inertial Sensors. Proceedings of the 2010 International Conference on Body Sensor Networks (BSN); Biopolis, Singapore. 7–9 June 2010;
[9] Nesime T., Mark B., Reed H., Steve M., Stan Z. Confidence-Based Data Management for Personal Area Sensor Networks. Proceedings of the First Workshop on Data Management for Sensor Networks (DMSN2004); Toronto, Canada. 30 August 2004;
[10] Li H.B., Takizawa K., Kohno R. Trends and Standardization of Body Area Network (BAN) for Medical Healthcare. Proceedings of the 2008 European Conference on Wireless Technology; Amsterdam, Netherlands. 27–28 October 2008;