International Journal of Computer Science Engineering & Technology
IJCSET
APPROVED BY
NATIONAL SCIENCE LIBRARY (NSL)
NATIONAL INSTITUTE OF SCIENCE COMMUNICATION AND INFORMATION RESOURCES (NISCAIR)
COUNCIL OF SCIENTIFIC AND INDUSTRIAL RESEARCH (CSIR)– NEW DELHI INDIA .
ISSN :2455-9091

SECURE BSN-CARE INHEALTHCARE SYSTEM USING HYBRID ATTRIBUTE BASED ENCRYPTION

[1] P. Priyanka, [2] Mr. N. Magendiran, M.E.,Ph.D.,
[1] Research Scholar, [2] Assistant professor in computer science
[1, 2] PaavaiEngineering CollegePavai Engineering College (Autonomous)
[1, 2] Namakkal(DT), Tamilnadu.

ABSTRACT: The Body Sensor Network (BSN) technology is one of the core technologies of Internet of Things (IoT) developments in healthcare system, where a patient can be monitored using a collection of tiny-powered and lightweight wireless sensor nodes. However, the development of this new technology in healthcare applications without considering security makes patient privacy vulnerable (week). BSN nodes are used to collect sensitive (life-critical) information and may operate in hostile environments, accordingly, they require strict security mechanisms to prevent malicious interaction with the system. In the health care environment keeping data confidential does not protect it from external modifications. It highlight the major security requirements in BSN-based modern healthcare system. Subsequently, it propose a secure IoT-based healthcare system using HABE, called BSN-Care (HABE), which can efficiently accomplish those requirements.

KEY WORDS: [Body Sensor Network (BSN), HABE (HybridAttribute Based Encryption), Radio Frequency Identification (RFID), Universal Mobile Telecommunication Standard (UMTS), Wireless sensor Network (WSN), Electrocardiogram (ECG), Electromyography (EMG), Electroencephalography (EEG), Blood Pressure (BP), Local Processing Unit (LPU),Global Mobility Networking (GLOMONET).]

1. INTRODUCTION

Lightweightwireless sensor nodes that are used to monitor the human body functions and surrounding environment. Since BSN nodes are used to collect sensitive information and may operate in hostile environments, accordingly, they require strict security mechanisms to prevent malicious interaction with the system. The healthcare remote monitoring systems have become a key contributor to the improvement of the elderly people' quality of life. The market sector of healthcare remote monitoring systems has increased significantly due to several reasons. The number of elderly people is increasing over the time where today in developed countries it is quite normal that elderly people usually live independently in their own homes. Furthermore, Internet of things (IoT) makes these healthcare remote monitoring systems technically feasible (IoT as the concept of a monitor able and modifiable world in which sensors and actuators over living and non-living objects) and the even decreasing cost of sensors makes it economically feasible.

Due to the penetration of smart mobile technology, it is also expected that population is already prepared to accept this kind of solutions collecting in real time people's private and sensitive data such as temperature, blood glucose, heartbeat, pulse sensor to name a few. For instance, healthcare personal analyzers such as smart beds automatically inform who are occupying them and even more, they are able to inform about different patients' physiological levels, making real smart home medication dispensers to, for instance, automatically alert when medication is not taken. Several healthcare remote monitoring systems using different technology for monitoring and/or tracking patients and/or biomedical equipment within Hospitals and at their homes. Unfortunately, as far as itknow, most of these solutions are not flexible at the moment of adding new sensors during runtime. Neither it allows normal users to create ad-hoc alerts immediately with the new sensors added. 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.

In this Existing system operates as the medical professional used three electrodes of ECG on the patient's body and connect with a temperature sensor, a blood glucose level sensor and a blood pressure sensor. It connect a wireless node and the Tablet or the Smartphone that has Lab View software running on it to take reading of the patient's physiological data. The data are saved according to the time and presented in a report format and the data is then published in the internet by using tablet or smart phone so that the patient's report can be accessed by the authorized healthcare persons from remote locations at any time.

