Asian Journal of Applied Science and Technology (AJAST)
Volume 1, Issue 5, Pages 183-189, June 2017

A Secure Healthcare System using IOT device and Body Sensor Network

A.kavimani[1] and F.Anishya[2]

[1]*UG scholar, Department of Information Technology, IFET College of Engineering, Villupuram, Tamilnadu, India.*
[2]*Assistant Professor, Department of Information Technology, IFET College of Engineering, Villupuram, Tamilnadu, India.*

Article Received: 09 June 2017 *Article Accepted: 23 June 2017* *Article Published: 28 June 2017*

ABSTRACT

Internet of things (IOT) is a technology which is growing quickly in various applications like business, healthcare and various technologies widely. This paper mainly focuses in healthcare applications. Body sensor network (BSN) is a technology which is used in healthcare system where a patient can be monitored using many minute sensors and tiny particles. However for a patient monitoring system security is more important so that the patient's private information cannot be misused. In this paper we propose a modern healthcare system in which an IOT device is used to intimate to any of the destination holders .Here the IOT device contains the SIM slot which contains the GPRS and mobile data that sends the link to the cloud storage and then it intimate to the destination person. In this proposed system the IOT device contains the SIM slot which stores the information about whom to inform and then the LED display will be there to display the sensor values about the sensors like ECG sensor, pulse rate sensor, temperature sensor. If there is abnormality in the patient's health condition then the alert will be gone to the family first and then to clinic and then to the emergency center.

Keywords: BSN (Body Sensor Network), IOT (Internet of Things), SIM, GPRS (General Packet Radio Service) and Mobile data.

1. INTRODUCTION

Health is one of the global challenges for humanity. In 21st century IOT become one of the most powerful communication paradigms. In the IOT due to environment all the objects that we are using daily will take place due to their communication and computing capabilities [like microcontroller, transceivers for digital communication]. It extends the concept of internet and make pervasive. IOT provides similar interaction between medical sensors, monitoring cameras and home appliances. According to the constitutions of World Health Organization (WHO) the highest attainable standard of health is a fundamental right for an individual. Healthy individuals also reduce pressure on the already overwhelmed hospitals, clinics, and medical professionals and reduce workload on the public safety networks, charities, and governmental (or non-governmental) organizations. The body sensor network (BSN) technology is one of the imperative technologies used in IoT-based modern healthcare system. It is basically a collection of low-power and lightweight wireless sensor nodes that are used to monitor the human body functions and surrounding environment.

BSN nodes are used to collect sensitive information and operate in hostile environments. A recent report from the United Nations guesses that by 2050, the population would comprise of 2 billion older people (about 22% of the world population) about 80% of aged people older than 65 suffer from at least one disease. With the arrival of IoT, it is possible to achieve seamless communications among different devices - medical sensors, monitoring cameras, home appliances, etc. Healthcare Research Project developed at Harvard Sensor Network Lab, Wireless sensors placed on the patient's body transmit data to their own authorized devices. Any doctor/medical professional who requests for this medical info queries using their own personal device. Focuses more on robust scalable communication with less focus towards security. In the Code blue technology sensors are placed on the human body physically and then only it interacts with the human local processing unit devices. Such that to protect the patients vital information many securities are proposed here to keep safe the patients information. By using the IOT device it saves the sensor values and it contains the SIM slot it stores the information about the person whom the patients information should be given as alert.

Symbol	Definition
S	BSN care server
L	Local processing unit(LPU)
aidL	One time alias identity of the LPU
IdL	Identity of the LPU
Sid	Shadow identity of the LPU
kem	Shared emergency key between LPU and server
kls	Shared key between LPU and server
trseq	Track sequence number
Lai	Location area identifier
H(.)	One way hash function

© 2017 AJAST All rights reserved.

