ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

# Mobile Health Monitoring Based On New Power Management Approach

R.Kanimozhi[1], M.Suguna[2]

Department of Information Technology, SNS College of Technology, Coimbatore, Tamilnadu, India[1, 2]

**ABSTRACT-** Mobile Phones is mainly used for communications purpose, (i.e., phoning with friends, relatives, etc.). Mobile Phones is not only used for phoning and also used for other applications like healthcare monitoring with the help of wireless body sensor network. In that the mobile phone's energy could be insufficient when an emergency takes place. With the help of mobile phones, mobile healthcare extends the operations of healthcare provider for better health monitoring. Mobile healthcare emergency services posses an important role but the data transmission and privacy disclosure is still a problem. However, the flourish of Mobile-Healthcare is still faces many challenges including information security, Energy based consideration and privacy preservation. In the proposed, SPOC (Security and Privacy Preserving opportunistic computing) framework aims at the security and privacy issues, and develops a user-centric privacy access control of opportunistic computing in Mobile-Healthcare emergency. Whenever, critical battery achieved in the patient's mobile then he/she can connect with other's mobile. The SPOC software installed in the mobile will detect the other mobiles that have SPOC software. While the data is transferred to the database by using others mobile then the data will be sending in the encrypted format by using AES (Advanced Encryption Standard) technique so, that the information is more security for privacy preserving opportunistic computing system.

**KEYWORDS—** opportunistic computing, User-Centric Privacy access control, Healthcare monitoring, wireless body sensor network

## I. INTRODUCTION

Mobile Emergency-Health or Mobile-Health broadly encompasses the use of mobile telecommunication and multimedia technologies as they are integrated within increasingly mobile and wireless health care delivery systems. The field broadly encompasses the use of mobile telecommunication and multimedia technologies in health care delivery. Mobile-Health is one aspect of Emergency-Health is pushing the limits of how to acquire, transport, store, process, and secure the raw and processed data to deliver meaningful results. However, the flourish of Mobile-Healthcare still faces many challenges including information security and privacy preservation. It proposes a secure and privacy-preserving opportunistic computing framework, called SPOC, for Mobile-Healthcare emergency.

Mobile-Health offers the ability of remote individuals to participate in the healthcare value matrix, which may not have been possible in the past. Participation does not imply just consumption of health care services. Detailed security analysis shows that the proposed SPOC framework can efficiently achieve user-centric privacy access control in Mobile-Healthcare emergency. In addition, performance evaluations via extensive simulations demonstrate the SPOC's effectiveness in term of providing high reliable PHI (personal health information) process and transmission while minimizing the privacy disclosure during mobile-Healthcare emergency. In many, cases remote users are valuable contributors to gather data regarding disease and public health concerns such as outdoor pollution, drugs and violence.

For example, as shown in Fig. 1,each mobile medical user's personal health information (PHI) such as heart beat, blood sugar level, blood pressure and temperature and others, can be collected by BSN, and it can be aggregated by Smartphone via Bluetooth .Personal health information (PHI), also referred to as protected health information, generally refers to demographic information, medical history, test and laboratory results, insurance information and other data that is collected by a healthcare professional to identify an individual and determine appropriate care. In

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

addition, performance evaluations via extensive simulations demonstrate the SPOC's effectiveness in term of providing high reliable PHI process and transmission while minimizing the privacy disclosure during Mobile-Healthcare emergency.

