International Research Journal of Computer Science (IRJCS)
Issue 5, Volume 2 (May 2015)
ISSN: 2393-9842
www.irjcs.com

SAFEGUARDING PATIENTS' MEDICAL RECORDS IN A REMOTE MEDICAL MONITORING SYSTEM

Anigbogu, Sylvanus O.
Dept. of Computer Science
Nnamdi Azikiwe University, Awka

Oji, Ifeoma V.
Dept of General Studies
Petroluem Training Institute, Effurun

Abstract- Remote medical monitoring requires the monitoring of the vital signs of patients in a remote location and sending same to a central monitoring station for doctor's assessment and intervention. This is achieved by embedding the patients with sensors creating a Body Sensor Network (BSN) which collect the information from the patients and transmit these information through networking by using wireless routers or the internet. As the patients' medical records travel through the networks, they are exposed to hackers who may intercept and change the records which can be detrimental to the patients. Communication of health related information between sensors in BSN and the remote medical server has to be strictly private and confidential to protect patient privacy. To overcome unauthorised access to patients' medical records, the sensor information is encrypted as it travels from the sensors to the central monitoring system. This research work simulates the patient id, blood pressure and pulse rate, encrypts the patient id which contains the patient's medical records and sends it to the database. The encryption is done by using the symmetric key encryption algorithm which employs the Advanced Encryption Standard to produce the cipher text which is the encrypted text sent to the central monitoring station where it can be decrypted by persons with authorised access. The encryption program is written in java because of its portability and web based features. The result of this research effort is the efficient protection of the patients' medical records as it travels through the networks in a Remote Medical Monitoring System.

Keywords: Remote Medical Monitoring, Encryption, Body Sensor Network, Blood Pressure, Database

I. INTRODUCTION

Remote medical monitoring of patients requires monitoring the physiological state of patients with acute or chronic conditions or chronic disease states which requires intensive condition tracking. More particularly, the invention is directed to a condition monitoring system which includes one or more remote modular testing units and a central station. The remote units include physiological parameter testing modules to acquire data from one or possibly many patients and communicate with a central station typically capable of interfacing with a large number of patient-operated units or clinician-operated units testing many patients. The central station, in turn, may interface and communicate with any number of other devices as by networking. Parameters checked may include but are not limited to blood pressure, pulse rate, blood oxygen saturation, weight, blood glucose, temperature, prothrombin (clotting) time and pulmonary function, including respiratory rate and depth. Other functions, such as ECG (electrocardiograph) traces and infant breathing monitoring for detection of SIDS (sudden infant death syndrome) onset are also contemplated [4].

Persons requiring critical care; patients who have undergone surgery or persons with chronic ailments require continuous health monitoring and real-time feedback for immediate action in emergency situations. The patients would be subjected to discomfort and inconvenience due to prolonged hospitalization. Frequent visits to hospitals may also be required for follow up treatment and care. Use of Body Sensor Network can provide an alternative solution for remote monitoring of patients residing in the comfort of the homes. Patients can move about and follow their daily routine without the necessity of being confined to their beds. Data obtained over a long period of time in the patient's natural environment would offer the doctors a better insight into the patient's health condition and such data can be analyzed to arrive at the correct diagnosis and provide the right care [4].

Communication of health related information between sensors in BSN and the remote medical server has to be strictly private and confidential to protect patient privacy [1]. The sensor data sent using Internet and wireless transmission is prone to different types of attack such as eavesdropping, sending false values or replay of previous data. Medical professionals have to be certain that the data is not tampered on transit or at a point of origin as proper diagnosis requires accurate data.

II. RELATED WORK

SPINS [5] a paper on Security Protocols for Sensor Networks provides confidentiality and authentication using symmetric cryptography. SPINS made use of two protocols, SNEP (Secure Network Encryption Protocol) which provides confidentiality and authentication and TELSA (Timed, Efficient, Streaming, Loss-tolerant Authentication protocol) which provides authenticated broadcast for severely resource-constrained environments.

These schemes are however more generic in nature and the unique security requirements of medical applications were not addressed. Conventional public key cryptographic systems cannot be directly applied due to constraints in sensor power and memory.

