Secure and Privacy Approach in Mobile Healthcare

Ambika. S
UG Student
Department of Information Technology
SNS College of Technology

Hamsa Priyaa. M
UG Student
Department of Information Technology
SNS College of Technology

Lalitha. R
UG Student
Department of Information Technology
SNS College of Technology

Rajakuamri. K
Assistant Professor
Department of Information Technology
SNS College of Technology

Abstract

The m-Healthcare system can benefit medical users by providing high-quality pervasive healthcare monitoring, the growing of m-Healthcare system still strangest on how we fully understand and manage the challenges facing in this m-Healthcare system, especially on during a medical emergency. A secure and privacy-preserving opportunistic computing framework, called SPOC, for m-Healthcare emergency is proposed. With SPOC, smart phone resources including computing power and energy can be opportunistically gathered to process the computing-intensive personal health information (PHI) during m-Healthcare emergency with minimal privacy disclosure. An efficient user-centric privacy access control in SPOC framework is introduced which is based on attribute access control and also a new privacy-preserving scalar product computation (PPSPC) technique is introduced to makes a medical user (patient) to participate in opportunistic computing in transmitting his PHI data.

Keywords: Mobile Healthcare, Opportunitic Computing, User-centric, Privacy-Preserving Scalar Product Computation Protocol (PPSPC)

I. INTRODUCTION

In Mobile Healthcare System Has Been Envisioned As An Important Application Of Pervasive Computing To Improve Healthcare Quality And Save Lives, Where Miniaturized Wearable And Implantable Body Sensor Nodes And Smart Phones Are Utilized To Provide Remote Healthcare Monitoring To People Who Have Chronic Medical Conditions Such As Diabetes And Heart .Specifically, In An M-Healthcare System, Medical Users Are No Longer Needed To Be Monitored Within Home Or Hospital Environments. Instead, After Being Equipped With Smartphone And Wireless Body Sensor Network Formed By Body Sensor Nodes, Medical Users Can Walk Outside And Receive The High-Quality Healthcare Monitoring From Medical Professionals Anytime And Anywhere. For Each Mobile Medical User's Personal Health Information (Phi) Such As Heart Beat, Blood Sugar Level, Blood Pressure And Temperature And Others, Can Be First Collected By Bsn, And Then Aggregated By Smartphone Via Bluetooth. Finally, They Are Further Transmitted To The Remote Healthcare Center Via 3g Networks. Based On These Collected Phi Data, Medical Professionals At Healthcare Center Can Continuously Monitor Medical Users' Health Conditions And As Well Quickly React To Users' Life-Threatening Situations And Save Their Lives By Dispatching Ambulance And Medical Personnel To An Emergency Location In A Timely Fashion.

Although M-Healthcare System Can Benefit Medical Users By Providing High-Quality Pervasive Healthcare Monitoring, The Flourish Of M-Healthcare System Still Hinges Upon How We Fully Understand And Manage The Challenges Facing In M-Healthcare System, Especially During A Medical Emergency. To Clearly Illustrate The Challenges In M-Healthcare Emergency, We Consider The Following Scenario. In General, A Medical User's Phi Should Be Reported to the Healthcare Center Every 5 Minutes for Normal Remote Monitoring. However, When He Has An Emergency Medical Condition, For Example, Heart Attack, His Bsn Becomes Busy Reading A Variety Of Medical Measures, Such As Heart Rate, Blood Pressure, And As A Result, A Large Amount Of Phi Data Will Be Generated In A Very Short Period Of Time, And They Further Should Be Reported Every 10 Seconds For High-Intensive Monitoring Before Ambulance And Medical Personnel's Arrival. However, since Smartphone Is Not Only Used For Healthcare Monitoring, But Also For Other Applications, I.E., Phoning With Friends, The Smartphone's Energy Could Be Insufficient When An Emergency Takes Place. Although This Kind Of Unexpected Event May Happen With Very Low Probability I.E., 0.005, For A Medical Emergency, When We Take Into 10,000 Emergency Cases Into Consideration, The Average Event Number Will Reach 50, Which Is Not Negligible And Explicitly Indicates The Reliability Of M-Healthcare System Is Still Challenging In Emergency. To Propose A New Secure And Privacy Preserving Opportunistic Computing Framework To Address This Challenge. With The Proposed Framework, Each Medical User In Emergency Can Achieve The User-Centric Privacy Access Control To Allow Only Those Qualified Helpers To Participate In

The Opportunistic Computing To Balance The High-Reliability Of Phi Process And Minimizing Phi Privacy Disclosure In M-Healthcare Emergency. Specifically, The Main Contributions Of This Paper Are Threefold.