Even though all the existing state-of-the-art BSN based healthcare solutions addressed the requirement for security and privacy for the sensitive data, but only three of them Alarm-net, Median, BSN Care embedded any security. Keeping data confidential does not protect it from external modifications, BSN should modify patient's vital information to external or neighboring network, Network security comprises authentication.

Related work

P. Gope and T. Hwang, says Untraceable sensor movement in distributed IoT infrastructureRecent advances in information and communication technologies and embedded systems have given rise to a new disruptive technology, the Internet of Things (IoTs). IoT allows people and objects in the physical world as 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. In this paper, at first, it propose a distributed IoT system architecture. Subsequently, it propose an anonymous authentication scheme, which can ensure some of the notable properties, such as sensor anonymity, sensor untraceability, resistance to replay attacks, cloning attacks, and so on. It is argued that the proposed authentication scheme will be useful in many distributed IoT applications (such as radio-frequency identification-based IoT system, Biosensor-based IoT healthcare system, and so on), where the privacy of the sensor movement is greatly desirable.

P. Gope and T. Hwang says A realistic lightweight authentication protocol preserving strong anonymity for securing RFID system Radio Frequency Identification (RFID) system is a contactless automatic identification system using small, low-cost RFID tag to an animate or inanimate object. Because of the advantage of simultaneous recognition of massive amounts of information, it is expected to replace the traditional bar-code system.

However, two major issues with an RFID system are: i) an adversary can access the tag information, which may cause privacy and forgery problems; ii) the computational capability of the RFID tags is very limited. Although, to deal with these issues, impressive efforts have been made by designing anonymous authentication schemes with the help of lightweight cryptographic primitives such as one way hash function, symmetric key encryption/decryption, exclusive-OR. However, to the best of knowledge none has succeeded so far. In this article, ittake an initial step to shed light on the rationale underlying this prominent issue. In order to do that, it will first demonstrate that the existing lightweight cryptographic primitive based anonymous authentication protocols in RFID systems are impractical. Subsequently, it propose a realistic lightweight authentication protocol for RFID system, which can ensure various imperative security properties such as anonymity of the RFID tag, untraceability, forward security etc.

T. Hwang and P. Gope Says Provably secure mutual authentication and key exchange scheme for expeditious mobile communication through synchronously one-time secrets the Universal Mobile Telecommunication Standard (UMTS) is continuously evolving to meet the increasing demand of modern mobile and Internet applications for high capacity and advanced features in security and quality of service. Although admittedly enhanced in terms of security as compared to GSM (2G) systems, UMTS still has some may often lead to several security incidents. In this article, it come up with a novel authentication mechanism based on the one-time-secret security capabilities, which can assure an expeditious mobile communication environment and simultaneously be able to deal with the several issues related to security vulnerabilities (Redirection Attack, Man-in-the-Middle-Attack) and others like the excessive bandwidth consumption, storage overhead in VLR etc. existing in the current mobile communication (UMTS). In addition, here it also introduce a new concept called “Neighborhood Policy”, where several VLRs can form groups among themselves and carry out significant responsibilities in order to authenticate a User without interfering HLRs even though the User moves to a new VLR (belongs to the same group). It saysthat the proposed solution not only achieves the mutual authentication in a secure manner, but at the same time, it also greatly reduces the computation and communication cost of the mobile User as compared to the existing state of the art authentication schemes.

P. Gope and T. Hwangdescribe Enhanced secure mutual authentication and key agreement scheme preserving user anonymity in global mobile networks,Rapid development of wireless networks brings about many security problems in mobile communications. In this regard, designing a secure user authentication scheme, especially for recognizing legal roaming users is indeed a challenging task. Recently, Qi et al. proposed such scheme, which is claimed to be a slight modification of Qi et al.’s protocol based on smart card. However, itreveal that both the schemes still suffer from certain weaknesses and thus they cannot achieve desired security. Therefore, here it propose an improved protocol of Qi et al. which can immune to various known types of attacks like forgery attack, replay attack, known session key attack, backward and forward secrecy etc.

