International Journal on Applications in Electrical and Electronics Engineering
Volume 1: Issue 2: Feburary 2015, pp 12-17. www.aetsjournal.com

A Secure Information Forwarder for Mobile Healthcare System Using Sensors

A.Santhi, V.Senthilkumar

Abstract— A secure information forwarder for mobile healthcare system that combines mobile with sensor network to monitor the health condition of patients.The mobile Healthcare system can benefit medical users by providing high-quality healthcare monitoring, the challenges facing in m-Healthcare system, especially during a medical emergency. It provides a wide range of effective, comprehensive, and convenient healthcare services. The sensor measures the health parameters dynamically, and is connected, according to the concept of Bluetooth and 3G network, to the sensor node for wireless transmission through the internet. A visualization module of the recorded biomedical data on Android mobile devices used by patients and doctors at the end of the networks in real-time. Our approach for a mobile healthcare solution is managed to process the large amount of biomedical data combining 3G network and mobile technology for daily lifestyle to users appropriately.

I. INTRODUCTION

Information and communication technologies are transforming our social interactions, lifestyles, and work places. One of the most promising applications of information technology is healthcare and wellness management. Healthcare is moving from an approach based on the reactive responses to acute conditions to a proactive approach characterized by early detection, prevention, and long term management of health conditions. The current trend places an emphasis on the monitoring of health conditions and the management of wellness as significant contributors to individual healthcare and wellbeing. This is particularly important in developed countries with a significant aging population, where information technology can significantly improve the management of chronic conditions and thereby improve quality of life. In particular, the continuous or even occasional recording of biomedical data is critical for the advancement of temperature and pressure by using sensors.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.

A.Santhi andV.Senthilkumar are with Department of Electronics and Communication Engineering, Oxford Engineering College, Pirattiyur, Trichy (Email: santhiviji12@gmail.com)

II. LITERATURE REVIEW

M. Conti, S. Giordano, M. May, and A. Passarella [2010] Personal computing devices, such as smart-phones and PDAs, are commonplace, bundle several wireless network interfaces, can support compute intensive tasks, and are equipped with powerful means to produce multimedia content. Thus, they provide the resources for what we envision as a human pervasive network: a network formed by user devices, suitable to convey to users rich multimedia content and services according to their interests and needs. Similar to opportunistic networks, where the communication is built on connectivity opportunities, we envisage a network above these resources that joins together features of traditional pervasive networks and opportunistic networks fostering a new computing paradigm: opportunistic computing. In this article we discuss the evolution from opportunistic networking to opportunistic computing; we survey key recent achievements in opportunistic networking, and describe the main concepts and challenges of opportunistic computing.

Marco Li, W. Lou, and K. Ren [2010] proposed the wireless body area network has emerged as a new technology for e-healthcare that allows the data of a patient's vital body parameters and movements to be collected by small wearable or implantable sensors and communicated using short-range wireless communication techniques. WBAN has shown great potential in improving healthcare quality, and thus has found a wide range of applications from ubiquitous health monitoring and computer assisted rehabilitation to emergency medical response systems. The security and privacy protection of the data collected from a WBAN, either while stored inside the WBAN or during their transmission outside of the WBAN, is a major unsolved concern, with challenges coming from stringent resource constraints of WBAN devices, and the high demand for both security/privacy and practicality/usability. In this article we look into two important data security issues: secure and dependable distributed data storage, and fine-grained distributed data access control for sensitive and private patient medical data. We discuss various practical issues that need to be taken into account while fulfilling the security and privacy requirements.

J. Sun and Y. Fang [2010] ProposedCross-organization or cross-domain cooperation takes place from time to time in Electronic Health Record (EHR) system for necessary and high-quality patient treatment. Cautious design of delegation mechanism must be in place as a building block of cross-domain cooperation, since the cooperation inevitably involves exchanging and sharing relevant patient data that are

considered highly private and confidential. The delegation mechanism grants permission to and restricts access rights of a cooperating partner. Patients are unwilling to accept the EHR system unless their health data are guaranteed proper use and disclosure, which cannot be easily achieved without cross-domain authentication and fine-grained access control. In addition, revocation of the delegated rights should be possible at any time during the cooperation. In this paper, we propose a secure EHR system, based on cryptographic constructions, to enable secure sharing of sensitive patient data during cooperation and preserve patient data privacy.

