SECURE PATIENT MONITORING SYSTEM

[1]R.SUJI PRAMILA, [2]A.SHAJIN NARGUNAM

[1]Asstt Prof, Department of Computer Science and Engineering, Noorul Islam Centre for Higher Education
Kumaracoil, Tamilnadu, India

[2] Prof , Department of Computer Science and Engineering , Noorul Islam Centre for Higher Education,
Kumaracoil, Tamilnadu, India

E-mail: [1]sujisymon@gmail.com , [2]ashajins@yahoo.com

ABSTRACT

Patient monitoring in hospital increases the cost, waiting time and the workload of doctors. These issues are eliminated by in-home patient monitoring system. This system is designed with wireless body area networks. Here, a group of body sensors are fitted on the patient's body and these sensors monitor and collect body parameters continuously. In general, the monitoring systems initially collect and forward the patient's data to the personal computer (PC) in patient's home and send them to the hospital via internet. Here the need for a PC is eliminated by GPS enabled smart phone. The smart phone also supports long range outdoor monitoring. Security and privacy are the important issues for in-home patient monitoring system. Different methods are analyzed to accomplish security and efficiency of data sharing. The main objectives of the proposed system are to eliminate the need for a PC and to support the outdoor monitoring by GPS enabled mobile phone. Security and access control are supported by cryptographic operations. This work provides better medical treatments, reduces the health care costs and improves the quality of treatments.

Keywords: *Body area network, body sensors, data sharing, access control, Global Positioning System (GPS), CP-ABE, outdoor monitoring.*

1. INTRODUCTION

The area of healthcare is not only used in medical institution and hospital, but also accessible by persons who are not physically present in hospitals. This is possible by in-home patient monitoring system which provides good results and more efficiency in terms of healthcare. This in-home patient monitoring system has high demand for aging population and the elderly people. As the aging population is more prone to chronic diseases and is in need of an effective in-home health monitoring system, recently, a Wireless Body Area Network (WBAN) with wearable medical sensors was developed [10]. With the help of different sensors, the patient's health related parameters are continuously monitored and transferred to the medical database. The received data are analyzed by the medical professionals to provide better medical treatment.

Currently, some in-home patient monitoring system has been designed with the help of PC, which is located in patient's home. [18]. The patient's data collected from sensors are initially stored in PC and transmitted to the hospital database via internet. The main drawbacks of using PC are the cost, delay that are possible when sending data, if the PC is off and moreover it is difficult to use PC for elderly people. Some of the existing systems use wearable health monitoring device with number of access points (AP) within the patient's home [4] and all the access points are connected to the local database. During the patient movement, the health monitoring device selects any one of the AP and sends movement details to the local database. Here, the main drawback is that when a patient moves away from the home environment, the movement patterns in outdoor environment cannot be tracked.

To eliminate the need for a PC and to support the patient monitoring in outdoor environment GPS enabled mobile phone is used in the proposed system. Security is the major issue when storing Personal Health Records (PHR), because PHR contains sensitive data and they have to be securely stored and accessed [9]. If it is not possible to obtain the authentic and correct data by the medical experts, it leads to wrong and ineffective treatment [10]. A new variant of cipher text Policy Attribute Based Encryption is used in the proposed system. The persons who satisfy the access policy are allowed to access PHRs. employed.

2. LITERATURE REVIEW

2.1 Health Monitoring With Body Sensors

For in-home patient monitoring, Wireless Sensor Network (WSN) is also used. A distributed telemonitoring system was proposed in [8]. It uses Services laYers over Light PHysical devices (SYLPH) model. It uses service oriented architecture model. The main objective is to distribute the resources among multiple WSN. Different networks with varying wireless technologies can also be connected using this model. In [6], Infrared (IR) sensor based system was proposed. It was installed in house and collects the motion values of the patient and different feature values like activity level, mobility level and non response level. Support Vector Data Description (SVDD) method was used to differentiate normal and abnormal behaviors. Behavior pattern classification algorithm was used to classify the behavior patterns here. These schemes were expected to be applicable in home environment but there is no proof.