2. RELATED WORK

[1] Advancement in the wireless sensor network (WSN) and embedded computing technologies in healthcare monitoring devices is feasible. It provides continuous monitoring and analysis of the physiological parameter of the body. The aim of this system to control and quickly analysis of the patient's disease. It contains the Holter monitor. This Holter monitor can record up to 24 hours of ECG signals, and the recorded data is subsequently retrieved and analyzed by a clinician. They can also detect and signal a warning in real-time if any abnormal changes in the body is captured. Recent research has also focused on the development of wireless sensor networks (WSN) and monitoring systems for cardiac patients.

[2] WSN provides communication in the healthcare system. This sensor with advance Micro-Electro-Mechanical Systems (MEMS) technology, create a Body Sensor Network (BSN) that continuously monitors the abnormal changes in health of patients. This system designed for measuring health parameters of patient body in which it consists of temperature and pulse sensor, this sensor is connected to Base Station through a microcontroller and that device have the ability to be control and monitored by remote computer.

[3] The purpose of the unique healthcare monitoring system using sensor and Zigbee Technology that remotely measuring and monitoring the patient's physiological parameter of the body. This paper present by measuring and monitoring the patients' health information it monitors the ECG, lung functioning, heart rate and temperature signals. The proposed system can monitor the different aspect of the human body such as Blood Pressure, Electrocardiogram (ECG), Electroenchaplogram (EEG), Temperature, glucose, respiratory (spirometer). The system in which it gathered the information from patient through different aspect of body function and these information is transmitted to zigbee and from that zigbee it sends data from one zigbee to another zigbee, after receiving the information it display on the display module such as mobile of doctor or family or emergence unit.

[4] In this system it monitors complex patient handling activities. The patient having multiple IMU sensors on the body and this sensor are located at different location on the body. In this system in which automatically patient handling activity (PHA) recognition. The mostly important device used in this proposed system name as smart insole 2.0. This device wear on the patient body with rich number of sensor and all this sensor are capture the information of Patient Handling activity (PHA). The device Smart Insole 2.0, it utilizes an advanced electronic textile (etextile). This sensor technique providing accurate measurement in ambulatory and static status.

[5] This IOT device can communicate with each other via wireless or wired technology. The Internet of Things (riot) is an important concept. Its main purpose is to allow users to connect various sensors and smart devices to collect real-time data from the environment. E-Health and m-Health architectures are use smartphone sensors to sense the data from the patient and transmit important data related to a patient's health are to transmit to the doctor. All the medical professionals can access and view the data, take decision accordingly to provide services remotely.

3. SECURE IOT-BASED HEALTHCARE SYSTEM USING BSN (BSN-CARE)

Body Sensor Network (BSN) allows the in intelligent, miniaturized low-power sensor nodes in, on or around human body to monitor body functions and the surrounding environment. It 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. Now, our BSN-Care is a BSN architecture composed of wearable and implantable sensors. Each sensor node is integrated with biosensors such as

Electrocardiogram (ECG), Electromyography (EMG), Electroencephalography (EEG), 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. For example, in general BP less than or equal to 120 is normal, when the BP of the person reaches say 125, the LPU will provide a gentle alert to the person through the LPU devices (e.g. beep tone in a mobile phone). BSN-Care server receives data of a person (who wearing several bio sensors) from LPU, then feeds the BSN data into its database and analyzes those data. Subsequently, based on the degree of abnormalities', it may interact with the family members of the person, local physician, or even emergency unit of a nearby healthcare center. Precisely, considering a person (not necessarily a patient) wearing several bio sensors on his body and the BSN-Server receives a periodical updates from these sensors through lpu.

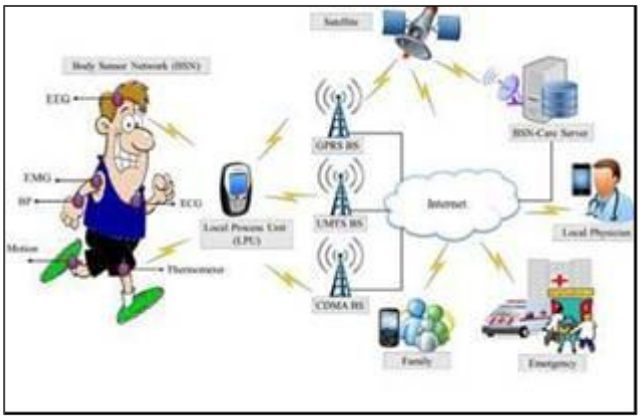

Fig.1 BSN Architecture

This feeds the BSN data into its database and analyzes those data. Subsequently, based on the degree of abnormalities', it may interact with the family members of the person, local

