INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS
ISSN 2320-7345

BODY SENSOR NETWORKING FOR HEALTH CARE

[1] M. Esakki, [2] Dr.Y.Harold Robinson Ph.D.,
[1] PG Scholar, 2 Associate Professor & Head
SCAD College of Engineering and Technology, Cheranmahadevi.

Abstract: - Body Sensor Network (BSN) which can be used mainly for Physiological monitoring (i.e., Blood Oxygenation, Pulse Rate, etc..)IoT based Body Sensor network should be implemented in order to improve security. It is mostly useful for the physicians and the patients for real time monitoring, patient information management and health care management. The security requirements can be satisfied using Attribute Based Encryption (ABE) algorithm. It is an type of public-key encryption in which the secret key of a user and the cipher text are dependent upon attributes. Here the patient id and name is used for encryption. It should be noted that if the BP rate of a person is less than or equal to 120, it is considered to be normal and the server does not perform any action. When the BP of the person reaches say 130, the LPU will provide a gentle alert to the person through the LPU devices like Phone, tablet, etc.. (e.g. beep tone) to the 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. Key Authority is needed for this to generate key for security purposes. The learning method contains lightweight anonymous authentication protocol and offset codebook mode where they are used for resolving the authentication problem. The proposed system contains Attribute Based Encryption (ABE) which resolves all the security requirements by taking the attributes separately and encrypting.

1. INTRODUCTION

The BSN based healthcare system is mainly used to automatically monitor the patient health condition and information management using a wearable or implanted sensors and then transmit it to the end user device. It consists of security and privacy issues which should be taken into consideration. BSN uses two types of sensor networks to transmit it to the end user device and they are In-body Sensor and On-body Sensor. 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. The security requirements are characterized into Network and Data security. To achieve the security requirements used this Lightweight Anonymous Authentication Protocol and OCB Authenticated Encryption Mode. The Security is not considered as an imperative aspect and thus it makes patient privacy vulnerable.

In this paper a secure IoT based healthcare system is proposed for patient health monitoring and information management which is called as BSN-Care. IoT allows seamless interactions among different types of devices such as medical sensor, monitoring cameras, and home appliances so on. The security requirements such as Network and data security is developed using some protocol named as Attribute Based Encryption (ABE). This project propose an IoT-aware architecture for healthcare remote monitoring systems for patients at home (suffering chronic diseases and or disabilities), which allows during runtime adding new sensors that become immediately available in order users may create/edit alerts' rules using also these new data.

1.2 ENFORCEMENT SECURITY REQUIREMENT

1.2.1 LIGHTWEIGHT ANONYMOUS 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 objectives of our proposed lightweight authentication scheme are as follows:

- To achieve mutual authentication property
- To achieve anonymity property
- To achieve secure localization property
- To defeat forgery attacks
- To reduce computation overhead

1.2.2 OFFSET CODEBOOK (OCB)

OCB mode was designed to provide both message authentication and privacy. It is essentially a scheme for integrating a Message Authentication Code (MAC) into the operation of a block cipher. In this way, OCB mode avoids the need to use two systems: a MAC for authentication and encryption for privacy. This result in lower computational cost compared to using separate encryption and authentication functions.

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.

2 RELATED WORKS

2.1 UBIQUITOUS MONITORING ENVIRONMENT FOR WEARABLE AND IMPLANTABLE SENSORS (UBIMON)

Ubiquitous Monitoring Environment for Wearable and Implanted Sensors shows the aim of having a UbiMon for wearable and implantable sensors is to provide continuous management of patients under their natural physiological states. The system is mainly used for collecting, gathering and analyzing data from number of sensors. The software for the BSN node is developed based on TinyOS. Instead of using the TinyOS protocol and radio stack, a lightweight protocol and special TDMA is developed to deal with the high data rate requirement of the ECG signal.

2.2 ALARM-NET: WIRELESS SENSOR NETWORKS FOR ASSISTED LIVING AND RESIDENTIAL MONITORING

WSN for assisted living and residential monitoring says ALARM-NET is used mainly used for assisted-living and residential monitoring. It integrates environmental and physiological sensors which allow real time collection and processing of sensor data. ALARM-NET integrates heterogeneous devices in a common architecture, spanning wearable body networks, emplaced wireless sensors, and IP-network elements. A query protocol allows real-time collection and processing of sensor data by user interfaces and back-end analysis programs.

2.3 CODEBLUE: AN AD HOC SENSOR NETWORK INFRA STRUCTURE FOR EMERGENCY MEDICAL CARE

Sensor devices integrating embedded processors, low-power, low bandwidth radios, and a modest amount of storage have the potential to enhance emergency medical care. Wearable vital sign sensors can track patient status and location, while simultaneously operating as active tags. Code Blue will enhance first responders' ability to assess patients on scene, ensure seamless transfer of data among caregivers, and facilitate efficient allocation of hospital resources. Intended to scale to very dense networks with thousands of devices and extremely volatile network conditions, this infrastructure will support reliable, ad hoc data delivery, a flexible naming and discovery scheme, and a decentralized security model.