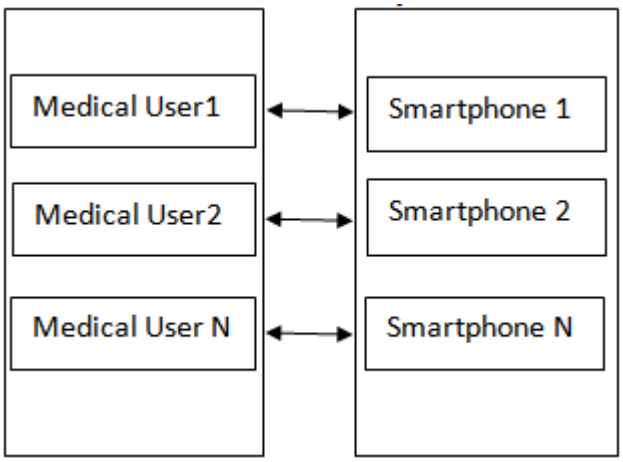
A. Passarella, M. Conti, E. Borgia, and M. Kumar [2010] proposed that we present an analytical model that depicts the service invocation process between seekers and providers. Specifically, we derive the optimal number of replicas to be spawned on encountered nodes, in order to minimize the execution time and optimize the computational and bandwidth resources used. Performance results show that a policy operating in the optimal configuration largely outperforms policies that do not consider resource constraints.Making new connections according to personal preferences is a crucial service in mobile social networking, where the initiating user can find matching users within physical proximity. Usually all the users directly publish their complete profiles for others to search. However, in many applications, the users 'personal profiles may contain sensitive information that they do not want to make public

A. Toninelli, R. Montanari, and A. Corradi [2009] Advances in wireless networks, sensors, and portable devices offer unique chances to deliver novel anytime anywhere medical services and information, thus enabling a wide range of healthcare applications, from mobile telemedicine to remote patient monitoring, from location-based medical services to emergency response. Mobile e-health has great potential to extend enterprise hospital services beyond traditional boundaries, but faces many organizational and technological challenges. In pervasive healthcare environments, characterized by user/service mobility, device heterogeneity, and wide deployment scale, a crucial issue is to discover available healthcare services taking into account the dynamic operational and environmental context of patient-healthcare operator interactions. In particular, novel discovery solutions should support interoperability in healthcare service descriptions and ensure security during the discovery process by making services discoverable by authorized users only.

III. SYSTEM ANALYSIS

A. Existing System

In the Existing system, with the pervasiveness of smart phones and the advance of wireless body sensor networks(BSN), mobile Healthcare, which extends the operation of Healthcare provider into a pervasive environment for better health monitoring, has attracted considerable interest recently.



Block Diagram

Each mobile medical user's PHI such as blood pressure and temperature, can be first collected by using sensors. Sensor data aggregated by smartphone via Bluetooth.Further transmitted to healthcare center via network.Healthcare center maintaining the data base.If up normal condition, the healthcare center by dispatching the ambulance to the medical user's current location.

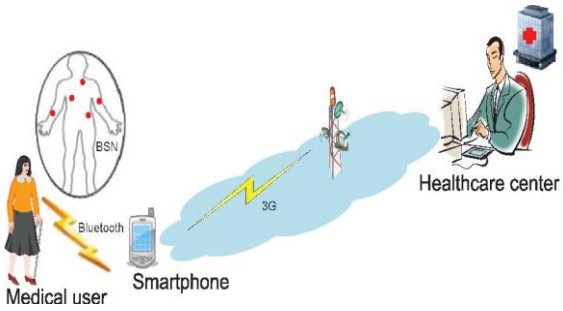


Fig 1 pervasive health monitoring in mobile healthcare system

The mobile 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. 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, 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 challenging in emergency.The personal information and very sensitive to medical users, once the 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.

B. Proposed System

In the proposed system, a secure information forwarder for mobile healthcare system using sensors, to overcome this challenge. 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. We introduce an efficient user-centric privacy access control, which is based on an attribute-based access control and a new privacy preserving scalar product computation (PPSPC) technique, and allows a medical user to decide who can participate in the opportunistic computing to assist in processing.We propose mobile healthcare system, which consists of three parts: system initialization, user-centric privacy access control for m-Healthcare emergency, and analysis of opportunistic computing in m-Healthcare emergency.

B1. Body sensor network

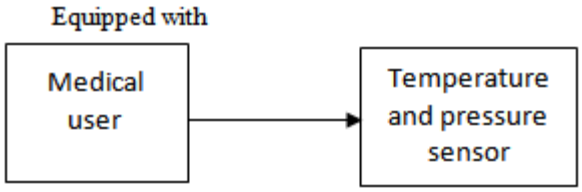


Fig 2 body sensor network

The temperature and pressure sensor will be equipped directly in the medical user. The sensor data will transmit the user details for every time period that we have indicated. For example, each mobile medical user's personal health information such as blood pressure and temperature and other details will be captured by the medical users Smartphone.

B2. Smartphone communication

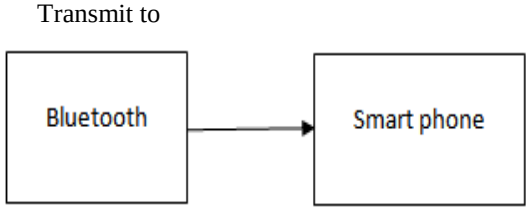


Fig 3 smartphone communication

For each sensor data transmitted from sensor will be aggregated by the Smartphone that, the medical users having with them using Bluetooth communication. This received medical information or symptom will be transmitted to healthcare center periodically with the help of 3G network.