To Propose A Secure And Privacy Preserving Opportunistic Computing Framework For M-Healthcare Emergency. With This Project, The Resources Available On Other Opportunistically Contacted Medical Users' Smart Phones Can Be Gathered Together To Deal With The Computing-Intensive Phi Process In Emergency Situation. Since The Phi Will Be Disclosed During The Process In Opportunistic Computing, To Minimize The Phi Privacy Disclosure, It Introduces A User-Centric Two-Phase Privacy Access Control To Only Allow Those Medical Users Who Have Similar Symptoms To Participate In Opportunistic Computing. To Achieve User-Centric Privacy Access Control In Opportunistic Computing, We Present An Efficient Attributebased Access Control And A Novel Non Homomorphic Encryption-Based Privacy Preserving Scalar Product Computation(Ppspc) Protocol, Where The Attributed-Based Access Control Can Help A Medical User In Emergency To Identify Other Medical Users, And Ppspc Protocol Can Further Control Only Those Medical Users Who Have Similar Symptoms To Participate In The Opportunistic Computing While Without Directly Revealing Users' Symptoms. Note That, Although Ppspc Protocols Have Been Well Studied In Privacy-Preserving Data Mining Yet Most Of Them Are Relying On Time-Consuming Homomorphic Encryption Technique. To The Best Of Our Knowledge, Our Novel Non Homomorphic Encryption-Based Ppspc Protocol Is The Most Efficient One In Terms Of Computational And Communication Overheads.

II. EXISTING SYSTEM

The existing systems use the opportunistic computing paradigm in wireless sensor network to solve the problem of storing and executing application that exceeds the memory resources available on a single sensor node. Especially, the solution is based on the idea of partitioning the application code into a number of opportunistically cooperating modules, and each node contributes to the execution of the original application by running a subset of the application tasks and providing service to the neighboring nodes.

In existing system FLA (First Level Analyzer) is used to analyze the data from the sensor gateway. Checks whether the value is in specific range or not. If it is in specific range, it will analyze the data or else it generates an alarm stating that the value will be out of range, so avoid the false alarm triggering and also it checks whether the value will be in critical range or not. If it is in critical range it generates a critical alarm in the hand held devices as well as in the system. Then the data will be processed and stored in the log file

A. Drawbacks:

- Need an end-to-end sensor network platform to support automated patient monitoring
- Have to be collaborated closely with the diverse groups of stakeholders within the disaster response
- Designed for improving patient monitoring. It is not designed to optimize extensibility, scalability, and cost
- Must be integrated with new sensor modalities to address a wide variety of problems within disaster response

III. PROPOSED SYSTEM

In our system, a medical personnel at the health care centre who is considered trustworthy is responsible for initializing and controlling the entire health care system. A user who wishes to get the benefits of the mobile healthcare system registers himself as a medical user under a particular health care centre, then a medical professional examines the user and generates his health profile. Based on the health profile, the users are then provided with the particular type of sensors such as heart rate, blood sugar level and other materials. Once being equipped with the sensors the users can move anywhere unlike in hospital [8], [9], [10] .The sensors begin to collect the sensed data and transmit them to the user's smart phone which is then transmitted to the health care center. The sensors and the smart phone plays a vital role in mobile monitoring of patients. The sensors are used only for sensing hence they can be charged up every day and used whereas the smart phones are used for various purposes, the power of the smart phone may not be sufficient under emergency circumstances. Hence we make use of opportunistic computing where whenever a medical user is in emergency other medical users in the nearby area can contribute their resources

A. Centric Privacy Access Control for M-Healthcare:

When a critical situation happens to medical user in m-Healthcare, e.g., user U0 accidentally fell with in no time as not usual, the healthcare representatives will handle and controls that patient‟s situation, and thereafter in emergency an ambulance and a medical representative will be sending to the respective place. Usually the vehicle will be dispatched nearly 15 to 20 minutes. Meanwhile the medical representative requires high-intensive PHI to real-time monitor U0. Howsoever, the energy of U0‟s Smartphone device may not be flexible to engage in the high-intensive PHI process and transmission. At this time, the opportunistic computing, as shown in Fig. is launched, and the below user-centric privacy access control is processed to reduce the PHI privacy exposure in opportunistic computing.