2.4 UNTRACEABLE SENSOR MOVEMENT IN DISTRIBUTED IOT INFRA-STRUCTURE

IoT allows people and objects in the physical world as well as data and virtual environments to interact with each other so as to create smart environments, such as smart transport systems, smart cities, smart health, and so on. However, IoT raises some important questions and also introduces new challenges for the security of systems and processes and the privacy of individuals, such as their location and movements and so on. Here, a distributed IoT system architecture.

3. DEPLOYMENT STRATEGY

3.1 REGISTRATION

In this module, registration of a Patient's, personal details such as, Name, and Contact No will be stored and patient ID will be given to the every Patient, physician registration and also family member registration takes place. Determining whether the person has been previously registered by searching a database and reviewing possible matches.

3.2 KEY AUTHORITY

These are key generation centers that generate public/secret parameters. The key authorities consist of a central authority and multiple local authorities. We assume that there are secure and reliable communication channels between a central authority and each local authority during the initial key setup and generation phase. Each local authority manages different attributes and issues corresponding attribute keys to users. They grant differential access rights to individual users. The key authorities are assumed to be honest-but-curious. That is, they will honestly execute the assigned tasks in the system , however they would like to learn information of encrypted contents as much as possible.

3.3 LPU

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. After authenticating the ID, the LPU and server interact with each other.

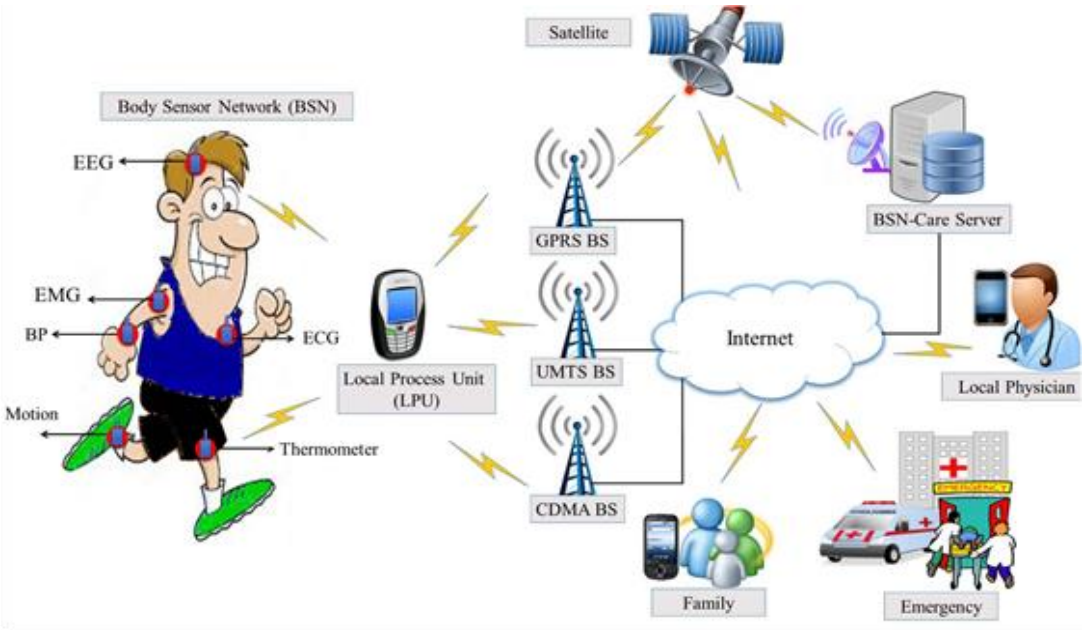
3.4 BSN CARE SERVER

The BSN-Care server receives data of a person (who wearing several bio sensors) from LPU, then it feeds the BSN data into its database and analyzes those data. It may interact with the family members of the person, local physician, or even emergency unit of a nearby healthcare center. BSN-Care server maintains an action table for each category of BSN data that it receives from LPU.

4. 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

5. SYSTEM ARCHITECTURE



6. CONCLUSION

The security and the privacy issues in healthcare applications are considered as most imperative aspect in IoT based Body Sensor Network (BSN). Subsequently, by using Attribute Based Encryption (ABE) the security issues is satisfied. Key authority also helps in providing the key for a particular patient in order to maintain their health records securely. 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.

7. REFERENCES

[1] P. Gope and T. Hwang (2015), "Untraceable sensor movement in distributed IoT infrastructure," IEEE Sensors J., vol. 15, no. 9, pp. 5340–5348.

[2] D. Malan, T. Fulford-Jones, M. Welsh, and S. Moulton (2004), "CodeBlue: An ad hoc sensor network infrastructure for emergency medical care," in Proc. MobiSys Workshop Appl. Mobile Embedded Syst. (WAMES), Boston, MA, USA, pp. 1–8.

[3] J. W. P. Ng et al (2004), "Ubiquitous monitoring environment for wearable and implantable sensors (UbiMon)," in Proc. 6th Int. Conf. Ubiquitous Comput. (UbiComp), Nottingham, U.K., , pp. 1–2.

[4] A.Wood et al (2006), "ALARM-NET: Wireless sensor networks for assisted living and residential monitoring," Dept. Comput. Sci., Univ. Virginia, Charlottesville, VA, USA, Tech. Rep. CS-2006-01.