A Body Sensor Network (BSN) which is designed with a group of body sensors for optimal allocation of resources was discussed in [18]. The major challenges of health monitoring system like sustainable power supply and Quality of Service (QoS) were efficiently solved here. A survey on wearable sensor based system for health monitoring was discussed in [1]. Different systems were evaluated based on evaluation features.

The use of PC was eliminated in [13]. WSN was installed at home. Then it was connected to the hospital sever through internet. Only ECG signals were collected using group of sensors. Initially ECG signals were sampled and transmitted to the access point which is placed in patient's home. Then they were transmitted to the hospital through internet and analyzed to detect heart related diseases. Multiple patients who were monitored with ECG sensors was discussed. ECG sensors are fitted on the chest of the patient to get heart related information like heart rate, heart activity, etc. Here the patients are considered as nodes of the network and hospital is acting as a central node. Two modules were used here: patient home and hospital.

In the home module, continuously monitored heart related data were transmitted to the Wireless Patient Portable Unit (WPPU) which is also embedded on patient's body. Then it was forwarded to the hospital using Wireless Access Point Unit (WAPU) through internet. In hospital, any abnormalities were identified from the received signals, the doctor can contact the patient and gives some advice or sends an ambulance to the corresponding patient's home, in case of any emergency. There is no outdoor environment monitoring and no security in this system.

2.2 Health Monitoring Using Smart Phones

The sensor network in [7] was based on sensors placed on clothes. The patient's vital signs were collected by the sensors and are transmitted to the mobile phone which is carried by the patient. The mobile phone securely receives, stores and forwards the data to the trusted medical professionals. The patient only controls the accessibility of data to other parties. All the processes are done by mobile phone and PC was not used here. Data mining techniques were used to filter the unwanted data sequences and only the necessary data are transferred by the handheld device. Bluetooth or WLAN 802.11 was used to communicate between patient's mobile and expert's device. Emergency calls are generated by patient's device and forwarded to the caregiver's device in case of any emergency conditions.

A novel Wearable Mobility Monitoring System (WMMS) was introduced in [2]. It used smart phone and took photographs when a change of state was detected. On demand positioning and tracking system was proposed in [3]. It was based on Global Positioning enabled devices and suitable for large environments. Smart phone was used between two terminals for making initial communication. In the synchronization phase initial communication is performed. Here requesting terminal T1 sends synchronization Short Message Service (SMS) to the requested terminal T2. If T2 refuses the message, it finishes the process. Otherwise, the location of the terminal is sent in any one of the format like text format (SMS) or multimedia format (MMS). Only the coordinate values of the terminal were present in the text format, but the image which represents the map of the terminal's location was present in the multimedia format. The communication between two terminals is accomplished by simple Peer to Peer (P2P) protocol.

2.3 Health Monitoring With Security

Different security and privacy mechanisms were used in health monitoring. In [7], smart phone was used to receive, store and transmit the patient's vital parameters. Between sensors and central hub AES-

128 encryption was used and between hub and patient's mobile phone Bluetooth encryption was used. In the handheld device, the secure data storage is achieved by AES-128 encryption. Message authentication codes and AES-128 encryption were used for secure data communication from handheld device to medical professional's device. In [17] different cryptographic algorithms and key sizes were proposed. Here the trusted parties are identified by 2048 bit RSA keys and certificates, 256 bit ECC keys or any shared key of at least 112 bits. The certificate authority (CA) was used for issuing certificates. Certificate revocation was done by Certificate Revocation List (CRL). CRLs are automatically generated by CA.

Cipher text Policy Attribute Based Encryption (CP-ABE) with security improvement methods were proposed in [5]. Key escrow problem and user revocation were the two major problems in CP-ABE. In CP-ABE, the private keys of users are generated by Key Generation Center (KGC) by applying set of user attributes with KGC's master secret keys. KGC was not trusted one because it has the ability to decrypt the ciphertext of user if it wants to know the original data. This is known as key escrow problem. In some cases users may change their attributes frequently or some private keys are compromised. To maintain the system secure, it is necessary to update each attribute frequently. This is known as user revocation. These two problems were solved in this paper.