© 2017 AJAST All rights reserved.

physician, or even emergency unit of a nearby healthcare center. Precisely, considering a person (not necessarily a patient) wearing several bio sensors on his body and the BSN-Server receives a periodical updates from these sensors through lpu. Now, our BSN-Care server maintains an action table for each category of BSN data that it receives from lpu. Now, when the bp rate becomes greater than 130, then it informs family members of the person.

If the bp rate becomes greater than 145 and there is no one attending the call in family, then the server will contact the local physician. Furthermore, if the bp rate of the person cross 160 and still there is no response from the family member or the local physician then the BSN-Care server will inform an emergency unit of a healthcare center and securely provides the location of the person. Here, the response parameters "fr" (Family Response), "pr" (Physician Response), and "er" (Emergency Response) are the Boolean variables, which can be either true (t) or false (f). If the value of any response parameter is false, then the server repeats its action. For example, when the family response parameter "fr: f", then the server repeatedly call his family members. Once, the family members of the concern person pick-up the call, then the value of the family response parameter (fr) will become true i.e. "fr: t". Now, if "fr:f" and bp > 130 then the BSN-Care server will call the local physician. In case, when the physician also does not respond to the server's call, then the value of the physician response parameter "PR" will stay in false. In this regard, the server will repeatedly call both the family members and the physician. Unless any of the response parameter (FR, PR) value becomes true. Meanwhile, if "fr: f", "pr: f" and bp >160, then the BSN-Care server immediately inform to the emergency unit of a healthcare center nearest to the concern person. Once the emergency unit responds, then the value of the emergency response parameter "ER" will become true i.e. "er: t". It should be noted that, our BSN-Care system is not only designed for the patient, instead of that it can be useful for providing a decent quality of life for the aged people.

BSN bp data	**Action**	**Response**
bp <=120	None	Null
bp>130	Inform to the family	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

Table.2 BSN BP Data

4. SECURITY IN IOT BASED HEALTHCARE SYSTEM

By dividing security requirements as mentioned above into two parts

- Network security,
- Data security.

Network security contains authentication, anonymity, and secure localization. And data security includes data privacy, data integrity, and data freshness. By proposing the autonomous authentication protocol to accomplishment of the data security requirements.

A. Autonomous Authentication Protocol

In our BSN-Care system, when a LPU wants to send the periodical updates to BSN-Care server, then the server needs to confirm the identity of LPU using a lightweight anonymous authentication protocol. In this section we describe our anonymous authentication protocol in details. Our proposed authentication protocol consists of two phases: In Phase 1, the BSN- Care server issues security credentials to a LPU through secure channel, this phase is called registration phase. The next phase of the proposed authentication protocol is the anonymous authentication phase, where before data transmission from the LPU to BSN-Care server, both the LPU and the server will authenticate each other. So, the objective of our proposed lightweight authentication scheme is as follows:

- To attain mutual authentication property.
- To attain anonymity property.
- To attain secure localization property.
- To conquest forgery attacks.
- To reduce computation overhead.

Phase 1.Registration phase

A LPU [local processing unit] submits the identity idL the health care server through a secure channel. After receiving the request from LPU, the server generates the random number (R) and then computes

$$kls = H(idL \| R) \oplus idS$$

Subsequently, the server generates the unlinkable id's sid = {sid1, sid2, ...}, where for each sidj€sid, then the server computes the

sidj= H(idL ||rj||klS) then randomly the server generates a set of emergency keys kem={kem1, kem2 ,...}.corresponds to the sidj=sid server generates track sequence number trSeq, which is a sequence number of 32-bit. This sequence number is generated randomly. Further for each request of LPU, the server random generates number M and then sets trSeq = M and frequently sends trSeq to the LPU and keeps copy in the database, in which the server can see the recent track sequence number for each LPU idL registered into the

© 2017 AJAST All rights reserved.

system. This sequence number can be used to speed up the authentication process and to prevent any of the replay attempt from any, where by seeing the trSeq and comparing with the stored value of its database, the server can understand the LPU. Here, we assume that every person wearing the bio-sensor for monitoring the deformity of any organ, maintain LPU with unique identity idL.