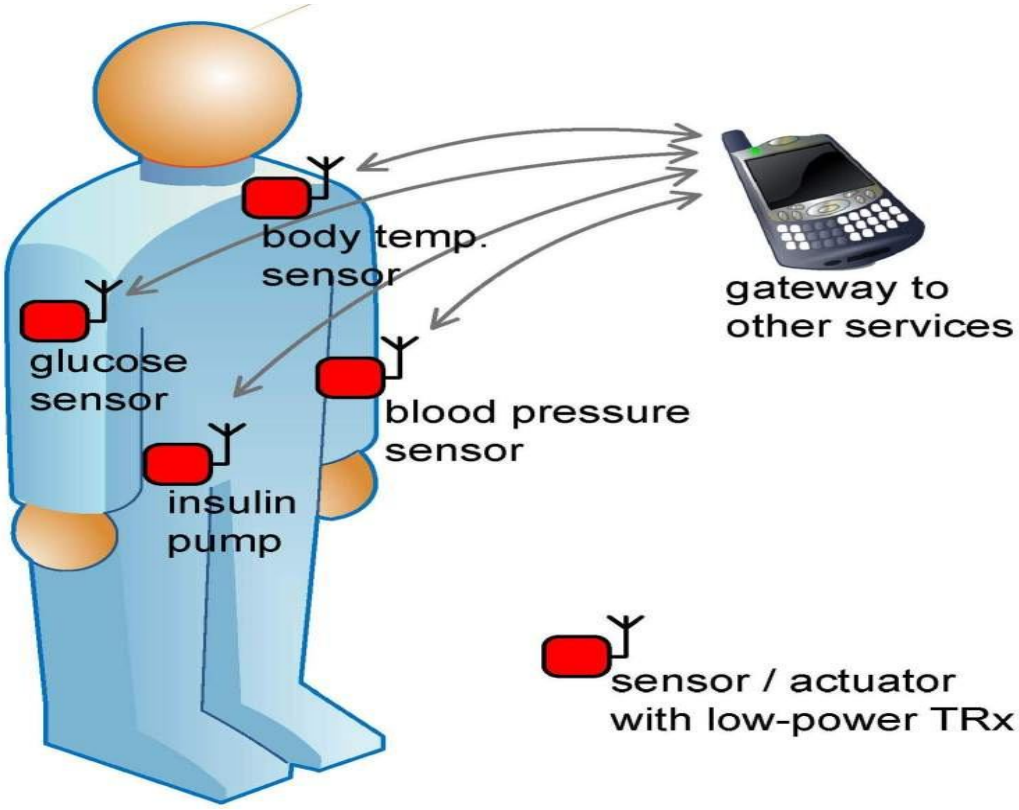


Fig 1.Wireless Body Sensor Networks Monitoring the m-Healthcare system.

## II. SYSTEM ARCHITECTURE

The details of the medical user's personal health information (PHI) such as heart beat, blood sugar level, blood pressure and temperature. Every Medical user's can installed SPOC Software for getting the details of the own PHI process. The Medical User's information's are passed though the database by the third party in encrypting format. so, that the getting output of Medical user's is very privacy and Security.

Input should be consider as N number of users and the users are login to the database that is proposed model and the proposed model is SPOC,PPSPC,AES encrypting file. Using the software and protocol the getting output is very secure and privacy preserving of PHI (personal Health Information) process for every medical users.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

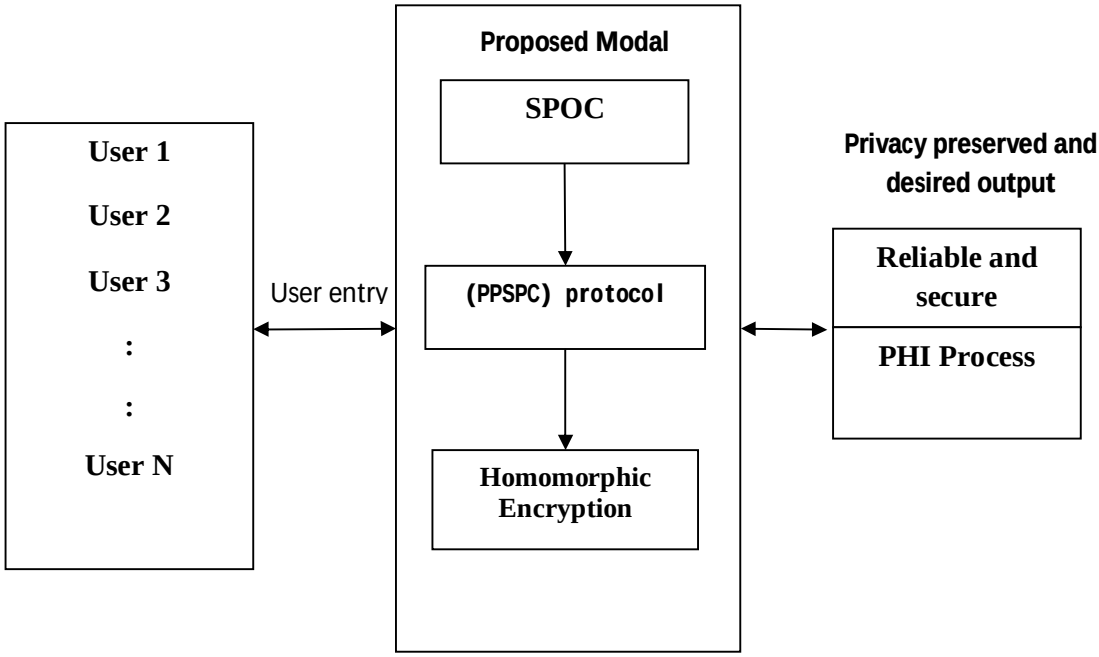


Fig 2.System Architecture.