CodeBlue, a Harvard University project is designed to provide routing, naming, discovery and security for wireless medical sensors [6]. ALARMNET, a system for assisted-living and residential monitoring that uses a two-way flow of data and analysis between the front and back-ends to enable context-aware protocols that are tailored to residents' individual patterns of living [8]. It uses Advanced Encryption Standard (AES) for encryption of data transmitted over the network. The paper discusses query management, context aware privacy, power management and IP network security. The paper did not discuss issues related to key management. I-LIVING is an Open System Architecture for Assisted Living [7] that allows independent parties work together in a dependable, secure and low-cost fashion with predictable properties. Wireless Sensor Network for Wearable Physiological Monitoring [3] discusses a fabric embedded with sensors that monitor the physiological parameters and transmit wirelessly to a remote monitoring station.

Cherkuri et al discussed the use of biometrics for securing the communication between the sensors implanted in the body [2]. They proposed a system in which sensors are implanted in the human body which monitors the health condition of the person. They also propose an approach where the biometrics derived from the body is used for securing the keying material. This work did not take up any other security features.

III SYSTEM ARCHITECTURE

As the patients' medical records travel across networks, it is pertinent that they are protected against unauthorized access which might intercept the data along the way.

In view of this, the patients' medical records are encrypted as they travel across the networks, from the Patient Data Acquisition Centre (PDAC) to the Central Hospital Monitoring System. This encryption is done by using the symmetric key encryption algorithm which employs the Advanced Encryption Standard (AES). In the encryption, the original text called the plaintext is encrypted using an encryption algorithm, to generate the encrypted text called the cipher text that can only be read if decrypted.

The encryption scheme uses a pseudo-random encryption key generated by the algorithm. In the symmetric key scheme, the encryption and decryption keys are the same, thus communicating parties must have the same key before they can achieve secret communication.

The encrypted text which is the cipher text is decrypted in the server by only authorized users using the decryption key which is the same key as the encrypted key.

In the security architecture, each patient is assigned a unique ID called Patient ID (PID) which is generated using random number generation. The patient id generated is automatically encrypted. The patients' data are simulated with the Simulated Patient Data Software (SPDS) and sent to the Patient Data Acquisition Centre (PDAC) through wireless connection for consolidation and further transmission to the Central Hospital Monitoring System (CHMS) for processing and follow up by the medical care givers. The security architecture is shown in Fig. 1.

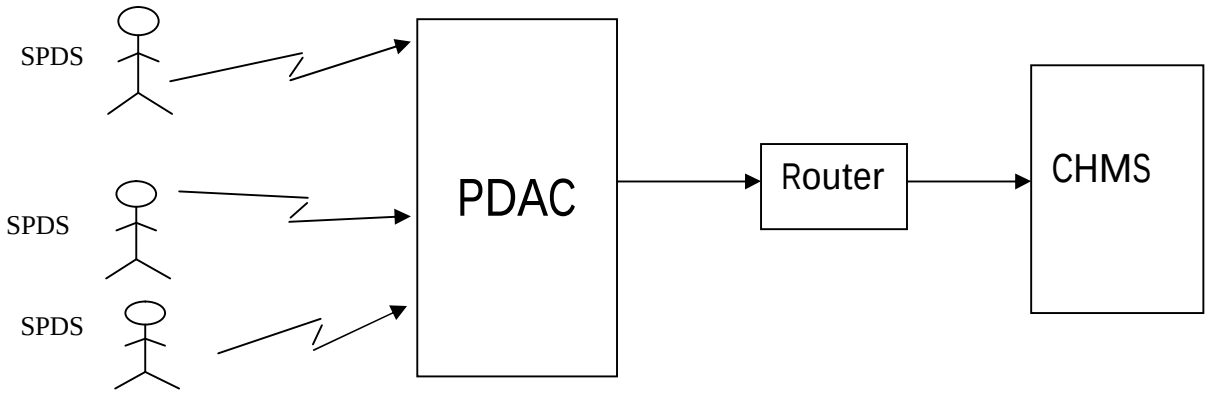

Fig 1: The Security Architecture

Each patient is identified with a unique ID called Patient ID (PID). The PID identifies the origin of the data. The transmission of patient medical data between the PDAC and the CHMS can be carried out by using a wireless router or the internet. The patients can be at home carrying out their normal duties while their physiological parameters are being monitored. Medical personnel can also monitor the patient data and alert the experts in emergency situations. Wireless transmission can be insecure and prone to data loss. Therefore the security of the patient data is of utmost importance and this is ensured by encryption and decryption of the patient data as it travels from the PDAC to the CHMS. Two physiological parameters; namely, Blood Pressure and Pulse Rate are monitored. The normal values of the parameters are given in Table 1. [5]