Currently, during the execution of the anonymous authentication phase, if the trSeq provided by the LPU doesn't match the stored value of the healthcare server. Then the server will proximately stop the connection. In that case, the LPU will be asked to use it's one of the unused pair of shadow identity sidj ⊕ sid and emergency key kemj ⊕ kem. Just the once a pair of (sidj,kemj) is used up, then that must be deleted from the list by both the LPU and the server. Now, at the end of the registration phase, the server securely sends {kls,(sid,kem),trSeq,H(.)}to the LPU through the secure channel and then it stores a copy of idL,kls,(sid,Kek), and trSeq in its own database for further communication.

Phase II: Lightweight Anonymous Authentication Protocol
This phase achieves goals of mutual authentication among the LPU, and the server by preserving anonymity, and secure localization. This phase consists of the following steps:

Step 1 MA1: LPU→Server:{aidL, Nx, trSeq (If req.), EL, V1}.

The LPU generates a random number Nl and aidL = H (idL||kls||R||trSeq), el = lail ⊕ H(kls||Nl), Nx = kls ⊕ Nl,V1=h(Nl||LAIl||Kls).

At last, the LPU forms a request message MA1 besides then sends it to the Healthcare server. Here, lail is the location area identifier of the base station, which characterizes the physical connection between the LPU and the base station of a mobile network and it will used to provide secure localization. In case of loss of organization, the LPU needs to choose one of the unused pair of (sidj, kemj) and subsequently, assigns the sidj as aidL i.e. aidL = sidj and then assigns kemj as kls. In such case, LPU won't send any track sequence number trSeq in MA1

Step 2 MA2: Server→LPU :{ T r, V2,x(if req.)}.
Upon receiving the request message from the LPU, the server will checks the track sequence number trSeq is valid or not and instantaneously also computes and checks whether the parameters V1,aidL, and lail are valid or not. If so, then the server generates a random number m and assigns trSeqnew = m. Afterwards, the server computes tr=H (kls||idL||Nl)⊕trSeqnew, V2=H(tr||kls||idL||Nl) Lastly, the server computes the klsnew = H (kls||idL||trSeqnew and updates its database with trSeq = tr Seq new, kls = k lsnew. If any parameter is worthless then the server stops the connection request. In case if the server can't find any trSeq in MA1, then the server will validate the aidL first, where the system will try to diagnose the sidj in aidL. If so, then only the system (health-Care server) will proceed for any further computation and at the send it generates randomly a new shared key i.e. klsnew and encodes it by using the emergency key kemj (used on that particular transaction) and the real identity of the LPU idL, i.e. X= ktsnew ⊕H(idL||kemj) and sends the X with the other response parameters in MA2 .

Now, after receiving the response message MA2 the LPU. At first computes the H(tr||kls||idL||Nl) and Then Verifies whether it is equals to V2 or not. If so, then the LPU derives trSeqnew = H(kls||idL||Nl)⊕T r, klsnew h(kls||idL||trSeqnew) and subsequently updates and stores T rSeq = T rSeqnew , Kls = Klsnew for further communication.

In the healthcare system when the sensor needs to send BSN data to LPU. In that case, by assuming that both the sensor and the LPU can connect each other through the password-based conventional Bluetooth authentication process. However lightweight two-party authentication scheme can be used during the verification process between a sensor node and LPU.

A. Data Security in Health Care System
Data security is of the continuous anxiety in a healthcare infrastructure like BSN-Care. Actually several open questions remain. How safe and dependable are these clinical devices that are worn or implanted? How we can ensure that BSN- Care server received the unaltered data from LPU? How do we ensure data security in BSN. For example, a bio sensor sending ECG signal to patient is errored or altered such that wrong diagnosis and treatment are agreed which may cause even death.