CP-ABE was proposed based on access policy in [9]. Different algorithms were used for generating keys, encrypt and decrypt the data. To ensure confidentiality and dependability multiple secret sharing was used in [14]. To support dynamic integrity, orthonormal vectors were used. Data security and privacy in wireless body area network were discussed in [10]. SKC (Symmetric Key Cryptography) and PKC (Public Key Cryptography) schemes to achieve access control were discussed. Secure data storage scheme with dynamic integrity assurance was proposed in [11].

Distributed data access control scheme to enforce fine-grained access control over sensor data was introduced in [15]. It was resilient against strong attacks such as sensor compromise and user colluding and it exploits a novel cryptographic primitive called attribute-based encryption (ABE). It satisfies both performance and security requirements. Reliable transmission protocol based on anycast routing was used for wireless patient monitoring was proposed in [16]. It automatically selects the closest data receiver to reduce the transmission latency. A study on Data confidentiality in early detection of Alzheimer's disease was discussed in [12]. The new secure and efficient data storage approaches for WBAN were proposed in [14]. Confidentiality, dependability and integrity were achieved here.

3. PROPOSED WORK

In the proposed work, a Body Sensor Network (BSN) is designed with a group of body sensors. The architecture used in the proposed system is shown in Fig 1. It consists of patient data reader, client manager, data server and hospital reporting system. Patient data reader represents the body sensors and they are fitted on patient's body to collect the body parameters like blood pressure, body temperature, pulse rate and ECG signals. They continuously collect the body signals and sent to an aggregator. GPS enabled mobile phone (client manager) is acting as an aggregator.

The patient data reader and client manager are combined into data owner as shown in Fig 2. In some of the existing systems outdoor environment monitoring was not supported. That is when a patient moves away from the home environment, it is difficult to monitor the patient. But in the proposed work, the GPS enabled mobile phone supports outdoor monitoring also. Because the mobile phone is always carried by the patient, it continuously collects the body parameters even when the patient is in out of home environment. The communication between sensors and mobile phone is done by short range Bluetooth communication.

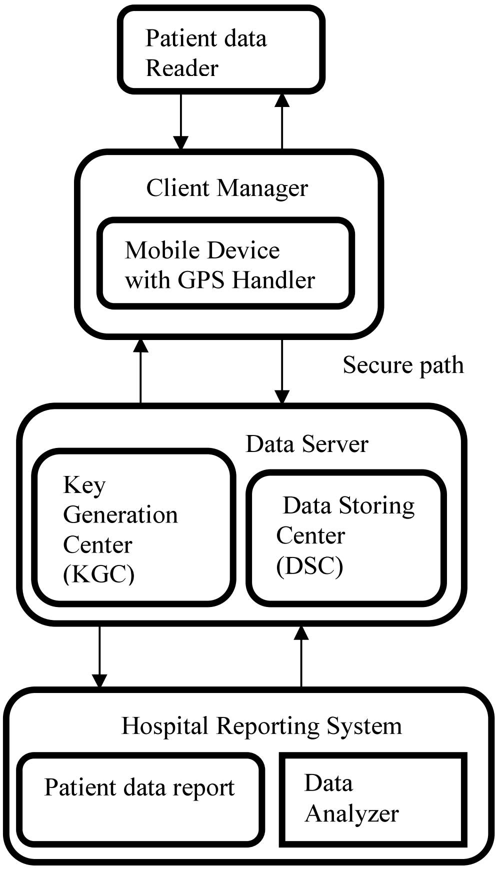
Patient data Reader
Client Manager
Mobile Device with GPS Handler
Secure path
Data Server
Key Generation Center (KGC)
Data Storing Center (DSC)
Hospital Reporting System
Patient data report
Data Analyzer

Fig 1: Architecture Of In-Home Patient Monitoring System

The simplified data sharing system architecture is shown in Fig 2

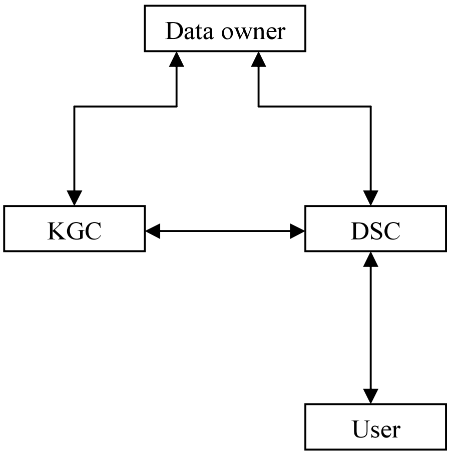

Fig 2: Simplified Data Sharing System Architecture.

