INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 4 ISSUE 2 (2017) PAGES 3308 - 3316
RECEIVED : 15.03.2018 PUBLISHED : 18.04.2018
April 18, 2018

AN IMPREGNABLE IOT BASED LEADING EDGE HEALTH AEGIS SYSTEM ADAPTING BSN - CARE

Parkavi.S. M.E[1]Samundeeswari.M.M.Tech[2]
parkavisivaa@gmail.com[1]samusankar@gmail.com[2]

ABSTRACT

An elevation in intelligence and communication technologies has paved a way for the increased emergence of the Internet of Things (IoT). The leading century of the healthcare environment, applying IoT technologies brings the efficient opportune for both physician and patients. One of the vital core elements of IoT technologies is the Body Sensor Network (BSN) which is a wearable computing device. This paper presents an impregnable IoT based Health aegis system adapting BSN, called BSN-care. The sensor will sense the patient's body and transmit it wirelessly to the end-user device such as PDA, Laptop etc for further analysis. Based on the degree of abnormalities it will alert the family members, personal doctor or emergency unit. It is mainly designed for patient health monitoring in the assisted-living and home environment. It provides the continuous and timely monitoring of the patients physiological status. In sensor network application the communication is mostly wireless in nature. This may result in various threats to these systems. To overcome this problem a lightweight anonymous authentication protocol is used along with OCB authenticated encryption mode. It helps to monitor the individuals without violating the data privacy of patient's information.

Key words: BSN, Data privacy, integrity, Authentication, Secure localization.

I. INTRODUCTION

According to the Eurostat population projection, by 2030 the percentage of elderly people (65 years old and older) will increase with 6.1%, compared to 2008, with the assumption that the growth will continue in the future. Meanwhile, we are facing the problem of birth rates that are below the level needed for a sustained population. In 2008, one person aged 65 or older among the four people of working age people. There is the need for less expensive solutions in healthcare that will utilize the benefits of modern technology, providing long distance monitoring of elderly, in the need of the critical situation. Technical advances in physiological sensing devices and wireless connectivity provided by the IoT can make dramatic changes in the ways remote healthcare will be performed in the future. However, for such changes to take place, the enabling technologies must be employed with the well-being of the patient in focus, since neither individuals nor society would accept IoT solutions. The body sensor network (BSN) technology is one of the most important technologies used in an IoT based modern healthcare system. It is the collection of low-power and lightweight wireless sensor nodes that are mostly used for monitoring the human body functions. It can also be used to locate the surrounding. Since BSN nodes are used to collect sensitive information and may operate in critical environments. They require strict security mechanisms to prevent malicious activities with the system.In this article, at first, the several security requirements in BSN based leading-edge healthcare aegis system are addressed. Then, a secure IoT based health aegis system adapting BSN, called BSN-Care, is proposed.

II. HEALTHCARE MONITORING

The improvement of BSN in healthcare applications has made patient monitoring more comfortable. Recently, several wireless healthcare types of researchers and projects have been emerged, which can aim to provide continuous patient monitoring in the critical environment (e.g. athlete health monitoring). In the current system, the sensor senses the patient’s body and transmits it wirelessly to the end-user device (PDAs, laptop, and personal computer) for further analysis. It is mainly designed for patient health monitoring in the assisted-living and home environment. It provides the continuous and timely monitoring of the patient’s health status. This data is sent to a Local Processing Unit (LPU) which is a user held device PDA, Laptop etc This LPU analyzes the data and depending on the requirement, it will send the alert to one or multiple of the following through the BSN-Care Server such as Family members, Physician or Emergency Unit.