Those issues are required to be considered. Now, in order to accomplish data privacy, data integrity, and the data freshness with the reasonable computational overhead, here we adopt an authenticated encryption scheme offset codebook (OCB) mode. OCB is well-suited for expeditious and secure data communication, where only encryption can guarantee both the secrecy and integrity of the data in a single pass without any additional cryptographic primitive like hash function, MAC, CRC support. Hence, OCB is also well-suited for the energy constrained sensor or LPU devices. In this subsection we briefly review the OCB authenticated encryption mode.

OCB: It is a block-cipher mode of operation that features authenticated encryption, which is provably secure and is parameterized on a block cipher of block size n and a tag of τ, where τ is defined such that an adversary is able to forge a valid cipher-text with the probability of 2−τ . OCB operates as follows. Let D be the arbitrary length data needs to be encrypted and authenticated, K be the encryption key, and N , be a non-repeating nonce. Encryption oracle of OCB takes in D, K, and N, and generates the cipher- text core C.

Concurrently, using the plain-text data D; OCB generates the cipher-text C and the Tag of length τ. Now, this output pair (C, T ag) is sent to the receiving end. After receiving (C, T ag), the receiving end performs reverse operation on C to arrive at plain-text data D. Then the receiver ensures that the T ag is as expected. If the receiver computes different T ag than the once in the cipher-text, the cipher-text is considered to be invalid. In this way, if the data D is divided into n blocks, then OCB needs only n + 1 encryption to support both the privacy and integrity.

© 2017 AJAST All rights reserved.

5. SECURITY ANALYSIS

In this segment, by demonstrating that this proposed health care system can satisfy the vital security requirements of IoT based healthcare system using BSN.

SR1: Achievement of the Mutual Authentication

Proof. In proposed scheme, the BSN-Care server authenticates the LPU by verifying the one-time-alias identity aidL, the track sequence number trSeq, and the parameter V1 in the request message of MA1, where a genuine LPU can form a valid request message MA1. Also, in case of loss of synchronization, server will authenticate the LPU by using the unused shadow identity sidj in aidL and the value of the request parameter V1, which must be equal to the H(Nl||lai||kls). On the other side, the LPU can authenticate the legality of the BSN-Care server by using the parameter V2, which must be equal to the H(t r||kls||idL||Nl). In proposed health Care system satisfy the mutual authentication property.

SR2: Achievement of the Anonymity

Proof. In this scheme, both the shadow identity with the emergency key pair and one-time-alias identity with track sequence number can firmness the issues like anonymity and untraceability. Since the usage of (shadow-ID, emergency key) pair in each round may cause excessive storage cost in both the LPU and healthcare server. Therefore, the concept of (shadow-ID, emergency key) pair we only use for dealing with de-synchronization or DoS attack, which may occur because of loss of synchronization between the LPU and the server. That can be comprehended, if the response message MA2 has been interrupted, so the LPU cannot receive message within a specific time period. In that case, only a reasonable number of (shadow-identities, emergency keys) pair is required to be stored. Besides, it should be noted that, during the execution of our anonymous authentication process, none of the parameter in the request message MA1 is allowed to send twice. This approach of the proposed scheme is quite effective for privacy against eavesdropper (PAE) to achieve.

SR3: Achievement of the Secure Localization

Proof. In healthcare applications, the estimation of the patient's location is important. In real-time applications, a lack of smart tracking approach may allow an attacker to send the incorrect location by using false signals [15]. Our proposed anonymous authentication scheme can easily resolve this issue. When the HealthCare server wants to know the patient location, then it will use the encoded location area identity i.e. EL, the server at first decodes the lail From it i.e. lail = EL ⊕ H (kls||Nl), which represents the physical connection between the LPU and the base station of a mobile network. Subsequently, the server will also ask the base station to provide its identity i.e. LAIl.