In most of the existing systems, the collected body parameters from the sensors are stored in PC. There are some problems when using PC. In the proposed work, the need for a PC is eliminated by GPS enabled mobile phone. The data server consists of client key manager (KGC) and Data Storing Center (DSC). KGC and DSC are responsible for generating keys for secure transfer of medical data. Data owner represents the patient and user refers the medical professionals at the hospital side.

Here security is enhanced in the patient monitoring based on cryptographic operations. Both KGC and DSC generate keys. There are three main cryptographic operations are used here. Owner Key Generation (OKG), Patient data encryption at home environment and patient data decryption at hospital environment. Initially a pair of private and public keys (P1, R1) are generated by KGC and given to data owner. Similarly DSC generates its own private and public keys (P2, R2). From these two different key pairs, data owner can generate new private and public keys (P3, R3). R3 is known by authorized user at hospital side. P3 is used for patient data encryption at home and R3 is used for data decryption at hospital. Based on the decrypted data, response will be sent to the patient.

4. COMPARISION AND ANALYSIS

In the existing system, KGC is responsible for generating keys for different parties and it is not trusted because it knows the private key to get the original data from the cipher text. This is known as key escrow problem. This problem is solved in the proposed system because the private key to encrypt the sensor data is generated by the patient or data owner itself. Here the elimination of PC and the outdoor monitoring is done by GPS enabled mobile phone. Some of the existing systems are compared with the proposed system as shown in table 1. It shows that the proposed system satisfies the important aspects of effective in-home patient monitoring system.

Table 1: Comparison Of Proposed System With Existing Systems

System	Wearability	Security	No PC	Outdoor Monitoring	Ease of use
[10]	Yes	No	No	No	Yes
[12]	Yes	No	Yes	No	Yes
[4]	Yes	Yes	No	No	Yes
[6]	Yes	No	Yes	Yes	Yes
[5]	Yes	No	Yes	No	Yes
[9]	Yes	No	No	No	Yes
Proposed	Yes	Yes	Yes	Yes	Yes

The architecture of the proposed in-home patient monitoring system is implemented in java with the help of standard RSA algorithm. Different key sizes can be given for RSA algorithm to generate keys. This algorithm is tested for key sizes 1024 bits and 2048 bits. Initially the system is tested for the key size of 1024 bits. The execution is repeated for 6 iterations and the time requirement for different operations is listed in Table 2.

Table 2: Time Requirement For Different Operations When The Key Size Is 1024 Bits

Exe. Iter	1	2	3	4	5	6
OKT (ms)	441	508	504	502	505	516
ET (ms)	216	294	301	257	295	312
DT (ms)	16	18	26	19	24	21

The data owner can create his own private and public key pair using (P1,R) and (P2,R2). This time is represented by Owner Key generation Time (OKT). Data owner encrypts its data with its private key P3 and gives to DSC. This encryption time is represented by Encryption Time (ET). Authenticated user can get encrypted data from DSC and decrypts it by R3. This time is represented by Decryption Time (DT). The values in Table 2 are plotted in Fig 5.

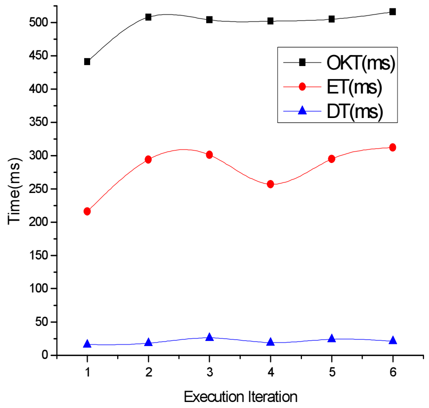

Fig 5: Execution Iteration Vs Time When Key Size=1024 Bits

Table 3 represents the time requirement for different operations when using the key size of 2048 bits.