III. SENSOR

There are three types of sensor are used. They are

- Temperature sensor
- Respiratory Sensor
- Heartbeat Sensor

A. TEMPERATURE SENSOR

A temperature sensor is a device which is used to measure the temperature through an electrical signal. It is mostly fixed in mouth, forehead etc. There are many sensors are used to measure the temperature such as Thermocouple, Thermistor, RTD etc. This different temperature sensor works on different principles. Among these LM35 is more comfortable for an integrated circuit. It works on the principle of whose output voltage is linearly proportional to the Celsius temperature. The low output impedance of LM35 device makes interfacing to readout easily. It gives more accuracy than other temperature sensors. The main advantages of using LM35 are cost effective.

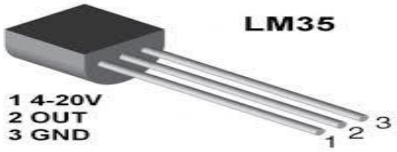


Fig 1: LM35 sensor

B. RESPIRATORY SENSOR

The Respiratory sensor is used to measure the respiratory rate. It will count the number of inhalation and exhalation taken per minute. It is also known as ventilation rate. The efforts of respiratory monitoring show patient's inability to oxygenate their blood, where the patient is in the need of mechanical ventilation. The normal breath rate of a person is 12 to 20 breaths per minute and 12 or over 20 is abnormal.

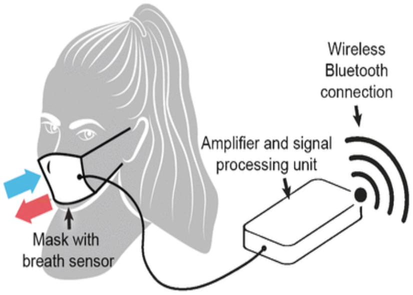


Fig 2: Respiratory sensor

C. HEARTBEAT SENSOR

The Heartbeat Sensor will measure the flow of blood volume that is circulating from one region to another region. It will pass the Light Emitting Diode (LED) in one side of the finger to measure the intensity of Light received on other side using LDR. Based on this intensity the Heartbeat will be measured. The normal Heartbeat of a person is from 72 to 80 times per minute. During the blood pumping more light is absorbed which leads to decrease in intensity of light received on LDR. As a result, the LDR value will be an increase. It is denoted in Beat per minute (BPM)

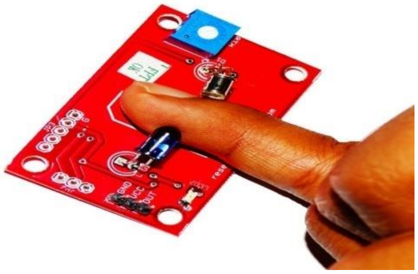


Fig 3: Heartbeat sensor

IV. RELATED ISSUES

- In the existing system, security issues were a major drawback.
- It has lack of Security.
- Due to this, some patient’s vital information is lost.
- The Implementation price of overall monitoring is high.
- It is a fixed infrastructure network and not flexible.

- It leads to the vulnerability of the patient privacy.

V. SECURE IoT BASED HEALTH AEGIS SYSTEM ADAPTING BSN-CARE

The proposed system consists of major security requirements in BSN based leading-edge health aegis system. A secure IoT based health aegis adapting BSN, called BSN-Care, which can efficiently accomplish security requirements such Network security of Mutual authentication, anonymity, secure localization and Data security of data privacy, data integrity, and data freshness. There are two types of BSN sensor which is in body sensor and on body sensor. The main advantage of this system is to protect the patient's information.