Then the server needs to verify whether the LAIl provided by the base station, is it equals to the lail in EL or not. If the verification is successful then the sever believes the legitimacy of the base station. In other words, the signal is not false. Hereafter the server can easily locate the LPU by using the lail, and eventually can reach the person having BSN.

SR4: Resistance to Replay and Forgery Attacks

Proof. Having intercepted previous communication, the attacker can replay the same message of the receiver or the sender to pass the verification process of the system. In proposed authentication protocol, none of the parameter in the request message MA1 can be sent twice. Hence, if the attacker tries to intercept and resend the same request message, then by using the most recent track sequence number or a valid shadow identity, the server can easily detect it. In similar way, if the attacker attempts to send the same response message MA2 to the LPU, then the LPU can easily comprehend that. In that case, the value of the Parameter V2 will not be equal to the H (tr||kls||idL||Nl).In this way our proposed anonymous authentication protocol can resist replay attacks. Now, an attacker may also attempt to intercept and modify any previous legal message of the LPU to pass the verification process of the server. In that case, the attacker needs to construct a valid request message MA1 with a valid track sequence number to pass the server's verification. However, to do that, he/she needs to extract the most recent track sequence number from t r, i.e. tr = H(kls||idL||Nl)⊕trSeqnew and the attacker also needs to know the secret shared key kls, which is quite impossible for him/her to figure out these are the unknown secrets and without prior knowledge of the attacker cannot convince the server. On the other hand, the attacker may masquerade as server to gain the benefits. In that case, the attacker needs to form a valid response message MA2 and for that also he/she needs to know the secret key kls. In this way, our proposed scheme can resist forgery attacks.

SR5: Achievement of the Data Security

Proof. As we mentioned before that data security comprises of the data privacy, data integrity, and data freshness. Due to the nature of the sensor network and wireless communication, the BSN data could easily be altered and replayed by the opponent; this cloud be dangerous in the case of life-critical events. OCB based data encryption can satisfy all the three properties of the data security, where any alternation of data and any replay attempt by an adversary can easily be detected using tag, which is unforgeable.

6. PROPOSED SYSTEM

At first by highlighting the major security requirements in BSN based modern healthcare system. Proposing a secure IoT based healthcare system using BSN. The body sensor network (BSN) technology is one of the core technologies of IoT developments in healthcare system, where a patient can be monitored using a collection of tiny-powered and lightweight wireless sensor nodes.

In existing system security issues were the main drawback. Due to the lack of security patient's vital information in lost and lets to the vulnerability.so that by proposing this technique using the IOT device connected to the microcontroller it alerts the hospital and the family and emergency ward. The IOT device contains the SIM slot which contains the SIM card for storing the contact details and then to alert the members at the other side. From the IOT device the information is passed to the cloud storage as a link whereas the IOT device contains the GPRS and the mobile data the emergency ward and the peoples who are important

© 2017 AJAST All rights reserved.

to the patient will get the information from the cloud storage as a link. In this it contains the IOT device to share the link to the cloud as information and then gives alert to the family, if they response then gives alert to the nearest clinic and then if the clinic also didn't response then it gives alert message to the emergency station. And this proposed system contains the four modules. And it contains the SIM slot to store the information. In the LCD device it displays the sensor values for each sensor for example ECG sensor, pulse rate sensor, and then the temperature sensor it contains the IC and the microchip.

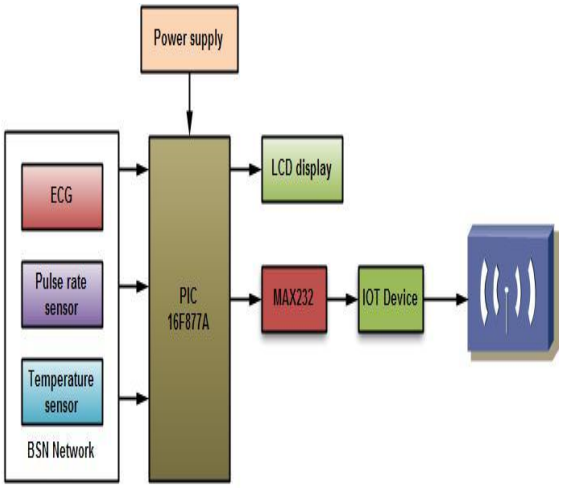

Fig 2: Block diagram of proposed system

7. SYSTEM MODULES

1. Sensors working
2. Sensor Data Read & Display
3. Serial Communication System & Sensor Monitoring
4. Sending Mail & Storage

