Asian Journal of Applied Science and Technology (AJAST)
(Open Access Quarterly International Journal) Volume 2, Issue 2, Pages 44-50, 2018

Bio Medical Based End To End Security by Using IOT

A.Abitha[1], V.Dharshini[1], V.Jananipriya[1] and Mrs.M.Tamilarasi[2]

[1]*UG Scholar, Department of ECE, Excel Engineering College, Komarapalayam, Tamilnadu, India.*
[2]*Assistant Professor, Department of ECE, Excel Engineering College, Komarapalayam, Tamilnadu, India.*

Article Received: 24 December 2017 *Article Accepted: 27 February 2018* *Article Published: 03 April 2018*

ABSTRACT

Wireless communication is the biggest contribution to mankind compared to the other technologies. It is enhanced to convey the information quickly to the consumers. In the modern health care environment, the usage of internet of things (IOT) with global system for mobile communication (GSM) brings convenience of physicians and patients. The body sensor networks are one of the core technologies of IOT developments in health care system. IOT and GSM based monitoring system is proposed for continuous monitoring of patients health condition using sensors.This focus on the measurement and monitoring of various biological parameters using web server and android application. Doctor can monitor the patient condition on his/her smart phone with the secure manner by using AES algorithm.

Keywords: IoT, Security, health care, mobile communication, AES algorithm.

1. INTRODUCTION

A Wireless sensor network (WSN) is a computer network consisting of spatially distributed autonomous devices using sensors to cooperatively monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants, at different locations. The development of wireless sensor networks was originally motivated by military applications such as battlefield surveillance. However, wireless sensor networks are now used in many civilian application areas, including environment and habitat monitoring, healthcare applications, home automation, and traffic control.

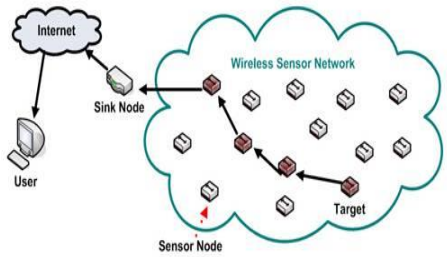

Figure 1.1 Wireless Sensor Network

As shown in figure 1.1 each node in a sensor network is typically equipped with a radio transceiver or other wireless communications device, a small microcontroller, and an energy source, usually a battery. The size a single sensor node can vary from shoebox-sized nodes down to devices the size of grain of dust. The cost of sensor nodes is similarly variable, ranging from hundreds of dollars to a few cents, depending on the size of the sensor network and the complexity required of individual sensor nodes. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed and bandwidth. The topology of the WSNs can vary from a simple star network to an advanced multi-hop wireless mesh network. The propagation technique between the hops of the network can be routing or flooding. Typical applications of WSNs

include monitoring, tracking, and controlling. Some of the specific applications are habitat monitoring, object tracking, nuclear reactor controlling, fire detection, traffic monitoring, etc. In a typical application, a WSN is scattered in a region where it is meant to collect data through its sensor nodes.

2. EXISTING SYSTEM

In the existing system they use Zigbee technology for monitoring the patients in hospital.

