An Efficient Mobile Health Care Emergency Services

A.Shanmugapriya[1] S. Rajeswari (SE.G) [2]

[1]M.Tech (Information and communication Technology)
J.J. College of Engineering and Technology, Trichy- 09

[2]Department of Information and Technology
J.J College of Engineering and Technology, Trichy- 09

***Abstract*— Technological advances are leading to a world replete with mobile and static sensors. Hence mobile Healthcare (m-Healthcare) extends the operation of Healthcare provider into a developing environment for better healthcare monitoring systems. Even now there were many challenges in m-healthcare services that include information security and privacy preservation. Hence a secure and privacy-preserving opportunistic computing framework for m-Healthcare emergency has been introduced. Using opportunistic computing smart phone resources including computing power and energy can be distributed to process the computing-intensive personal health information (PHI).The proposed project introducing a reconstruction algorithm for scanning process in m-healthcare monitoring. Algorithms are used to improve the reliability of PHI process. It also introduced an efficient user-centric privacy access control, and it also allows a user to decide who can assist them in processing his PHI data. The proposed computing framework can efficiently achieve user-centric privacy access control in m-Healthcare emergency.**

***Keywords*— Personal healthcare information, m-Healthcare, Opportunistic computing, attribute based encryption, body scanning process.**

I. INTRODUCTION

Improvement in the medical science was not feasible for the medical users in emergency situation. Wireless sensor networks (WSNs) are massively distributed networks that do not require any external infrastructure and are typically used to monitor a physical phenomenon [3],. Sensor network applications can play a key role in many different areas, such as intrusion detection and surveillance, wildlife monitoring, precision agriculture and building monitoring. The physical proximity of sensors to the observed phenomenon and the programmability of nodes can increase the level of accuracy and adaptability of the sensing process with respect to traditional solutions. 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 smart phone via Bluetooth. Finally, it can further transmitted to the remote healthcare canter via 3G networks.

Based on these collected PHI data, medical professionals at healthcare canter 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. 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.

It is exciting to have convenient PHR data services for everyone, there are many security and Privacy risks which could impede its wide adoption. The main concern is about whether the patients could actually control the sharing of their sensitive personal health information (PHI), especially when this can be stored on a third-party server which people may not fully trust. On the one hand, although there health care regulations such as HIPAA which is recently amended to incorporate business associates, cloud providers are usually not covered entities. On the other hand, due to the high value of the sensitive Personal Health Information (PHI), the third-party storage servers are often the targets of various malicious behaviours which may lead to exposure of the PHI [4] ,[5].

II. RELATED WORK

In the proposed system the main feature is PHI. Physical Health Information (PHI) that is transmitted over the cellular network is highly sensitive to the individual person. Security of the PHI was one of the biggest challenging in the context of mobile healthcare. Another major issue in mobile healthcare is power supply to the cell phone. These need other nodes to transmit the PHI to the healthcare centre.

Opportunistic computing paradigm can be applied in m-Healthcare emergency to resolve the challenging reliability issue in PHI process. However, PHI is personal information and very sensitive to medical users, once the raw PHI data are processed in opportunistic computing, the privacy of PHI would be disclosed. Therefore, how to balance the high reliability of PHI process while minimizing the PHI privacy disclosure during the opportunistic computing becomes a challenging issue in m-Healthcare emergency [3],[7].

Privacy-Preserving Scalar Product Protocol (PPSPP) is privacy issues have become important in data analysis, especially when data is horizontally partitioned over several parties. In data mining, the data is typically represented as attribute-vectors and, for many applications; the scalar (dot) product is one of the fundamental operations that is repeatedly used. In privacy-preserving data mining, data is distributed across several parties[1],[2],[6],[10]. The efficiency of secure scalar products is important, not only because the can cause overhead in communication cost, but dot product operations also serve as one of the basic building blocks for many other secure protocols [14].

The Security of PHI in m-healthcare is based on the body sensors and wireless cellular node provide a significant advantage in mobile healthcare, there are some issues related to the security and privacy of medical user's physical health information in mobile healthcare solution [11],[13],[15]. As the mobile healthcare system consists of wireless sensor and mobile node, the security of patient's private data at the time of transmission from one wireless cellular node to another wireless cellular node is the main concern. Security must provide a confidence to the user that the highly sensitive physical health information will not be disclose to the unauthorized third party, only authorized person should have access to the patient's physical health information [4].