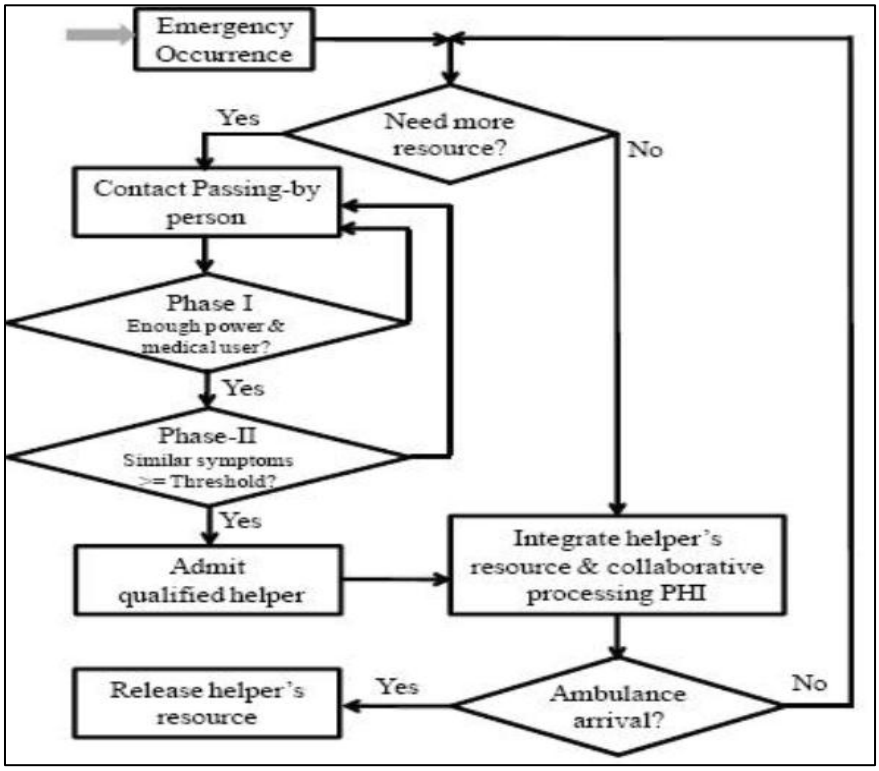

Fig. 1: Opportunistic computing with two-phase privacy access control for m-Healthcare emergency

1) *Access Control 1:*

The aim of phase-I access control is to locate if any other medical patient is in emergency. To attain the phase-I access control, U0"s Smartphone device first selects a number which is random, when patient Uj goes by the emergency place, U0 sends CData. After receiving CData, Uj will process the below steps:

- Uses pass by person"s access control key akj to compute Data;
- Compute Auth, where timestamp is the current timestamp, and returns Authktimestamp to U0. When user U0 receives Authktimestamp at time timestamp0, he first checks the validity of the time interval between timestamp0 and timestamp in order to resist the replaying attack. Once Authktimestamp is permitted, U0 accepts the Auth0. If it does hold, Uj is authenticated as a medical patient, and allows the phase-I access control.

2) *Access Control 2:*

Once Uj Passes The Phase-I Access Control, U0 And Uj Will Continue To Process The Phase-II Access Control To See Whether They Both Had Nearby Signs To Expose PHI. Let The Personal Health Information Of Medical Patient"S U0, Uj. U0 First Defines An Expected Threshold Th For The Number Of Common Signs. Then, In Order To Compute A Privacy-Preserving Route, U0 And Uj. Since The PPSPC Protocol Ensures Neither U0 Nor Uj Will Expose Their Personal Healthcare Information To One Another During The Computation It Can Efficiently Attain Privacy Preserving Access Control.

B. Analysis of Opportunistic Computing in M-Healthcare:

Consider The Ambulance Will Arrive At The Emergency Location In The Time Period T. To Gauge The Benefits Brought By Opportunistic Computing In M-Healthcare Emergency, We Analyze How Many Qualified Helpers Can Participate In Opportunistic Computing Within The Time Period T, And How Many Resources Can The Opportunities Computing Provide.For A Given Threshold Th, Respectively, Denoted As The Number Of Qualified Helpers (Nqhs) And The Number Of Nonqualified Helpers. For Any Arriving User At Time, The Probability That The User Is A Qualified Helper.