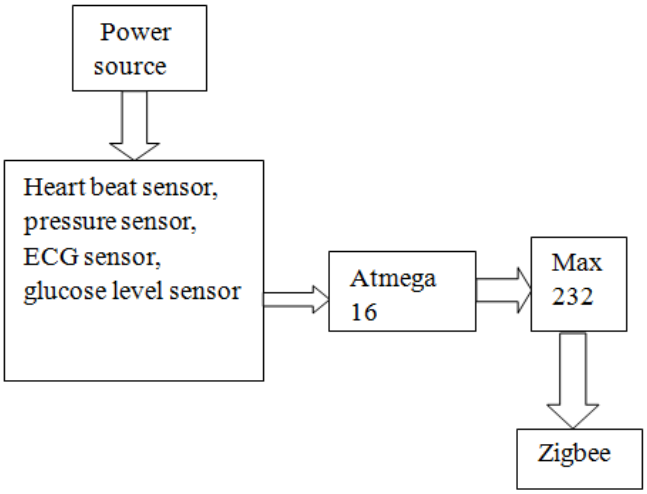

Figure1.2 Zigbee system

In existing system all the sensors data will be stored and send to the doctor using Zigbee. A Wireless Sensor Network (WSN) for monitoring patient's physiological conditions continuously using Zigbee. Here the physiological conditions of the patients are monitored by sensors and the output of these sensors is transmitted via Zigbee and the same has to be sent to the remote wireless monitor for acquiring the observed patient's physiological signal Infusion pump is a medical device. It is healthcare facilities used worldwide in hospitals, and at home. It can deliver fluids both in medicines and nutrients such as pain relievers chemotherapy drugs, hormones or insulin, and antibiotics into a patient's body in any amounts. There are many types of pumps including insulin pumps, syringe, large volume, elastomeric, patient-controlled analgesia (PCA), and enteral pump. Enteral pump is a pump that is used to deliver medications and liquid nutrients to a patient's digestive tract. Patient-controlled analgesia (PCA) pump is a pump that is used to deliver pain medication. Insulin pump is a pump that is used to deliver insulin to patients with diabetes which is frequently used in home. These devices are very important for nurses because they can show status of liquid that they give to patients. So, the devices are very popular in hospitals for checking status of medicine.

Drawbacks

- Improper measurement of the level of the saline droplet.
- Waste of time.

- Make disturbance to the patient.
- Zigbee covers short distance
- So communication level is poor.

3. PROPOSED SYSTEM

In our proposed system we combined the GSM technology and IoT for patient monitoring in hospital with the secure manner by using AES algorithm.