Another main feature is WBN (Wireless Body Area Network). it has emerged as a key technology to provide real-time health monitoring of a patient and diagnose many life threatening diseases. Among the various research issues required to be addressed to implement this technology effectively, security issue is one of the key issues. It surveys the issues related to security and possible solutions taken to address them in the research and the forthcoming IEEE standard. The survey brings out that the current proposed solutions in security are still having limitations needing further research [15].

III. PROPOSED ARCHITECTURE

In the developing proposed system the healthcare services in the opportunistic computing framework provide the healthcare user's with more provable opportunities. It also provides high level reliability in the healthcare system.

Opportunistic computing can be described as distributed computing with the caveats of intermittent connectivity and delay tolerance. The mobile and pervasive computing paradigms are also considered in the opportunistic computing for the natural evolutions of traditional distributed computing. In opportunistic computing, opportunistic connectivity leads to accessing essential resources and information. Opportunistic computing can benefit from the ongoing and past research outcomes in pervasive and sensor systems [8]. The main factor in Opportunistic computing was that humans' mobility and their stability nature is to enable a transformation only if two users are sufficiently close. The key challenges that affect the characteristics of opportunistic computing in the medical healthcare services is Connectivity, Delay tolerance and Heterogeneity [5],[7].

Mobile healthcare services in the proposed system have defined certain areas of applications [12]. They are education and awareness about disease prevention and precautions, care of support in point to point diagnostics, screening and clinical care , monitoring of patients for treatment adherence support, disease and epidemic outbreak and surveillance(i.e. real time tracking in case of infectious disease and emergency medical response and efficient system.

A.PROPOSED MODEL

In the proposed model group of opportunistic users are taken into account. There are more no of groups based on their location. Let consider that users as U1,U2,U3....Un and also no of groups as G1,G2,G3.....Gn. These users groups first have to register their details and get a medical user id. After that the Healthcare centre will regularly monitor the user. Location of the patients is finded out by using the patient's user id and their location mapping [12],[13].

The proposed architecture shown in Fig 1 defines the function of the healthcare service during emergency. The group of medical users can transfer the message using 3G services. The main functions provided by the healthcare service during emergency is to regularly monitoring patient details collecting and processing PHI, to check for the resource that are needed during emergency situation, calling medical professionals, checking patients past records. By performing these actions the emergency situations are handled more efficiently and save lives.

B.METHODS USED

Methodologies used in the proposed system include Healthcare monitoring, Body scanning process; secure data analysis, Sending SMS, Performance evaluation and Emergency search. These methods are used in the opportunistic computing framework to get reliable processing. Among these six methods performance evaluation will define the reliability of the secure PHI data transferring. The methods used are defined below.