- Theorem 1: The Expected Number Of The Qualified Helpers Participating In Opportunistic Computing Within Time.
- Theorem 2:The Expected Resources That Can Be Provided By Opportunistic Computing

C. Advantages:

- SPOC framework allows a medical user to decide who can participate in the opportunistic computing to assist in processing his overwhelming PHI data.
- The user-centric privacy access control to allow only those qualified helpers to participate in the opportunistic computing to balance the high-reliability of PHI.
- The attributed-based access control can help a medical user in emergency to identify other medical users.

IV. IMPLEMENTATION

A. Therapeutic User:

In this module an application for Android smart phone is developed, to register the therapeutic user, then send and view their heal reports

B. Therapeutic Registration:

The user is prompt to register with trusted authority to send the report and view diagnosis, on the time of registration user need to give their personal information such as name, age, address, contact number, email id. And username, password to login and send the reports, User need to give the emergency contact number to call immediately in emergency situations.

C. Crisis Call:

The user can call the emergency number by pressing a simple button, no need to open their dialler and entering the number or search the contacts and call the number, the user is prompt to give the emergency number to call at the time of registration, that number is called when the user in emergency situation by pressing a simple button.

D. Launch Report:

User periodically sends their health information (PHI) such as Pulse rate, Blood sugar, Blood pressure and Body temperature to the Trusted Authority. The values are compared with threshold values and status is given as Normal or Emergency.

E. Analysis Report:

User can view the report sent to the Trusted Authority and the diagnosis received from the trusted authority, then they can do the need full based on the diagnosis.

F. Settings:

User has the options to update their personal information, username, password and emergency number when they needed.

G. Trusted Authority:

This module is developed as PHP project, Trusted Authority can login in the web application running in the server and review all medical user PHI reports, time of the report and status, and have the options to filter by the medical user name to view the particular medical user report, then sent the diagnosis to the medical user based on their PHI status to their Smartphone application. The user can receive the diagnosis as the email in the address given at the time of registration, and can receive the report in SMS in the number given.

V. RESULTS AND DISCUSSIONS

A lot of experiments are made in the present system where a comparative analysis is taken between the present method to that of the several existing methods and it is also displayed or shown in the below block diagram. Here many experiments are conducted on several number of the data sets and plays a vital and a challenging role in order to satisfy the performance of the system in terms of the analysis oriented phenomena followed by the gain of the satisfaction related to the user respectively.

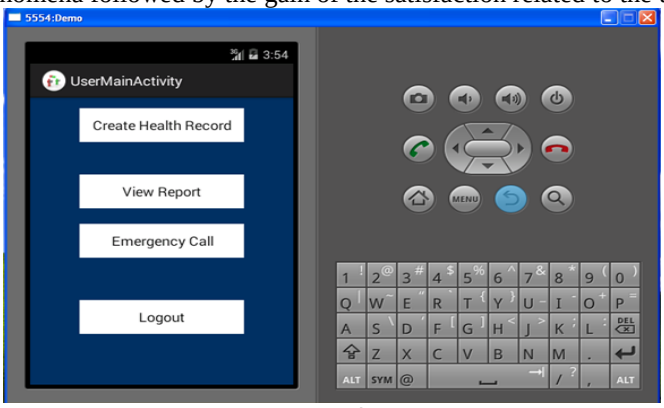

Fig. 2: User Activity

The user have to register in the application. After registering in the application the user can login using user ID and password given. The user can send their PHI report, view their report, and can make emergency call.