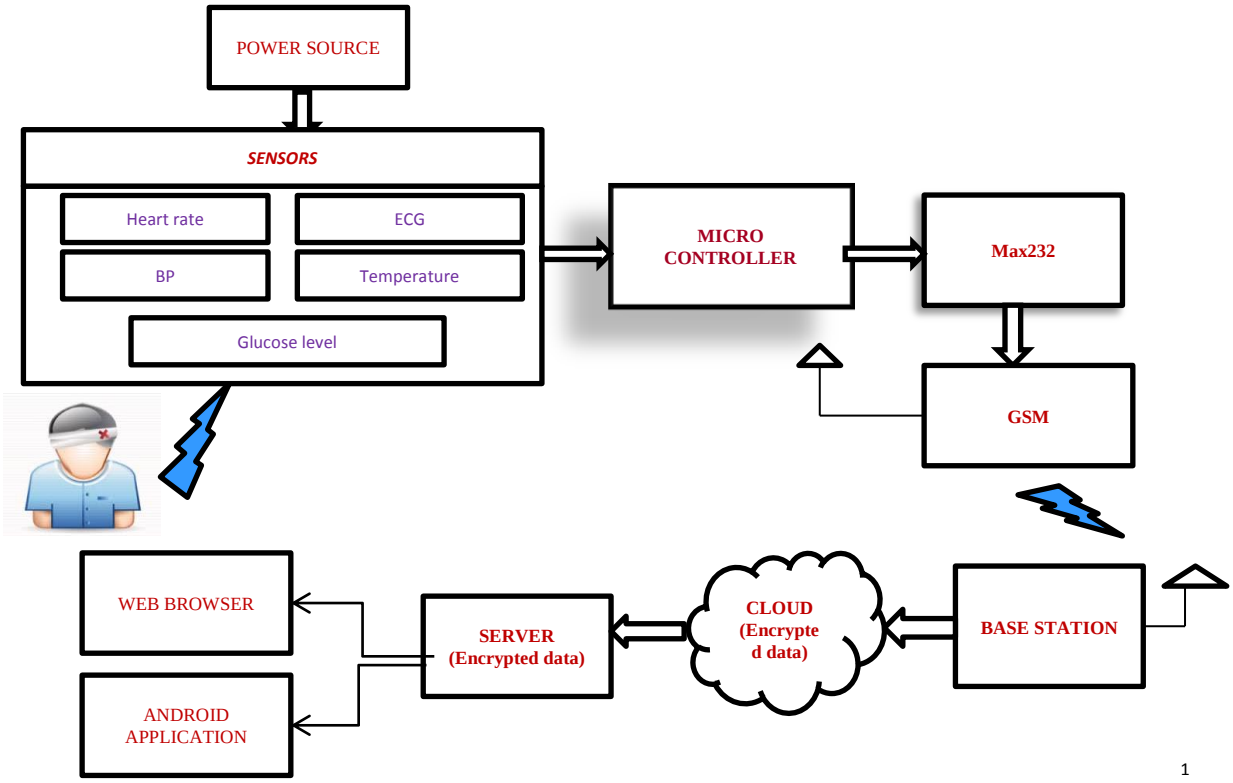

Figure:1.3 patient monitoring security by using IoT

Whenever the patient need emergency care, the proposed system alerts the predefined users and also it finds the nearby emergency contacts as shown in figure 4.1. The IOT technology uses internet to transfer the medical data about the patient continuously. Body Sensor Network (BSN) allows the integration of intelligent, miniaturized low-power sensor nodes in, on or around human body to monitor body functions and the surrounding environment. It has great potential to revolutionize the future of healthcare technology and attained a number of researchers both from the academia and industry in the past few years. Generally, BSN consists of in-body and on-body sensor networks. An in-body sensor network allows communication between invasive/implanted devices and base station. On the other hand, an on-body sensor network allows communication between non-invasive/wearable devices and a coordinator. Now, our BSN-Care BSN architecture composed of wearable and implantable sensors. Each sensor node is integrated with bio-sensors such as Electrocardiogram (ECG), Blood Pressure (BP), etc. These sensors collect the physiological parameters and forward them to a coordinator called Local Processing Unit (LPU), which

can be a portable device such as PDA, smart-phone etc. The LPU works as a router between the BSN nodes and the central server called BSN-Care server, using the wireless communication mediums such as mobile networks 3G/CDMA/GPRS. Besides, when the LPU detects any abnormalities then it provides immediate alert to the person that wearing the bio-sensors. The data will be very secure in the cloud, there is no possibility of hacking in this system.

4. ALGORITHM USED

The algorithm used to provide security for the cloud is Advanced Encryption Standard (AES).

Advanced Encryption Standard (AES)

AES comprises three block ciphers: AES-128, AES-192 and AES-256. Each cipher encrypts and decrypts data in blocks of 128 bits using cryptographic keys of 128-, 192- and 256-bits, respectively. The Rijndael cipher was designed to accept additional block sizes and key lengths, but for AES, those functions were not adopted.

Symmetric (also known as secret-key) ciphers use the same key for encrypting and decrypting, so the sender and the receiver must both know -- and use -- the same secret key. All key lengths are deemed sufficient to protect classified information up to the "Secret" level with "Top Secret" information requiring either 192- or 256-bit key lengths. There are 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys -- a round consists of several processing steps that include substitution, transposition and mixing of the input plaintext and transform it into the final output of cipher text.

The AES encryption algorithm defines a number of transformations that are to be performed on data stored in an array. The first step of the cipher is to put the data into an array; after which the cipher transformations are repeated over a number of encryption rounds. The number of rounds is determined by the key length, with 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys.

The first transformation in the AES encryption cipher is substitution of data using a substitution table; the second transformation shifts data rows, the third mixes columns. The last transformation is a simple exclusive or (XOR) operation performed on each column using a different part of the encryption key longer keys need more rounds to complete.

The AES Cipher

Like DES, AES is a symmetric block cipher. This means that it uses the same key for both encryption and decryption. However, AES is quite different from DES in a number of ways. The algorithm Rijndael allows for a variety of block and key sizes and not just the 64 and 56 bits of DES' block and key size. The block and key can in fact be chosen independently from 128, 160, 192, 224, 256 bits and need not be the same. However, the AES standard states that the algorithm can only accept a block size of 128 bits and a choice of three keys - 128, 192, 256

bits. Depending on which version is used, the name of the standard is modified to AES-128, AES-192 or AES-256 respectively. As well as these differences AES differs from DES in that it is not a feistel structure. Recall that in a feistel structure, half of the data block is used to modify the other half of the data block and then the halves are swapped. In this case the entire data block is processed in parallel during each round using substitutions and permutations.

A number of AES parameters depend on the key length. Rijndael was designed to have the following characteristics:

- Resistance against all known attacks.
- Speed and code compactness on a wide range of platforms.
- Design Simplicity.

Inner Workings of Round

The algorithm begins with an Add round key stage followed by 9 rounds of four stages and a tenth round of three stages. This applies for both encryption and decryption with the exception that each stage of a round the decryption Algorithm is the inverse of its counterpart in the encryption algorithm.