## III. ADVANCED ENCRYPTION STANDARDS

AES is the basic step for encryption but it is very efficient to mobile healthcare center,the basic steps for encryption is followed:

The Advanced Encryption Standard (AES) computer security standard is a symmetric block cipher that used for encrypts and decrypts 128-bit blocks of data. Standard key lengths of 128, 192, and 256 bits may be used. The algorithm consists of four stages that make up a round which is iterated 10 times for a 128-bit length key, 12 times for a 192-bit key, and 14 times for a 256-bit key. The key size used for an AES cipher and it can specifies the number of repetitions for transformation of rounds that convert the input, called the plaintext, and into the final output, called the cipher text.

The number of cycles of repetition are used in AES as follows:

- 10 cycles of repetition for 128-bit keys.
- 12 cycles of repetition for 192-bit keys.
- 14 cycles of repetition for 256-bit keys.

### 3.1 High level Description for AES algorithm:

1. Key Expansion - Cipher keys are derived from the Round key and, AES requires a separate 128-bit round key block for each round plus.
2. Initial Round

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

1. Add Round Key - Each byte is combined with a block of the round key using bitwise XOR.

3. Rounds
   1. Sub Bytes - A non-linear substitution step where each byte is replaced with another byte.
   2. Shift Rows - where each row of the state is shifted in transportation steps and it can cyclically represent the a certain number of steps.
   3. Mix Columns – It is a mixing operation, which operates the columns of the state, and it can combining the four bytes in each column.
   4. Add Round Key
4. Final Round (no Mix Columns)
   1. Sub Bytes
   2. Shift Rows
   3. Add Round Key.

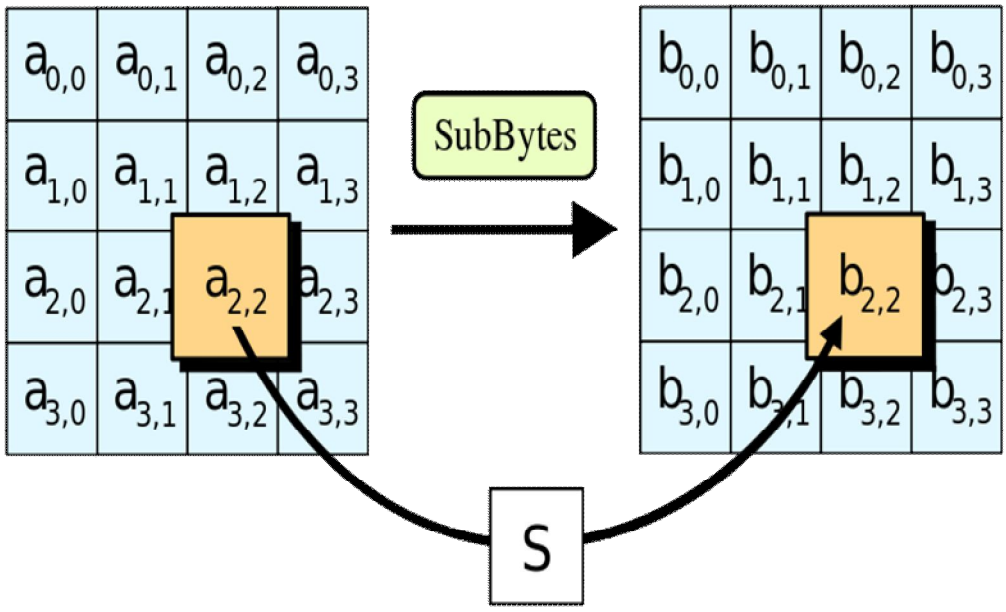


Fig 3.1 AES (Advanced Encryption Standards) Sub bytes.

Fig 3.1 Represent the AES Sub bytes and how it can works in Mobile-Healthcare centre in encrypted format, while the energy of the mobile is in critical position. The database can store the information about the Medical users PHI process.

## IV. RESULTS

The implementation of SPOC Software with using wireless body sensor networks,

- Base Station Activation
- Login Patient details entry
- Region details maintenance
- Mobile movement pattern analysis

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

- Similar Data sharing and route updating
- PHI data transaction
- Encrypting data
- PHI data stored in database
- Cluster

**STEPS FOR IMPLEMENTATION**

First activate the base station then only the node will be generated, that is the patient detail login from is allowed to register the PHI information's. Once the Base Station is activated the all information of user's PHI (Personal Health Information) are stored in database sequent.

The N number of SPOC users can register the new user login form and register the details of Medical User's Personal information details like node name, ip address, port, energy, address, contact number, age and login to the system then node will created successfully. Login the user node name into the base station one by one and the node login is created successfully. The energy level of the patient mobile energy will be store in the database. Once the energy level should be on means the energy level is automatically decreases by the seconds. Then the node activated successfully and analyzing the resources.