TABLE 1: SPECIFICATION OF VITAL PARAMETERS MONITORED

Vital Parameters	Specification
Blood Pressure	Systolic: 60- 200mm Hg Diastolic: 50 – 110mm Hg
Pulse Rate	72 – 90 beats per minute

The two parameters (Blood Pressure and Pulse Rate) are generated for continuous monitoring of the patients and the encryption and decryption process was done by using the Symmetric Key Encryption Algorithm.

A. Data encryption and authentication

The patient data sent from the PDAC to CHMS is encrypted using the symmetric key encryption algorithm and the secret key used is the generated key, k_s. The block diagram of the encryption and authentication is given in fig. 2.

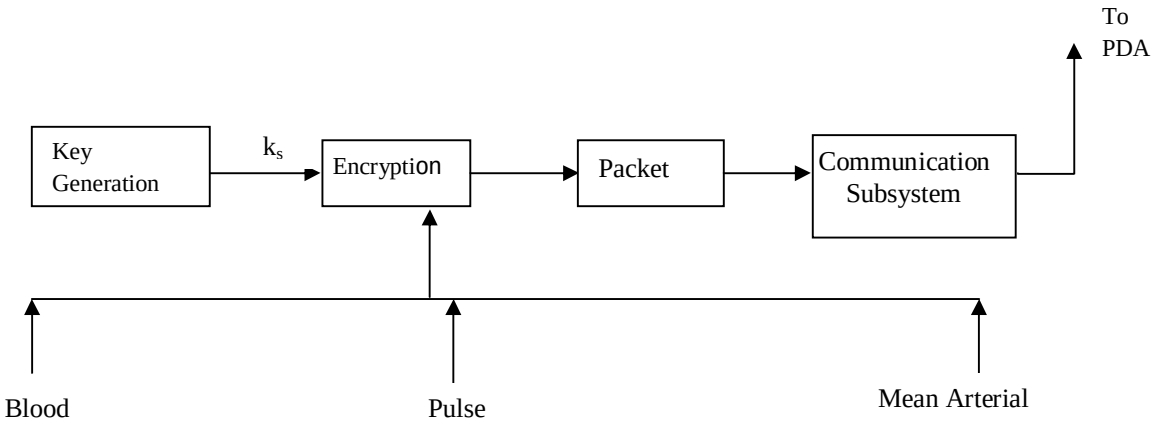

Fig. 2: Encryption/Authentication at SPDS

The SPDS simulates the data for the various patients, consolidates them and encrypts the data using a secret key. The patient ID (PID) is also encrypted with the patients' data. The secret key, the patient ID with the patient data are all combined into a data packet and transmitted to PDAC. On receiving the packet, the PDAC uses its secret key to compare and verify with the received secret key. This ensures the authenticity of the received data packet. PDAC then decrypts the packet. The block diagram of the decryption and authentication at PDAC is given in fig. 3.

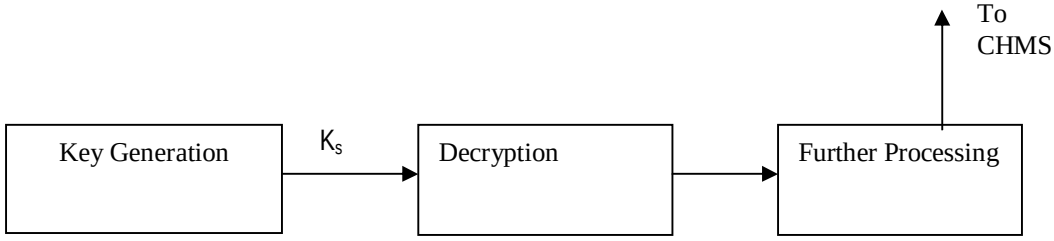

Fig. 3: Decryption/Authentication at PDAC

PDAC also verifies the PID transmitted with the patient's data. It compares the received PID with the list of valid PID. If the PID is not valid, the packet is discarded.