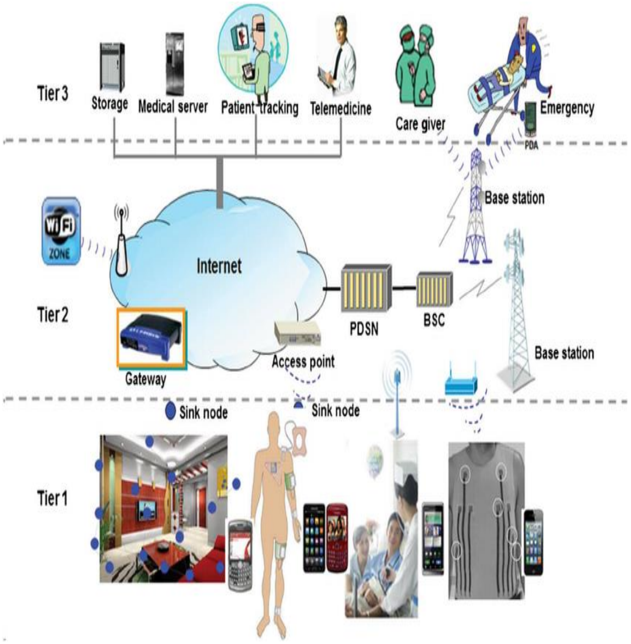


Fig 4: Secure IOT based health aegis system adapting BSN-care

VI. SECURITY IN BSN-CARE SYSTEM

The Security requirements of BSN-Care system is divided into two parts:
They are:

- Network Security
- Data Security

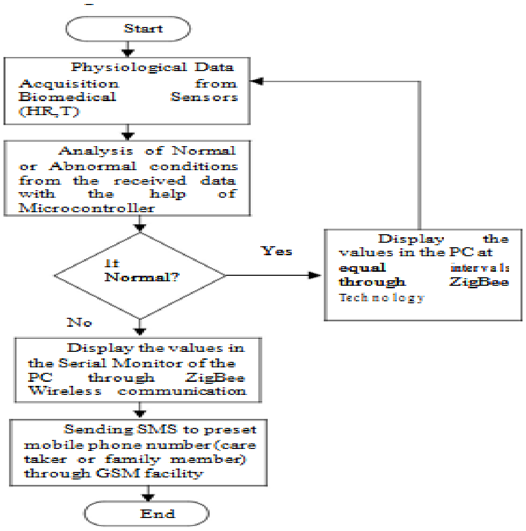

Start
Physiological Data Acquisition from Biomedical Sensors (HR,T)
Analysis of Normal or Abnormal conditions from the received data with the help of Microcontroller
If Normal?
Yes
No
Display the values in the PC at equal intervals through ZigBee Technology
Display the values in the Serial Monitor of the PC through ZigBee Wireless communication
Sending SMS to preset mobile phone number(care taker or family member) through GSM facility
End

Fig 5: Dataflow diagram

VII. NETWORK SECURITY IN BSN-CARE SYSTEM

The Network security of BSN-Care deals the following property:

- Mutual authentication property
- Anonymity property
- Secure Localization property.

In order to achieve all the above property, a Lightweight Anonymous authentication protocol was used.

A. LIGHTWEIGHT ANONYMOUS AUTHENTICATED PROTOCOL

In our BSN-Care system, when an LPU wants to connect to the server, then the server needs to confirm the identity of LPU using a Lightweight anonymous authentication protocol.

- First, an LPU submits its identity $ID_l$to the server through a secure channel.
- After receiving the request the server will generate the random number which is denoted as N_S and then computes $K_{LS\,=}\, h(ID_L \,\|\, N_S) \oplus ID_{S.}$
- Subsequently, the server generates a set of unlinkable shadow SID = $\{sid_{1,}\, sid_2\ldots\}$ where $sid_j \in$ SID which will be computed as $sid_j = h\,(ID_L \,\|\, r_j \| \, K_{LS})$.
- Then the server generates the Emergency key $K_{em} = \{k_{em1},\, k_{em2}\ldots\}$, and track sequence number $Tr_{seq.}$ For each request of LPU, the server generates the track sequence number Tr_{seq} = m and sends it to LPU. The copy of track sequence number will be stored in the server database.
- During execution, if the Tr_{seq} of LPU does not match with the stored value of database then the connection will be automatically terminated.
- In that case, an LPU will be asked to use the unused pair of shadow identity $sid_j$and emergency key $k_{emj.}$ Once the pair $(sid_j,\, k_{emj})$ is used, it should be deleted from both the LPU and the server.