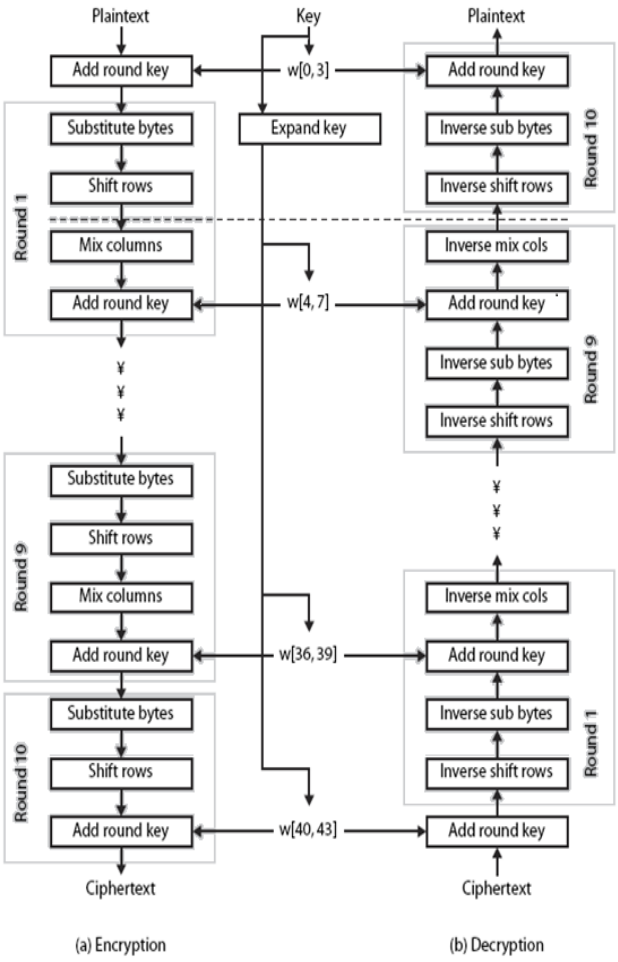

Figure:1.4 overview of AES

ADVANTAGES OF PROPOSED SYSTEM

- The IOT technology is faster and cheaper to implement.
- It monitors the patient's health continuously and log the data in a cloud storage location for future reference.
- The security system implemented in this technology will protect the privacy of the patient.

5. CONCLUSION

The proposed system found that even though most of the popular BSN based research projects acknowledge the issue of the security, but they fail to embedded strong security services that could be preserve patient privacy. Finally, we proposed a secure IoT based healthcare system using BSN, called BSN-Care, which can efficiently accomplish various security requirements of the BSN based healthcare system. All the sensor which is connected in the body is used to collect the abnormal symptoms of the human body and then it is collected back to the doctors through the IOT technology.

REFERRENCES

1. Bonetto.R, Bui.N, Lakkundi.V, Olivereau.A, Serbanati.A, and Rossi. (2012), "Secure Communication for Smart IOT Objects: Protocol Stacks, Use Cases and Practical Examples", *IEEE World of Wireless, Mobile and Multimedia Networks (WoWMoM)*.
2. Dev.J.A (2013), "Usage of Botnets for High Speed MD5 Hash Cracking".*3rd International Conference on Innovative Computing Technology, INTECH*.
3. Gillis.J, Calyam.P, Bartels.A, Popescu.M, Barnes.S, Doty.J, Higbee.D, and Ahmad.S (2015), " Panacea's Glass: Mobile Cloud Framework for Communication in Mass Casualty Disaster Triage", *IEEE Mobile Cloud*
4. Huber Flores.X.S, Kostakos.V, Ding.A.Y, Nurmi.P, Tarkoma.S, Hui.P, and Li.Y (2017), " Large-scale offloading in the internet of things", In
   International Conference on Pervasive Computiand Communications Workshops, PerCom WS
5. .Hummen.R, Wirtz.H, Ziegeldorf.J.H, Hiller.J, Wehrle.K (2013),"Tailoring End-to-End IP Security Protocols to the Internet of Things". *21st IEEE International Conference on Network Protocols (ICNP)*.
6. Huth.C, Zibuschka.J, Duplys.P, Guneysu.T (2015), "Securing Systems on the Internet of Things via Physical Properties of Devices and Communications", *Systems Conference (SysCon), 2015 9th Annual IEEE International*
7. IOT trends 2016- tech insider. http://www.businessinsider.com/ top-internet-of-things-trends-2016-
8. Iqbal.Md.A, Bayoumi.M (2016), "Secure End-to-End Key Establishment Protocol for Resource-Constrained Healthcare Sensors in the Context of IOT", *International Conference on High Performance Computing and Simulation (HPCS)*.
9. Khemissa.H and Tandjaoui.D (2016) " A novel light weight authentication scheme for heterogeneous wireless sensor networks in the context of internet of things", In *2016 Wireless Telecommunications Symposium, WTS 2016, London, United Kingdom, April 18-20, 2016*, pages 1–6.

10. Kuo.F.C, Tschofenig.H, Meyer.F, and Fu.X (2006), "Comparison Studies between Pre-Shared and Public Key Exchange Mechanisms for Transport Layer Security", *25th IEEE International Conference on Computer Communications. Proceedings (INFOCOM)*.