B. *The Encryption/Decryption Algorithm*

1.) Create the instance of javax.crypto.Cipher.
Cipher cipher = Cipher.getInstance("AES/CBC/PKCS5Padding");

2.) Create the instance of sun.misc.BASE64Decoder.
BASE64Decoder d64 = new BASE64Decoder();

3.) Decode encryption key using decodeBuffer method of sun.misc.BASE64Decoder which will return a byte array.
byte[]b = d64.decodeBuffer(ENCRYPTION_KEY);

4.) Now create javax.crypto.spec.SecretKeySpec object using the key byte array and "AES".
SecretKeySpec key = new SecretKeySpec(strPassword.getBytes(), "AES");

5.) Now create javax.crypto.spec.IvyParameterSpec object using your IVspec.
AlgorithmParameterSpec paramSpec = new IvParameterSpec (strPassword.getBytes());

6.) Call the init method of Cipher Instance using encryption mode, key spec (created at step 4), IVParameter Spec(created at step 5).
cipher.init(Cipher.ENCRYPT_MODE, key, paramSpec);

7.) Call doFinal method of Cipher by passing the byte array of data which needs to be encrypted.
encrypted = cipher.doFinal(input.getBytes());

8.) Now encode the encrypted data using sun.misc.BASE64Encoder.
output = new BASE64Encoder().encode(encrypted)

IV. RESULTS AND DISCUSSIONS

The patient id is generated using the random number generation and encrypted at the same time. The blood pressure, pulse rate and the arterial pressure are simulated for the particular patient and all are sent to the database.

My SQL is used for the database while the wamp server is used to activate the database.

In the database, it is only the administrator and the people he gives access to can access the database.

The encrypted patient id together with all the records of the particular patient are decrypted in the database. The symmetric key encryption algorithm is used for the encryption. The symmetric key encryption algorithm employs the Advanced Encryption Standard (AES). AES requires that the encryption password must be 16 bits. When this password is entered, the software generates the patient id and encrypts it at the same time. The patient vital signs, i.e the blood pressure, the pulse rate and the mean arterial pressure are also generated and all are sent to the database.

The decryption is done by using the same 16 bit key used for the encryption.
The output of the java program is shown figures 4 and 5.

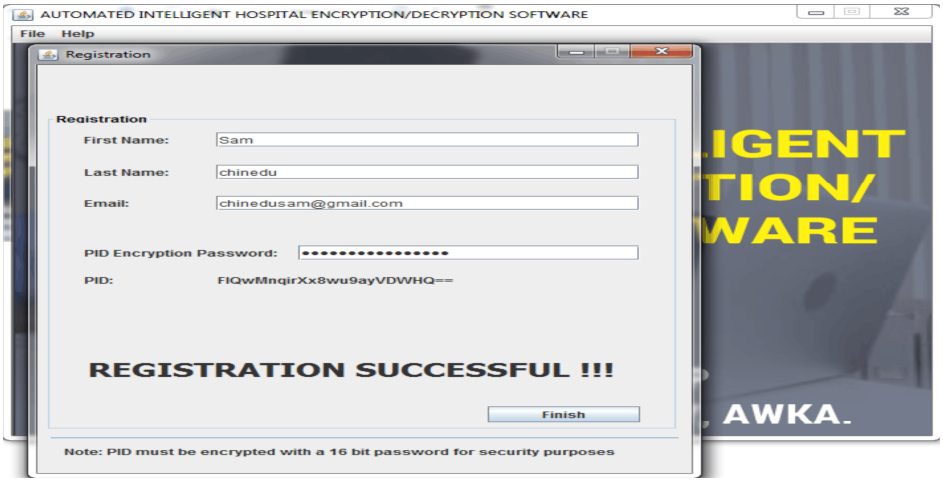

Fig. 4: Registration Page

The registration page allows a new patient to be registered given the patient's first name, last name, e mail and the PID encryption password. The patient is given a 16 bit password which is automatically encrypted and sent to the database.