Every medical user's roaming regions are analyzed. It will be updated sequentially to get movement details. And also each medical user's nearest helping medical users are also identified and updated in the database sequentially. If the user's condition is in emergency level but at the same time the user's battery is in critical condition means then the information of the user's can send by nearest neighbour. Movement of each medical user are monitored and maintained in the system. This is a centralized unit to maintain the entire medical users movement Patterns. So, that only helps to the emergency patients that are present in the same mobile regions.

The Emergency-Health Portal is containing services, personal Health Services, communication services and decision support tools. Medical user can get the updated information of nearest neighbouring medical user's details; those are having the same PHI software. So that they can help to them at the time of emergency. Also users can get the nearest hospital details those are present very near to the patients. This information is shared by the centralized unit.

User node will be created by the personal health information like user name, blood pressure, sugar rate, temperature, heat beat and its rates are analyzing sensor gateway and successfully send to database and also received the user's information. The user's information is viewed by third party by encrypting rates. So, they don't change the information and send it to the database. The database viewed the helper view by the information send by the other SPOC user they have the more energy level. User energy level, blood sugar, heartbeat, temperature, and pressure are in emergency level means the particular user PHI information's are transmitted through helper view. The helper view having more energy comparing to emergency level and the information's stored in database successfully.

Finally, For Cluster All the Patient Details are viewed by Base Station, by every 5 minutes and also shows medical users energy levels in critical position.

## V. CONCLUSION AND FUTURE WORKS

The SPOC framework aims at the security and privacy issues, and develops a user-centric privacy access control of opportunistic computing in Mobile- Healthcare emergency.

The opportunistic computing normally perform a loop that is

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

- To gather values from the sensing equipment,
- To elaborate such data,
- To send results to the base station.

A secure and privacy-preserving opportunistic computing (SPOC) framework for mobile-Healthcare emergency, which mainly exploits how to use opportunistic computing to achieve high reliability of PHI process and transmission in emergency while minimizing the privacy disclosure during the opportunistic computing. Detailed security analysis is shows that the proposed SPOC frameworks that can be achieve the efficient user-centric privacy access control for better health monitoring. In addition, through extensive performance evaluation. Have to demonstrated the proposed SPOC framework can balance the high-intensive PHI process and transmission and minimizing the PHI privacy disclosure in m-Healthcare emergency.

In our future work, SPOC frameworks become more effective and secure. In addition, we will also exploit the security issues using PPSPC (Privacy Preserving Scalar Product Computation) has followed the internal attackers, and where the internal attacker is not be honestly follows the protocol.

## REFERENCES

1. M. R. Yuce, S. W. P. Ng, N. L. Myo, J. Y. Khan, and W. Liu, "Wireless body sensor network using medical implant band," Journal of Medical Systems, vol. 31, no. 6, pp. 467–474, 2007.
2. M. Avvenuti, P. Corsini, P. Masci, and A. Vecchio, "Opportunistic computing for wireless sensor networks," in IEEE Proc. of MASS'07, pp. 1–6.
3. A. Passarella, M. Conti, E. Borgia, and M. Kumar, "Performance evaluation of service execution in opportunistic computing," in Proc. of ACM MSWIM '10, 2010, pp. 291–298.
4. M. Conti, S. Giordano, M. May, and A. Passarella, "From opportunistic networks to opportunistic computing," IEEE Communications Magazine, vol. 48, pp. 126–139, September 2010.
5. M. Conti and M. Kumar, "Opportunities in opportunistic computing," IEEE Computer, vol. 43, no. 1, pp. 42–50, 2010.
6. W. Du and M. Atallah, "Privacy-preserving cooperative statistical analysis," in Proc. of ACSAC '01, 2001, pp. 102–111.
7. Rongxing Lu, Member, IEEE, Xiaodong Lin, Member, IEEE, and Xuemin (Sherman) Shen, "SPOC: A Secure and Privacy-preserving Opportunistic Computing Framework for Mobile-Healthcare Emergency" IEEE Tran on Parallel and Distributed System, , vol. 24, no. 3, pp. 614-624, March 2013.
8. Y. Ren, R. W. N. Pazzi, and A. Boukerche, "Monitoring patients via a secure and mobile healthcare system," IEEE Wireless Communications, vol. 17, pp. 59–65, 2010.
9. J. Vaidya and C. Clifton, "Privacy preserving association rule mining in vertically partitioned data," in Proc. of ACM KDD'02, pp. 639–644.
10. R. Lu, X. Lin, X. Liang, and X. Shen, "Secure handshake with symptoms-matching: The essential to the success of mhealthcare social network," in Proc. BodyNets'10, Corfu Island, Greece, 2010.