1. Sensors working

Power supply is used to supply the overall power to the sensors and microcontroller. Read the values from the sensors such as ECG sensor, Pulse rate Sensor and Temperature sensor using micro controller. ECG sensor used the electrodes to detect the function of heart Pulse rate Sensor is used to measure the heart beat count per minute Temperature sensor is used to calculate the body temperature of a patient or person.

2. Sensor Data Read & Display

LCD display is an output device, which is used to display the all sensor values. LCD- Liquid Crystal Display

3. Serial communication system and sensor monitoring

In third Module, the communication takes place by using Max232 and RS232.Max232 is a logic converter, which is converting to TTL (Transistor –Transistor logic) into RS232 logic. Microcontroller works based on TTL (0 and 1) .IOT device is works based on RS232 (+9 voltage and -9 voltage) IOT device has SIM card for web application to share sensor information to the link.

4. Sending Mail & Storage

Computer has web application, which has Database. The Database is used to store the sensor values from the microcontroller. The Sensor values send to required mail (cloud link) using web application. The cloud link contains updatable values of BSN (Body Sensor Network).

8. CONCLUSION

In this paper we have demonstrated a secure IOT based healthcare system using an IOT device which provides security to the patient's vital information. In mobile physiological monitoring systems, sensor connected to microcontroller through wired communication and data from microcontroller are transmitted to cloud server through wireless communication. The computer has web application which has the database to store the patient's updates frequently and the sensor values are stored in the database from the microcontroller the sensor values are send to the required mail as a cloud link. The cloud link contains the updatable values of the sensor nodes. This system can be enhanced by acquiring other health parameter from the patient's body. In this paper, at first we have described the alert to doctor when abnormalities occurred in patient and privacy issues in healthcare applications using body sensor network (BSN). Subsequently, It is basically a collection of low-power and lightweight wireless sensor nodes that are used to monitor the human body functions and surrounding environment. Since BSN nodes are used to collect sensitive (life-critical) information and may operate in hostile environments, accordingly, they require keep records of patient to keep track of patient monitoring and future use of data. And major advantage is that to alert doctor and their colleagues to take instant action in case of abnormalities.

REFERENCES

[1] Body sensor network – a wireless sensor platform for pervasive healthcare monitoring [Benny P.L. Lo, Surapa Thiemjarus, Rachel King and Guang-Zhong Yang] 2015.

[2] Fuzzy Logic based Health Care System using Wireless Body Area [Prakashgoud Patil, Samina Mohsin, *Karnataka*, India] 2014.

[3] A Unique Health Care Monitoring System Using Sensors and Zig Bee Technology [EktaMadhyan Mahesh Kadam, *Department of Electronics & Telecommunications, Mumbai University, India]* 2013.

[4] Discovering Multidimensional Motifs in Physiological Signals for Personalized Healthcare. *[ArvindBal Subramanian, Jun Wang, and RamakrishnanPrabhakaran]* 2014.

[5] Dawlish A, and Hassanien AE 2012, 'Wearable and Implantable Wireless Sensor Network Solutions for Healthcare Monitoring Sensors', *12: 1237512376.*

[6] Ekta Madhyan and Mahesh Kadam2014, 'A Unique Health Care Monitoring System Using Sensors and ZigBee Technology', *International Journal of Advanced Research in Computer Science and Software Engineering* Volume 4, Issue 6.

© 2017 AJAST All rights reserved.

[7] Fen Miao and Xiuli Miao 2012, 'Mobile Healthcare System: Body Sensor Network Based MHealth System for Healthcare Application', E-*Health.*

[8] Bello and S. Zeadally, ''Intelligent device-to-device communication in the Internet of Things,'' *IEEE Syst. J.*, vol. 10, no. 3, pp. 1172–1182, Sep. 2016.