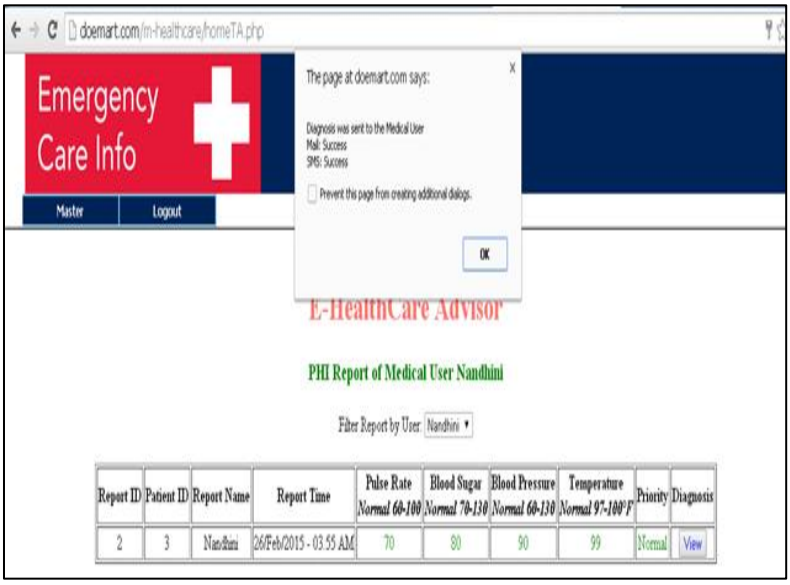

Fig. 3: Trusted Authority

The Trusted Authority view the patient's PHI report.After analysing the PHI values with threshold values, the Trusted Authority send diagnosis to the respective user via mail and SMS

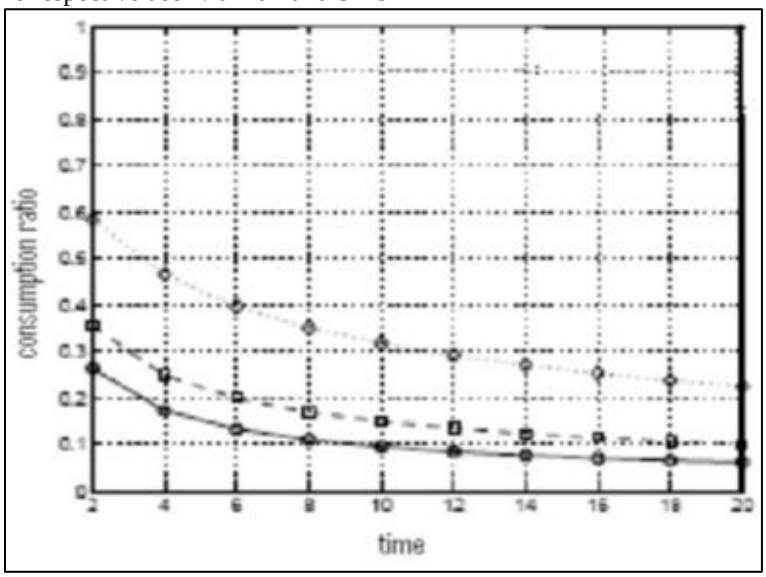

Fig. 4: Shows the graphical representation of consumption ratio

VI. CONCLUSION AND FUTURE WORK

The proposed a secure and privacy preserving opportunistic computing framework for m-Healthcare , 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 shows that the proposed SPOC framework can achieve the efficient user-centric privacy access control.

In addition, through extensive performance evaluation, we have also 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, we intend to carry on smartphone-based experiments to further verify the effectiveness of the proposed SPOC framework. In addition, we will also exploit the security issues of PPSPC with internal attackers, where the internal attackers will not honestly follow the protocol. To intend carry on Smartphone-based experiments to further verify the effectiveness of the proposed framework. In addition, we will also exploit the security issues of PPSPC with internal attackers, where the internal attackers will not honestly follow the protocol.