B. MUTUAL AUTHENTICATION PROPERTY

The authentication between the server and an LPU is provided by verifying the one-time-alias identity AID_L and the track sequence number $Tr_{seq.}$ In case of loss of synchronization the server will authenticate an LPU by using the unused shadow identity sid_j in AID_L. The parameter V_1 in the request Message M_1 must be equal to the $h(N_1||LAI_L||K_{LS})$. The authentication can also be done by the parameter V_2 which must be equal to $h(Tr||ID_L||N_L)$.

C. ANONYMITY PROPERTY

The anonymity property is one which is used to verify that two conversations originate from the same patient. It also helps to hide the source of the packet and enable confidentiality. The anonymity issue is resolved with the combination of (shadow identity, emergency key). Due to the excessive storage cost, the concept is used only in the following situation If an LPU cannot receive the message in a specific period of time, while none of the parameters of MA_1 is allowed to send twice for privacy purpose. Due to the loss of synchronization between the LPU and the server because of response message MA_2 has been interrupted.

D. SECURE LOCALIZATION PROPERTY

In healthcare monitoring, the tracking of patient’s location is very important. The server will track the patient’s location by using the Encoded location area identity EL. The server decodes the $LAI_l$from LAL_l= EL $\oplus h(K_{ls}||N_l)$. It will represent the physical connection between the LPU and the base station of a mobile network.

Subsequently, the server will ask the base station to sends its identity LAI_l, then it will be compared to the LAI_l in EL or not. If the verification is successful the server believes that it is not the false signal.

VIII. DATA SECURITY IN BSN-CARE SYSTEM

The data security of the BSN-Care is dealing with the following property:They are

- Data privacy
- Data integrity
- Data freshness

All the above requirements are accomplished by adapting an authenticated encryption scheme offset codebook (OCB) mode.

A. DATA PRIVACY AND INTEGRITY

OCB is well suited for secure data communication in LPU devices because of its single pass without any additional primitive like the hash function, MAC. It is a block-cipher mode of operation that features authenticated encryption. It has the block size of n and tag of γ.

Let,

D - Plain text data

K – Encryption key
N – Non-repeating nonce.
Now OCB generates the output pair (C, Tag) is sent to the receiving end.Then the reverse operation will be performed on C to arrive at plain text D.If the receiver computes the different Tag apart from the Tag in the cipher-text is considered to be invalid. Then the data D is divided into n blocks where OCB needs only n+1 encryption to support both the data privacy and integrity.

B. DATA FRESHNESS

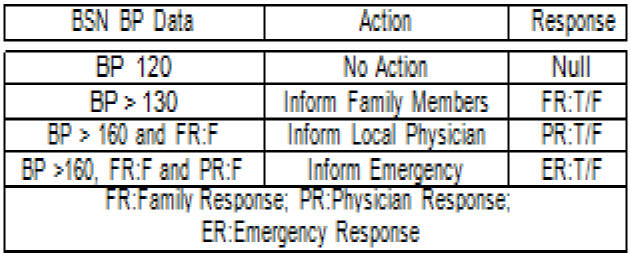
The freshness of the received data is also verified by OCB using incremental interface Δ where the Init (N) is the initial value for Δ. Like a counter, the incremental interface always provides a new incremental value through incrementing function. For each communication, both the sender and the receiver need to use the different nonce N which is not repeated. In this way, the freshness of the data is verified.

IX. EMERGENCY ALERT

The server periodically receives the patient's data from LPU, then it feeds the data into a database. Meanwhile, it may interact with the family members, the local physician, or emergency unit based on abnormalities.
Let the response parameters are
FR - Family Response
PR - Physician Response
ER – Emergency Response is the Boolean variables, which can be either True (T) or False (F).