Table 3: Time Requirement For Different Operations When The Key Size Is 2048 Bits

Exe. Iter	1	2	3	4	5	6
OKT (ms)	716	551	635	681	722	586
ET (ms)	316	298	286	291	318	302
DT	93	92	72	84	89	79

The values in Table 3 are plotted in Fig 6

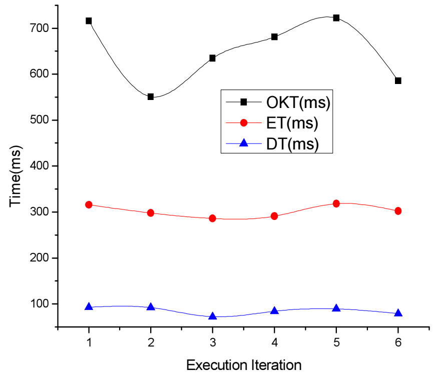

Fig 6: Execution iteration Vs time when key size=2048 bits.

The execution is repeated for two more key sizes (512 bits and 1536 bits). The average values are taken and listed in Table 4.

Time(ms)	Key size (bits)			
	512	1024	1536	2048
Owner key generation time	448	496	535	648.5
Encryption time	262	279	283	301.8
Decryption time	11	20.7	42	84.8

Table 4: Average values for different key sizes

The above values are plotted in a graph and it is shown in Fig 7.

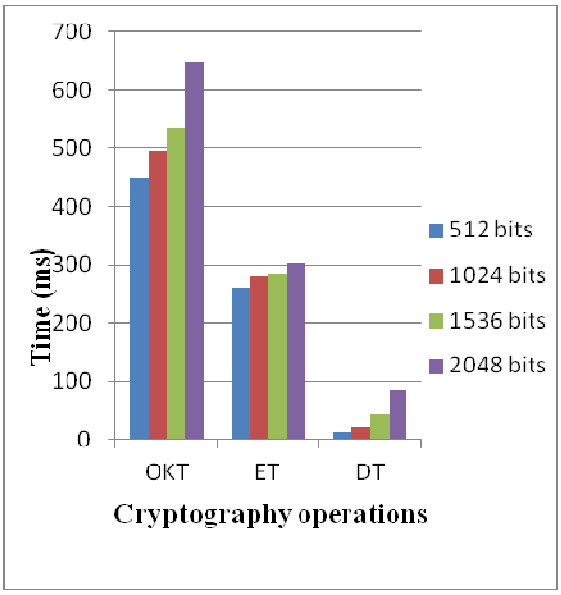

Fig 7: Average Time Requirement For CP-ABE Operations

Fig 7 shows the average time requirement for different operations when using the key sizes of 512 bits, 1024 bits, 1536 bits and 2048 bits. Here the elapsed time of cryptographic operations is different for various iterations. The reason is that a time-shared operating system uses CPU scheduling and multiprogramming concept where the CPU is switched to another job when it waits for any I/O operations. The security is improved when the key size is also increased. This graph shows that there is no large deviation in time even when the key size is increased. Thus the key size of 2048 bits is suitable for the proposed in-home patient monitoring system to provide better security.

5. DISCUSSION

In-home patient monitoring with body sensor network is an effective solution for patient monitoring. It reduces the health care cost and long hospital waiting time. Multiple patients can be monitored at a time. The body sensors continuously collect the body parameters of a patient and they are immediately forwarded to the hospital. So it reduces the chance of false treatment and improves the quality of treatment.

In the proposed system, patients can continue their normal lives and doctors can closely monitor their patients. There is no need of PC and hence there is a reduction in cost. The security is improved by eliminating key escrow problem.

6. CONCLUSION

The sensor based in-home patient monitoring system is used for early detection of diseases and it can be implemented for practice. In the proposed system, GPS enabled mobile phone is acting as an aggregator and also supports outdoor patient monitoring. It eliminates the need for a PC. The security is improved by cryptographic operations and it eliminates key escrow problem.

REFERENCES:

[1] Alexandros Pantelopoulos and Nikolaos G.Bourbakis, “A Survey on Wearable Sensor-Based Systems for Health Monitoring and Prognosis”, *IEEE Transactions on Systems*, Man and Cybernetics, Vol.40, No.1, January 2010, pp.1-12.