VII. REFERENCES

[1] M. Avvenuti, P. Corsini, P. Masci, and A. Vecchio, "Opportunistic Computing for Wireless Sensor Networks," Proc. IEEE Int'l Conf.Mobile Adhoc and Sensor Systems (MASS '07), pp. 1-6, 2007.
[2] A.Passarella, M. Conti, E. Borgia, and M. Kumar, "PerformanceEvaluation of Service Execution in Opportunistic Computing,"Proc. 13th ACM Int'l Conf. Modeling, Analysis, and Simulation ofWireless and Mobile Systems (MSWIM '10), pp. 291-298, 2010.
[3] M.Conti, S. Giordano, M. May, and A. Passarella, "FromOpportunistic Networks to Opportunistic Computing," IEEEComm. Magazine, vol. 48, no. 9, pp. 126-139, Sept. 2010.
[4] M. Conti and M. Kumar, "Opportunities in OpportunisticComputing," IEEE Computer, vol. 43, no. 1, pp. 42-50, Jan. 2010.
[5] W.Du and M. Atallah, "Privacy-Preserving Cooperative Statistical Analysis," Proc. 17th Ann. Computer Security Applications Conf.(ACSAC '01), pp. 102-111, 2001.
[6] J.Vaidya and C. Clifton, "Privacy Preserving Association RuleMining in Vertically Partitioned Data," Proc. Eighth ACM SIGKDDInt'l Conf. Knowledge Discovery and Data Mining (KDD '02), pp. 639-644, 2002.
[7] A. Amirbekyan and V. Estivill-Castro, "A New EfficientPrivacy-Preserving Scalar Product Protocol," Proc. Sixth AustralasianConf. Data Mining and Analytics (AusDM '07), pp. 209-214, 2007.
[8] R. Lu, X. Liang, X. Li, X. Lin, and X. Shen, "Eppa: An Efficient and Privacy-Preserving Aggregation Scheme for Secure Smart Grid Comm.," IEEE Trans. Parallel Distributed and Systems, to be published.
[9] X. Lin, R. Lu, X. Shen, Y. Nemoto, and N. Kato, "Sage: A Strong Privacy-Preserving Scheme against Global Eavesdropping for Ehealth Systems," IEEE J. Selected Areas in Comm., vol. 27, no. 4, pp. 365-378, May 2009.
[10] M. Li, W. Lou, and K. Ren, "Data Security and Privacy in Wireless Body Area Networks," IEEE Wireless Comm., vol. 17, no. 1, pp. 51-58, Feb. 2010.
[11] P.Paillier, "Public-Key Cryptosystems Based on CompositeDegree Residuosity Classes," Proc. 17th Int'l Conf. Theory andApplication of Cryptographic Techniques (EUROCRYPT '99), pp. 223-238, 1999.
[12] R. Lu, X. Liang, X. Li, X. Lin, and X. Shen, "Eppa: An Efficient and Privacy-Preserving Aggregation Scheme for Secure Smart Grid Comm.," IEEE Trans. Parallel Distributed and Systems, to be published.
[13] Darrell M. West, "Improving Health Care through Mobile Medical Devices and Sensors," Center for Technology Innovation at Brookings, October 2013. Brussels, "Green Paper on mobile Health ("mHealth")," European Commission, April 2014.
[14] KoushalModi and RadhaBaranMohanty, "White Paper on M-Health: Challenges, Benefits and keys to successful Implementation," Infosys-Building Tomorrow's Enterprise.
[15] Xuan Hung Le, Sungyoung Lee1, Phan Tran HoTruc, La The Vinh, AsadMasoodKhattak, Manhyung Han, DangViet Hung, Mohammad M. Hassan, Miso (Hyung-Il) Kim, Kyo-Ho Koo, Young-Koo Lee, Eui-Nam Huh, "Secured WSN-integrated Cloud Computing for u-Life Care," IEEE Communications Society, IEEE CCNC 2010 proceedings.
[16] Jun Zhou, ZhenfuCao, and XiaoleiDong, Xiaodonglin, V. Vasilakos, "Securing M-Healthcare Social Networks: Challenges, Countermeasures and Future Directions," IEEE Wireless Communications, August 2013.
[17] FenMiao1, Xiuli Miao2, Weihua Shangguan1, Ye Li1, "MobiHealthcare System: Body Sensor Network Based M-Health System for Healthcare Application," Scientific Research, January 2012.
[18] Jun Zhou, Xiaodong Lin,Xiaolei Dong, Zhenfu Cao, "PSMPA: Patient Self-controllable and Multi-level Privacy-preserving Cooperative Authentication in Distributed m-Healthcare Cloud Computing System," IEEE Transactions on Parallel and Distributed Systems, October 2014.
[19] Aleksandar Milenković, Chris Otto, Emil Jovanov, "Wireless Sensor Networks for Personal Health Monitoring:Issues and an Implementation", Electrical and Computer Engineering Department, The University of Alabama in Huntsville, 301 Sparkman Drive, Huntsville, AL 35899.
[20] Aashima Arya, Naveen Bilandi, "Wireless Body Area Networks for Health Care", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 2, Issue 4, April 2014.