For example, the normal Blood Pressure (BP) of person is ≤ 120, no action is required. In case if the BP > 130 the server repeatedly alert his family members. Once the FR response to the alert then FR will become True i.e FR: T. If FR: F and BP > 130 then the server will send the alert to Local Physician PR. Simultaneous the alert will be sent to both FR and PR. If both FR and PR are Falsei.e FR: F, PR: F and the BP > 160, then the server immediately sends the alert to the emergency unit. Once the server received the response from the emergency unit then ER will become true i.e ER: T. Finally the person is saved from the emergency situation

TABLE I: Action table using BP data



BSN BP Data	Action	Response
BP 120	No Action	Null
BP > 130	Inform Family Members	FR:T/F
BP > 160 and FR:F	Inform Local Physician	PR:T/F
BP >160, FR:F and PR:F	Inform Emergency	ER:T/F
FR:Family Response; PR:Physician Response; ER:Emergency Response		

X. CONCLUSION

Innovative uses of IoT technology in healthcare monitoring not only makes the lifestyle of individuals to lead a sophisticated life but also brings various challenges to their privacy. Inorder to overcome, all those problems our paper proposed an Impregnable IOT based health aegis system adapting BSN-care which can efficiently accomplish various security requirements.

ACKNOWLEDGEMENT:

I would like to thank my departmental staffs and friends, especially my guide for giving a restless effort to presenting this paper. Also a gratitude to many authors those who provide their material as reference.

REFERENCES

[1] R Chakarovarty, "A Programmable Service Architecture for Mobile Medical Care", March 2006.

[2] Dr. B .Eswara Reddy, Dr. Tv. Suresh kumar, "An Efficient Cloud Framework For Health care Monitoring system", Dec 2012.

[3] GiancartoFortino, Stefano Galzarano, "Programming Wireless Body Sensor Network Application Through Agents" 2010.

[4] Sourav Kumar, SumanSankar ,BhuviaNandhini Mukherjee, "Interference Aware Scheduling Of Sensor In IoT Enabled Health care Monitoring System" Dec 2014.

[5] ProsantaGope ,Tzonelih Hwang, "Untraceable Sensor Movement In Distributed IoT Infrastructure", June 2015.

[6] MrD.Stalin David, Dr.A.Jeyachandran, "A Comprehensive Survey of Security Mechanism In Healthcare Applications", March 2017.

[7] P. Rogaway, M. Bellare, and J. Black. OCB: A block–cipher mode of operation for efficient authenticated encryption. ACM Transactions on Information and System Security (TISSEC) 6 (3) pp. 365–403, 2003.

[8] T. Hwang, P. Gope, Provably Secure Mutual Authentication and Key Exchange Scheme for Expeditious Mobile Communication Through Synchronously One-Time Secrets. Wireless Personal Communica-tions 77(1), pp. 197-224, 2014.

[9] P. Gope, T. Hwang, "Enhanced secure mutual authentication, and key agreement scheme preserving user anonymity in global mobile net-works," Wireless Personal Communications, DOI: 10.1007/s11277-015-2344-z, 2015.

[10] Oracle Technology Network, "Java Cryptography Architecture",(JCA),http://docs.oracle.com/javase/6/docs/technotes/guides/crypto/ CrypoSpec.html.

[11] A. Kumar et al., "Caveat eptor: A comparative study of secure device pairing methods," IEEE International Conference on Pervasive Computing and Communications, 2009. PerCom 2009.

[12] P. Gope, T. Hwang, "Lightweight and Energy Efficient Mutual Authentication and Key Agreement Scheme with User Anonymity for Secure Communication in Global Mobility Networks," IEEE Systems Journal, DOI: 10.1109/JSYST.2015.2416396, 2015.

[13] T. Hwang, P. Gope, "IAR-CTR and IAR-CFB: Integrity Aware Real-time Based Counter and Cipher Feedback Modes," Security and Communication Networks (Wiley Journal), DOI: 10.1002/sec.1312, 2015.