P. Kumar and H.-J. Lee describes Security issues in healthcare applications using wireless medical sensor networks: A surveysaysHealthcare applications are considered as promising fields for wireless sensornetworks, where patients can be monitored using wireless medical sensor networks(WMSNs). Current WMSN healthcare research trends focus on patient reliablecommunication, patient mobility, and energy-efficient routing, as a few examples. However,deploying new technologies in healthcare applications without considering security makespatient privacy vulnerable.

Moreover, the physiological data of an individual are highlysensitive. Therefore, security is a paramount requirement of healthcare applications,especially in the case of patient privacy, if the patient has an embarrassing disease. It discusses the security and privacy issues in healthcare application using WMSNs.

Ithighlight some popular healthcare projects using wireless medical sensor networks and discuss their security. Itaim is to instigate discussion on these critical issues sincethe success of healthcare application depends directly on patient security and privacy, forethic as it as legal reasons.

In addition, itdiscuss the issues with existing securitymechanisms, and sketch out the important security requirements for such applications.Inaddition, the paper reviews existing schemes that have been recently proposed to providesecurity solutions in wireless healthcare scenarios. Finally, the paper ends up with asummary of open security research issues that need to be explored for future healthcareapplications using WMSNs.

2. SYSTEM MODEL

It proposes a secure IoT-based healthcare system using BSN, called Secure BSN-Care, which can efficiently accomplish those requirements.Now, the communication in sensor network applications (like BSN) in healthcare are mostly wireless in nature. This may result in various security threats to these systems. These are the security issues cloud pose serious problems to the wireless sensor devices.

In proposed BSN-Care healthcare system, HABE (HybridAttribute Based Encryption)is used for ensuring the all the requirements of the data security. Here itshow that HABE - based data security approach causes significantly more security as compared OCB, AES-CBC encryption with CBC-MAC.(Data Privacy, Data Integrity, Data Freshness, Authentication, Anonymity,Secure Localization)

Merits of Proposed System

BSN-Care healthcare system, it use HABE for ensuring the all the requirements of the data security. Here it show that HABE-based data security approach causes significantly less computational overhead as compared AES-CBC encryption with CBC-MAC and OCB.

1.HABE is required to protect the data from disclosure.

2.No Data loss can also occur due to the bad communication

3.Proposed authentication protocol is very secure compare then existing Technique and Algorithm.

Architecture Design

SECURE IoT- BASED MODERN HEALTHCARE SYSTEM USING BSN

3. PROBLEM DESCRIPTION

Attribute-based encryption is a type of public-key encryption in which the secret key of a user and the ciphertext are dependent upon attributes (e.g. the country in which he lives, or the kind of subscription he has). In such a system, the decryption of a ciphertext is possible only if the set of attributes of the user key matches the attributes of the ciphertext. A crucial security aspect of Attribute-Based Encryption is collusion-resistance: An adversary that holds multiple keys should only be able to access data if at least one individual key grants access Each sensor node is integrated with bio-sensors 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 with the BSN nodes and the central server called BSN-Care server, using the wireless communication mediums such as mobile networks 3G/CDMA/GPRS.

In itBSN-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 itdescribeanonymous authentication protocol in details.Itproposed 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 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) Phase I (Registration Phase):

A LPU submits its identity I DLto the BSN-Care server through a secure channel. After receiving the request from LPU, the server generates a random number NS and then computes

KLS=H(I DL||Ns)⊕I DS

Subsequently, the server generates a set of un linkable shadow-IDs SID={sid1,sid2) , where for each sidj∈ SID, the server computes idj=h(I DL||r j||Kls). Then the server also randomly generates a set of emergency keys kem={kem1,kem2,….}, each corresponds to a particularsidj∈ SID. Hereafter, the server generates a track sequence number TrSeq, which is basically a sequence number of 32-bit. This sequence number is randomly generated. Precisely, for each request of the LPU, the server generates random number m and then sets TrSeq= m and subsequently sendsTrSeqto the LPU and keeps a copy in its database, in which the server can see the most recent track sequence number for each LPU I DLregistered into the system. This sequence number can be used to speed up the authentication process as it as to prevent any replay attempt from any adversary, where by seeing the TrSeqand comparing it with the stored value of its database, the server can comprehend the LPU. Here, it assume that each person bio-sensor for monitoring the abnormality of any of the organ, maintain a LPU with unique identity I DL.