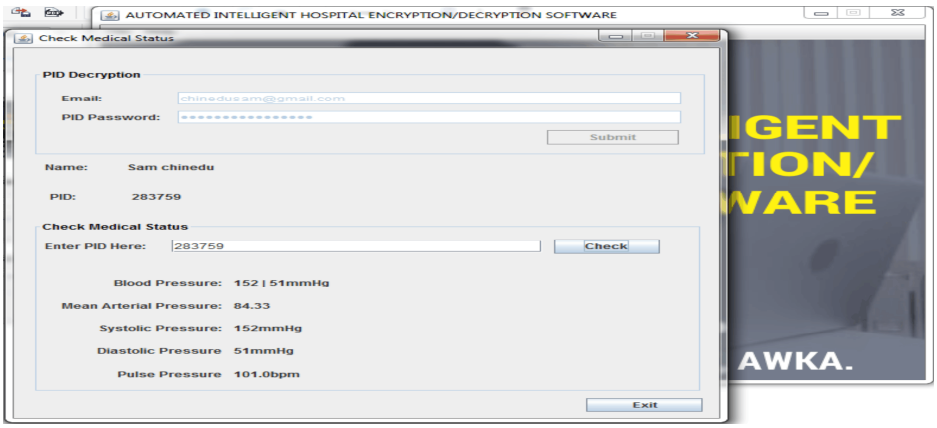

Fig. 5: Medical Status

The medical status page decrypts the PID and automatically generates the Blood Pressu1re, the Mean Arterial Pressure, the Systolic Pressure, the Diastolic Pressure and the Pulse Pressure. These readings are sent to the central database where they are stored for future references

V. CONCLUSION AND FUTURE WORK

We have presented a novel architecture for the continuous unobtrusive monitoring of patients' blood pressure and pulse rate who may be at home while these vital signs are monitored. We have also presented the protection of these patients' vital signs as they travel through the networks to prevent them from unauthorized access. Future work may include incorporating other vital signs like the Pulse Oximetry, Electrocardiogram (ECG), Electroencephalography (EEG), Electrooculography (EOG), Electromyography (EMG) etc and using the asymmetric key encryption algorithm which uses different keys for the encryption and the decryption.

REFRENCES

[1] A. Bhargava, M. Zoltowski, *Sensors and Wireless Communication for Medical Care: Database and Expert Systems Applications*, Proc. 14th International Workshop, 2003.
[2] S. Chekuri, K. K. Venkatasubramanian, S.K.S. Gupta "*BioSec: A biometric based approach for securing communication in wireless networks of biosensors implanted in the human body*", Parallel Processing Workshops, 2003.
[3] P. S. Pandian, K. P. Safeer, P. Gupta, D. T. Sankunthala, B.S. Sundersheshu, V. C. Padaki, "*Wireless sensor network for wearable physiological monitoring*", Journal of Networks, vol 3. 2008.
[4] S. Park and S. Jayaraman, *Enhancing the Quality of Life Through Wearable Technology*, IEEE Engineering in Medicine and Biology Magazine, vol. 22, pp 41–48 2003.
[5] A. Perrig, R. Szewczyk, J. D. *Tygar, V. Wen, and V. Culler, "SPINS: Security Protocols for Sensor Networks"*, Wireless Networks, vol. 8 pp. 521 – 534, 2002.
[6] B.R. Shnayder, K. Hen, T. R.F. Lorinez, Fulford-Jones and M. Welsh, "*Sensor Networks for Medical care"* Technical Report TR-08-05, Harvard University, 2005.
[7] Q. Wang, W. Shin, X. Liu, Z. Zeng, C. Oh, B. Al-Shebli, M. Caccamo, C. Gunter and E. Gunter, "*I-LIVING: An open system architecture for assisted living"*, IEEE SMC 2006.
[8] A. Wood, G. Virome, T. Doan, Q. Cao, Y. Selavo, L. Wu, Z. Fang, Z. He and J. Stankovic, "*ALARM NET: Wireless sensor network for assisted-living and health monitoring"*, Technical Report, University of Virginia 2006.