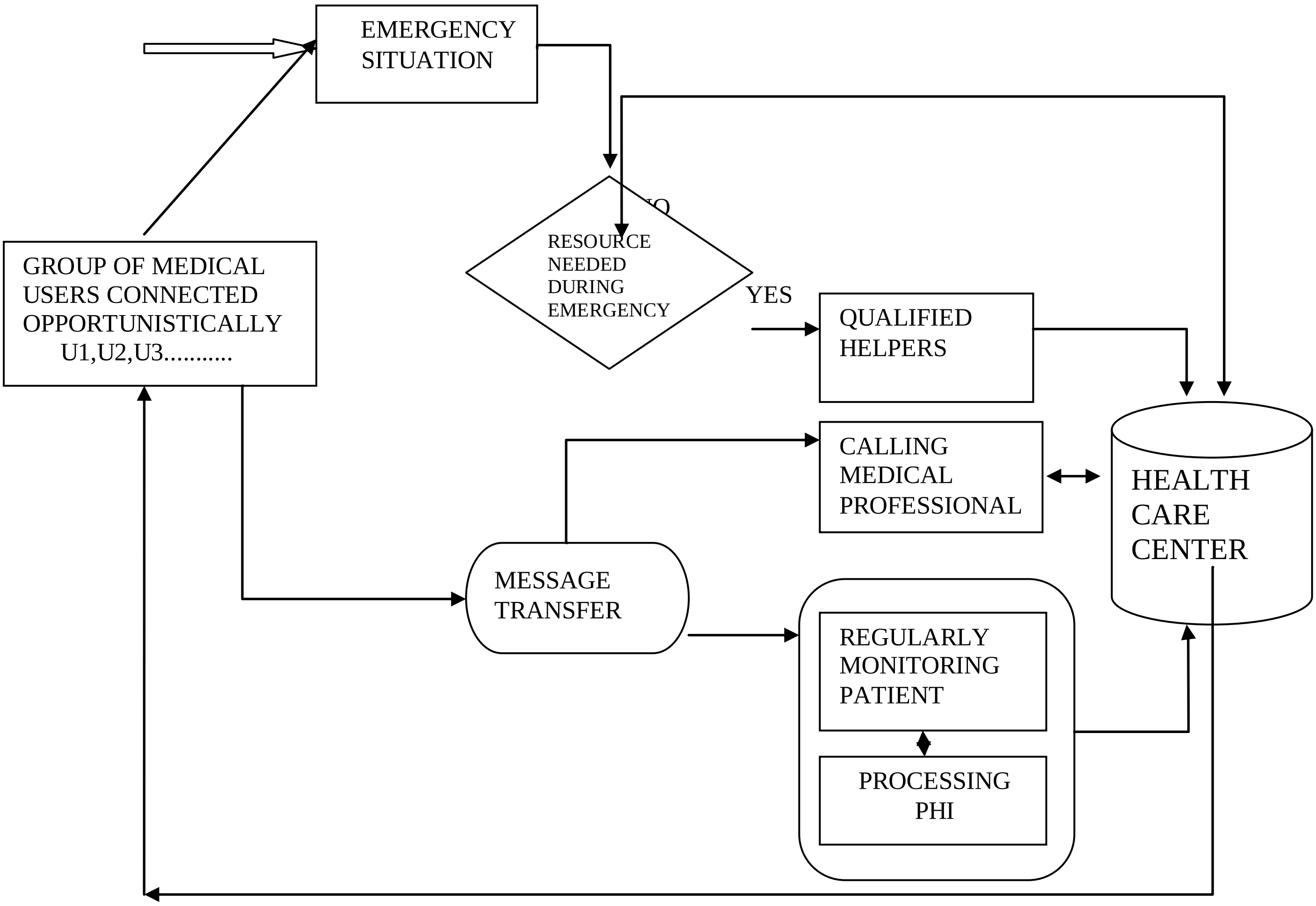
EMERGENCY SITUATION
NO
RESOURCE NEEDED DURING EMERGENCY
YES
GROUP OF MEDICAL USERS CONNECTED OPPORTUNISTICALLY U1,U2,U3...........
QUALIFIED HELPERS
CALLING MEDICAL PROFESSIONAL
HEALTH CARE CENTER
MESSAGE TRANSFER
REGULARLY MONITORING PATIENT
PROCESSING PHI

Fig1 Proposed Architecture

1) HEALTHCARE MONITORING

In this module, 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 and then the collected information's are send by smart phone through Bluetooth [4],[11],[12],[13]. Finally, it is further transmitted to the remote healthcare centre via 3G networks. Based on these collected PHI data, medical professionals at healthcare centre can continuously monitor medical users' health conditions and quickly react to users' life-threatening situations and save their lives by providing ambulance and medical personnel to an emergency location in a timely fashion. In this module the medical user first has to register their medical details and get their id for future references. This was the main characteristic function that gets information from the mobile phone for getting and processing information.

2) BODY SCANNING PROCESS

In this module, Body area networks (BAN), wireless body area network (WBAN) or body sensor network (BSN) are terms used to describe the application of wearable computing devices. This will enable wireless communication between several miniaturized body sensor units (BSU) and a single body central unit (BCU) worn at the human body. – Deploy wearable sensors on the bodies of patients in a residential setting – Continuously monitor physiological signals (such as ECG, blood oxygen levels) and other health related information (such as physical activity).

3) SECURITY DATA ANALYSIS

This Module is to develop a secure and privacy-preserving opportunistic computing framework to provide high reliability of PHI process and transmission while minimizing PHI privacy disclosure in m-Healthcare emergency [14],[16]. Specifically,

1. Apply opportunistic computing in m-Healthcare emergency to achieve high-reliability of PHI process
2. Develop user-centric privacy access control to minimize the PHI privacy disclosure.

4) *PERFORMANCE EVOLUTION*

In this module, the performance metrics used in the evaluation are:

1. The average number of qualified helpers (NQH), which indicates how many qualified helpers can participate in the opportunistic computing within a given time period, and
2. The average resource consumption ratio (RCR), which is defined as the fraction of the resources consumed by the medical user in emergency to the total resources consumed in opportunistic-computing for PHI process within a given time period [12].