Now, during the execution of the anonymous authentication phase, if theTrSeqprovided by the LPU does not match withthe stored value of the BSN-Care server. Then the server will immediately terminate the connection. In that case, the LPU will be asked to use it's one of the unused pair of shadow identity sidj∈SIDand emergency keykem j ∈kem. Once a pair of (sidj,kem j)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 ofIDL,Kls,(SID,Kem) and TrSeqin its own database for further communication.

2) 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(I freq.),EL,V1}:The LPU generates a random numberNland derives AIDL=h(I DL||Kls||Nl||TrSeq),EL=LAIl⊕h(Kls||Nl), Nx=Kls⊕ Nl,V1=h(Nl||LAIl||Kls).

Finally, the LPU forms a request message MA1 and then sends it to the BSN Care server. Here,LAIlis the location area identifier of the base station, which represents the physical connection to the LPU and the base station of a mobile network and it will It divide the all security requirements into two parts: network security, and data ecurity. Network security comprises authentication, anonymity, and secure localization. On the other hand, data security includes data privacy, data integrity, and data freshness.

Now, to the best of the knowledge there is no two-party authentication protocol which can achieve all the aforesaid properties of the network security. Hence, in order to achieve all the network security requirements here itpropose a lightweight anonymous authentication protocol. Subsequently, to accomplish all the data security requirements it adopt OCB authenticated encryption mode. Itproposea Secure lightweight anonymous authentication protocol. To accomplish all the data security requirements it adopt HABE authenticated encryption mode.

4. SYSTEM MODULES

1. **Login**
2. **Patient Registration**
3. **Key Authorities**
4. **LPU (Secure Lightweight Anonymous Authentication Protocol)**
5. **BSN Care Server**

PROJECT DESCRIPTION

Login

This module used to logon is the procedure used to get access to an operating system or application, usually in a remote computer. Almost always a logon requires that the user have (1) a user ID and (2) a password. Often, the user ID must conform to a limited length such as eight characters and the password must contain at least one digit and not match a natural language word. The user ID can be freely known and is visible when entered at a keyboard or other input device. The password must be kept secret (and is not displayed as it is entered). Some sites require users to register in order to use the site; registered users can then enter the site by logging on.

Patient Registration

In this module, Patient's personal details such as, Name, Contact No will be stored and patient ID will be given to the Every Patient presentation or booking contact, Collection of registration information into a system, Determining whether the person has been previously registered by searching a database and reviewing possible matches.

Key Authorities

They are key generation centers that generate public/secret parameters. The key authorities consist of a central authority and multiple local authorities. It assume that there are secure and reliable communication channels 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.

LPU (Lightweight Anonymous Authentication Protocol)

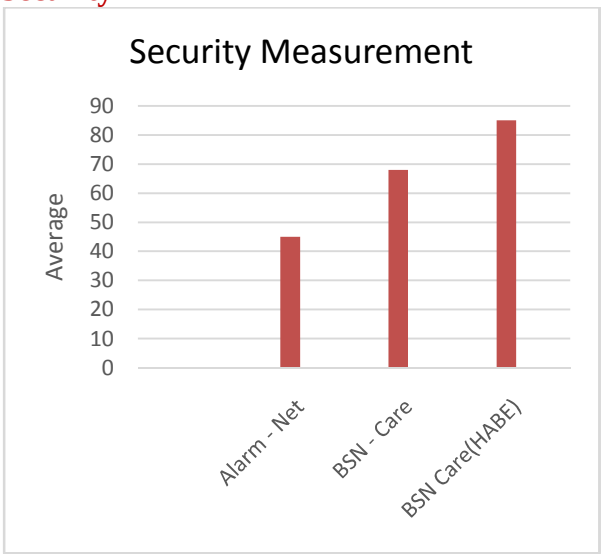
In itBSN-Care system, when a LPU wants to send theperiodical updates to BSN-Care server, then the server needsto confirm the identity of LPU.