[2] Gaetanne Hachette, Edward D. Lemaire and Natalie Baddour, “Wearable Mobility Monitoring Using a Multimedia Smartphone Platform”, *IEEE Transactions on Instrumentation and Measurement*, Vol. 60, No. 9, September 2011, pp.3153-3161.

[3] Godino et al, “P2P Multiuser Low-cost Universal Solution for On-Demand GPS Positioning and Tracking in Large Environments, *IEEE Transactions on Intelligent Transportation Systems*,2011

[4] H. Ting and W. Zhuang, “Bluetooth-Enabled In-home Patient Monitoring System: Early Detection of Alzheimer’s disease”, *IEEE Wireless Comm.*, February 2010, pp. 74-79.

[5] J. hur, "Improving Security and Efficiency in Attribute-Based Data Sharing", *IEEE Transactions on Knowledge and Data Engineering*. IEEE 2011.

[6] Jae Hyuk Shin, Boreom Lee, and Kwang Suk Park, "Detection of Abnormal Living Patterns for Elderly Living Alone Using Support Vector Data Description", *IEEE Transactions on Information Technology in Biomedicine*, Vol. 15, No. 3, May 2011, pp.438-448.

[7] Johannes Barnickel, Hakan Karahan and Ulrike Meyer, "Security and Privacy for Mobile Electronic Health Monitoring and Recording Systems," IEEE 2010.

[8] Juan M. Corchado, Javier Bajo, Dante I. Tapia, and Ajith Abraham, "Using Heterogeneous Wireless Sensor Networks in a Telemonitoring System for Healthcare," IEEE Transactions on Information Technology in Biomedicine, Vol. 14, No. 2, March 2010, pp.234-240.

[9] Luan Ibraimi, Muhammad Asim, Milan Petko vic, "Secure Management of Personal Health Records by Applying Attribute-Based Encryption", *IEEE* 2010.

[10] M. Li and W. Lou," Data Security and Privacy in Wireless Body Area networks", *IEEE Wireless Comm.*, Feb. 2010, pp. 51-58.

[11] Qian Wang and Kui Ren Wenjing Lou Yanchao Zhang, "Dependable and Secure Sensor Data Storage with Dynamic Integrity Assurance", IEEE INFOCOM 2009, pp.954-962.

[12] R. Suji Pramila, A. Shajin Nargunam, "A Study on Data Confidentiality In early Detection of Alzheimer's Disease", *IEEE 2012*, pp. 1004-1008.

[13] Reza S. Dilmaghani, Hossein Bobarshad, M. Ghavami, Sabrieh Choobkar, and Charles Wolfe, "Wireless Sensor Networks for Monitoring Physiological Signals of Multiple Patients", *IEEE Transactions on biomedical circuits and systems*, vol. 5, no. 4, August 2011, pp.347-356.

[14] Rong Fan, Ling-Di Ping, Jian-Qing Fu, Xue-Zeng Pan, "The New Secure and Efficient Data Storage Approaches for Wireless Body Area Networks", *IEEE* 2010.

[15] Shucheng Yu, Kui Ren, and Wenjing Lou," FDAC: Toward Fine-Grained Distributed DataAccess Control in Wireless Sensor Networks**"**, *IEEE Transactions on Parallel and Distributed Systems*, Vol. 22, No. 4, April 2011.

[16] Shyr-Kuen Chen et al. "A Reliable Transmission Protocol for ZigBee- Based Wireless Patient Monitoring", *IEEE Transactions on Information Technology in Biomedicine*, Vol.16, No.1 Jan 2012.

[17] W.T.Polk, D.K.Dodson and W.E.Burr, "Draft: Cryptographic algorithms and key sizes for personal identification verification (PIV)", *In NIST Special Publication* 800-78-2, 2009.

[18] Yifeng He, Wenwu Zhu and Ling Guan, "Optimal Resource Allocation for Pervasive Health Monitoring Systems with Body Sensor Networks", *IEEE Transactions on Mobile Computing*, Vol.10, No.1.