5) SENDING PHI INFORMATION

This application is created by using JSP, for user convenience healthcare care details are sent via handheld devices like mobile. Instead of meeting every time these kinds of details are send through mobile devices. This was the main advantage of this module. Here the health care details are set as Blood Pressure, Heartbeat Rate, Sugar Level, and Body Temperature [11]. In this module these corresponding values are sending to the Doctor. This module working at SMTP protocol and taken Gateway as Gmail. The Jar file is created as SMS gateway. The PHI information must also be kept secure and only the medical professional and users only can view the information.

6) EMERGENCY SEARCH

This module is created using JSP, In this module when the patient id is entered then the user's personal details and medical details and then the graphical medical details are displayed. This increases the speed. Time consumption is the main advantage of this module. Efficient searching algorithms are also used to define the process and performance.

IV. CONCLUSIONS

The proposed system provides a security protecting entrepreneurial computing framework for m-Healthcare crisis, which basically abuses how to utilize artful registering to accomplish high unwavering quality of PHI procedure and transmission in crisis while minimizing the protection revelation throughout the crafty registering. Detailed security investigation indicates that the proposed Secure Privacy preserving Opportunistic Computing schema can attain the productive client driven protection access control. Through broad execution assessment, it also additionally showed the proposed schema can adjust the high-serious PHI process and transmission and minimizing the PHI security exposure in m Healthcare issues. The future work expected to bear on cell phone based tests to further confirm the viability of the proposed computing schema. Moreover, it will additionally misuse the security issues of PPSPC with inner assaulters, where the inside aggressors won't sincerely accompany the convention.

ACKNOWLEDGMENT

I would like to thank all who offers several helpful discussion and the referees for their comments, as well as to other partner who are helping in the project development.

REFERENCES

1) A. Amirbekyan and V. Estivill-Castro, "A New Efficient Privacy-Preserving Scalar Product Protocol," Proc. Sixth Australasian Conf. Data Mining and Analytics (AusDM '07), pp. 209- 214, 2007.
2) M. Atallah, and W. Du "Privacy-Preserving Cooperative Statistical Analysis," Proc. 17th Ann. Computer Security Applications Conf. (ACSAC '01), pp. 102-111, 2001,
3) 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.
4) A. Boukerche , R.W.N. Pazzi and Y. Ren, "Monitoring Patients via a Secure and Mobile Healthcare System," IEEE Wireless Comm., vol. 17, no. 1, pp. 59-65, Feb. 2010.
5) E. Borgia, M. Conti, M. Kumar, and A. Passarella, "Performance Evaluation of Service Execution in Opportunistic Computing," Proc. 13th ACM Int'l Conf. Modeling, Analysis, and Simulation of Wireless and Mobile Systems (MSWIM '10), pp. 291-298, 2010.
6) C. Clifton, and J. Vaidya and "Privacy Preserving Association Rule Mining in Vertically Partitioned Data," Proc. Eighth ACM SIGKDD Int'l Conf. Knowledge Discovery and Data Mining (KDD '02), pp. 639- 644, 2002.
7) M. Conti, S. Giordano, M. May, and A. Passarella, "From Opportunistic Networks to Opportunistic Computing," IEEE Comm. Magazine, vol. 48, no. 9, pp. 126-139, Sept. 2010.
8) M. Conti and M. Kumar, "Opportunities in Opportunistic Computing," IEEE Computer, vol. 43, no. 1, pp. 42-50, Jan. 2010.
9) J.Y. Khan, W. Liu, N.L. Myo, S.W.P. Ng, and M.R. Yuce, "Wireless Body Sensor Network Using Medical Implant Band," J. Medical Systems, vol. 31, no. 6, pp. 467-474, 2007.
10) N. Kato, X. Lin, R. Lu, Y. Nemoto, and X. Shen, "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.
11) M. Li, W. Lou, K. Ren, S. Yu and Y. Zheng, "Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption," IEEE Trans. Parallel and Distributed System, to be published.
12) Rongxing, Xiaodong Lin, and Xuemin (Sherman) Shen, "SPOC: A Secure and Privacy-preserving Opportunistic Computing Framework for Mobile-Healthcare Emergency", IEEE Transaction.
13) R. Lu, X. Lin, X. Liang, and X. Shen, "A Secure Handshake Scheme with Symptoms-Matching for mHealthcare Social Network," Mobile Networks and Applications—special issue on wireless and personal comm., vol. 16, no. 6, pp. 683-694, 2011.

14) 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.

15) 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.

16) P. Paillier, “Public-Key Cryptosystems Based on Composite Degree Residuosity Classes,” Proc. 17th Int’l Conf. Theory and Application of Cryptographic Techniques (EUROCRYPT ’99), pp. 223-238, 1999.