BSN Care Server:

The BSN-Care server receives data of a person (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. ItBSN-Care server maintains an action table for each category of BSN data that it receives from LPU.

Performance benchmarking based on Security



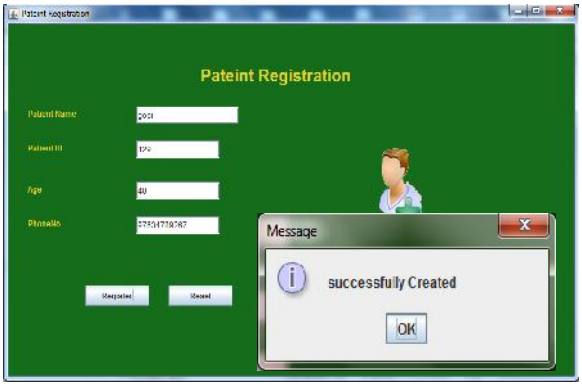
5. PARTIAL RESULTS

Sample Screen Shots

REGISTRATION FORM

6. ADMINISTRATION FORM

7. PATIENT REGISTRATION



CONCLUSION

In the modern health care environment, the usage of IoT technologies brings convenience of physicians and patients since they are applied to various medical areas (such as real-time monitoring, patient information management, and healthcare management). However, designing an expeditious anonymous-user authentication scheme in the Global Mobility Networking (GLOMONET) environment is always a challenging task. It proposed framework HABE and Secure IoT - based Healthcare System Using Body Sensor Network .It propose a secure IoT based healthcare system using BSN, called BSN-

Care, which can efficiently accomplish those requirements. In BSN-Care system, when sensor nodes send data to the LPU unit then they need to use HABE encryption mode with fresh nonce Nand the shared key K, the nodes and the LPU. Similarly, when LPU sends the periodical updates of the sensor data then LPU also needs to use encryption mode with a fresh nonce and the updated shared key Kls the LPU and the BSN-Care server for encipher the periodic data. Therefore, when the LPU receives the data from any sensor node then apart from privacy it can also check the integrity and freshness of the data. Similarly, the BSN-Care server receives the periodic updates from LPU then it can checks the privacy, integrity, and the freshness of the received data. Finally send SMS to all members of BSN-Care Server User.

REFERENCES

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

[2]. P. Gope and T. Hwang, "A realistic lightweight authentication protocol preserving strong anonymity for securing RFID system," Comput.secure., vol. 55, pp. 271–280, Nov. 2015.

[3]. T. Hwang and P. Gope, "Provably secure mutual authentication and key exchange scheme for expeditious mobile communication through synchronously one-time secrets," Wireless perscommun.,. vol. 77, no. 1, pp. 197–224, Jul. 2014.

[4]. P.Gope and T.Hwang ,"Enhanced secure mutual authentication and key agreement scheme preserving user anonymity in global mobile networks":wirelesspers commun.,vol.82,issue 4,pp 2231-2245,8 feb 2015.

[5]. P. Kumar and H.-J. Lee, "Security issues in healthcare applications using wireless medical sensor networks: A survey,"sensor , vol. 12, no. 1, pp. 55–91, 2012.

[6]. R. weinstein, "RFID: A technical overview and its application to the enterprise," IEEE IT Prof., vol. 7, no. 3, pp. 27–33, May/Jun. 2005.

[7]. R. Chakravorty, "A programmable service architecture for mobile medical care," Conf.PervasiveComput.Commun.Workshop(PERSOMV), Pisa, Italy, Mar. 2006, pp. 531–536.

[8]. J. W. P. Ng et al., "Ubiquitous monitoring environment for wearable and implantable sensor (UbiMon),"inPROC.6th.Conf.Ubiquitious.Comput. (Ubicomp), Nottingham, U.K., Sep. 2004, pp. 1–2.