[9] X. Cai, Y. Wang, X. Zhang, and L. Luo, ''Design and implementation of a Wi-Fi sensor device management system,'' *Proc. IEEE World Forum Internet Things (WF-IoT),* Mar. 2014, pp. 10–14.

[10] Y. Kawamoto, H. Nishiyama, N. Kato, Y. Shimizu, A. Takahara, and T. Jiang, ''Effectively collecting data for the location-based authentication in Internet of Things,'' *IEEE Syst. J.*, vol. PP, no. 99, pp. 1–9, Sep. 2015, doi: 10.1109/JSYST.2015.2456878.

[11] S. Cirani, M. Picone, P. Gonizzi, L. Veltri, and G. Ferrari, ''IoT-OAS: An OAuth-based authorization service architecture for secure services in IoT scenarios,'' *IEEE Sensors J.*, vol. 15, no. 2, pp. 1224–1234, Feb. 2015.

[12] H. Ning, H. Liu, and L. T. Yang, ''Aggregated-proof based hierarchical authentication scheme for the Internet of Things,'' *IEEE Trans. Parallel Distrib. Syst.*, vol. 26, no. 3, pp. 657–667, Mar. 2015.

[13]Y. Hong, T. B. Patrick, and R. Gillis, "Protection of patient's privacy and data security in e-health services," in Biomedical Engineering and Informatics, 2008. *BMEI 2008. International Conference, vol. 1. IEEE,* 2008, pp. 643–647.

[14] A. Act, "Health insurance portability and accountability act of 1996," *Public Law*, vol. 104, p. 191, 1996.

[15] J. Kulynych and D. Korn, "The new hipaa (health insurance portability and accountability act of 1996) medical privacy rule help or hindrance for clinical research?" *Circulation,* vol. 108, no. 8, pp. 912–914, 2003.

[16] C.-M. Yang, H.-C. Lin, P. Chang, and W.-S. Jian, "Taiwan‟s perspective on electronic medical records security and privacy protection: Lessons learned from hipaa," *Computer methods and programs in biomedicine,* vol. 82, no. 3, pp.277–282, 2006.

[17] J. Collmann, D. Lambert, M. Brummett, D. DeFord, J. Coleman, T. Cooper, K. McCall, D. Seymour, C. Alberts, and A.Dorofee, "Beyond good practice: Why hipaa only addresses part of the data security problem," *in International Congress Series*, vol. 1268. Elsevier, 2004, pp. 113–118.

[18] V. Oleshchuk, "Internet of things and privacy preserving technologies," in Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronics Systems Technology, 2009. *Wireless VITAE 2009. 1st International Conference-IEEE,* 2009, pp. 336–340.

[19] H. Office for Civil Rights, "Standards for privacy of individually identifiable health information. final rule." *Federal Register*, vol. 67, no. 157, p. 53181, 2002.

[20] G. M. Stevens, "A brief summary of the medical privacy rule." *Congressional Research Service, Library of Congress,* 2003.

[21] S. Goldwasser, S. Micali, and R. L. Rivest, "A digital signature scheme secure against adaptive chosen-message attacks," *SIAM Journal on Computing*, vol. 17, no. 2, pp. 281–308, 1988.

[22] J. Sun, X. Zhu, and Y. Fang, "Preserving privacy in emergency response based on wireless body sensor networks," *in Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE. IEEE,* 2010, pp. 1–6.

[23] M. Evered and S. B¨ ogeholz, "A case study in access control requirements for a health information system," in *Proceedings of the second workshop on Australasian information security, Data Mining and Web Intelligence, and Software Internationalization Volume 32. Australian Computer Society, Inc.*, 2004, pp. 53–61.

[24] C. Karlof, N. Sastry, and D. Wagner, "Tinysec: a link layer security architecture for wireless sensor networks," in *Proceedings of the 2nd international conference on Embedded networked sensor systems. ACM, 2004*, pp. 162–175.

© 2017 AJAST All rights reserved.