B3. Healthcare center

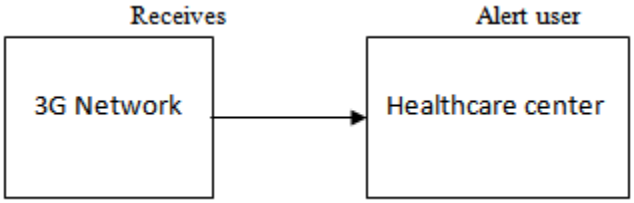


Fig 4 Healthcare center

A secure and privacy-preserving opportunistic computing framework for mobile Healthcare emergency. 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. To introduces a user centric two-phase privacy access control to only allow those medical users who have similar symptoms to participate in opportunistic computing.

I. MODELS AND DESIGN GOAL

A. System Model

In our system model, we consider a trusted authority and a group of medical users. TA is a trustable and powerful entity located at healthcare center, which is mainly responsible for the management of the whole m-Healthcare system, e.g., initializing the system, equipping proper body sensor nodes and key materials to medical users.

Each medical user is equipped with personal BSN and smartphone which can periodically collect PHI and report them to the healthcare center for achieving better health care quality. Unlike in-bed patients at home or hospital, medical users are considered as mobile ones, i.e., walking outside. BSN and smartphone are two key components for the success of m-Healthcare system. To guarantee the high reliability of BSN and smartphone, the batteries of BSN and smartphone should be charged up every day so that the battery energy can support daily remote monitoring task in m-Healthcare system. Since the BSN is dedicated for remote monitoring, after being charged every day, BSN can deal with not only the normal situations but also the emergency cases in m-Healthcare.

B. Security Model

Mobile healthcare system can enhance the reliability for high-intensive PHI process and transmission in m-Healthcare emergency. However, since PHI is very sensitive, a medical user, even in emergency, will not expect to disclose the PHI to all passing-by medical users. Instead, may only disclose PHI to those medical users who have some similar symptoms. In this case, the emergency situation can be handled by opportunistic computing with minimal privacy disclosure.

Specifically, the security model, essentially define two-phase privacy access control in opportunistic computing, which are required for achieving high-reliable PHI process and transmission in m-Healthcare emergency. The access control only allows those medical users who have some similar symptoms to participate in the opportunistic computing. The reason is that those medical users, due to with the similar symptoms, are kind of skilled to process the same type PHI.

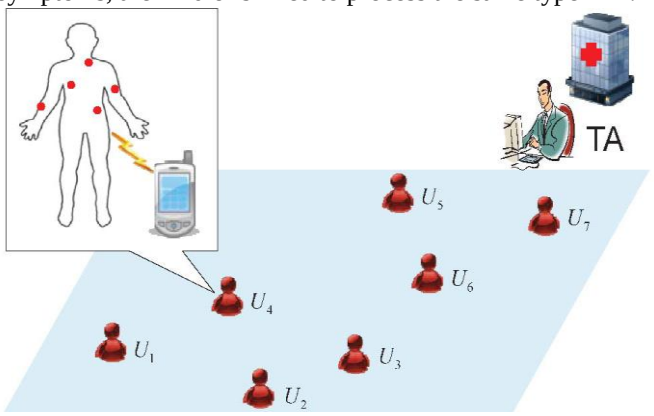


Fig 5 system model

C. Design Goal

The design goal is to develop a secure mobile healthcare system to provide high reliability of PHI process and transmission while minimizing PHI privacy in mobile Healthcare emergency. To apply opportunistic computing in m-Healthcare emergency to achieve high reliability of PHI process and transmission; and develop user-centric privacy access control to minimize the PHI privacy.The system using bilinear pairings, system initialization and user centric privacy access control.

The residual power of smartphone may be insufficient for high-intensive PHI process and transmission. To deal with this embarrassing situation, opportunistic computing provides a promising solution in mobile Healthcare system. Each medical user accessing the smartphone. The sensor data information transmit to the smartphone via Bluetooth. The smartphone data transmit to the healthcare center server and view the patient's current location.

V. RESULTS AND DISCUSSION

A. Simulation Output

Create app with android, eclipse software can run call service program. Google announced the availability of app inventor for eclipse, a web based visual development environment for novice programmers, based on MIT's open blocks java library and providing access to android devices GPS, accelerometer and orientation data, phone functions, text messaging, speech to text conversion, contact data, persistent storage and web services.

Android virtual device manager

The AVD manager provides a graphical user interface in which create and manage android virtual device, which are required by the android emulator.

Launch the AVD manager in one of the following ways:

- In eclipse: select window →android virtual device manager, or click the AVD manager icon in the toolbar.
- In android studio: select tools→android→AVD manager icon in the toolbar.

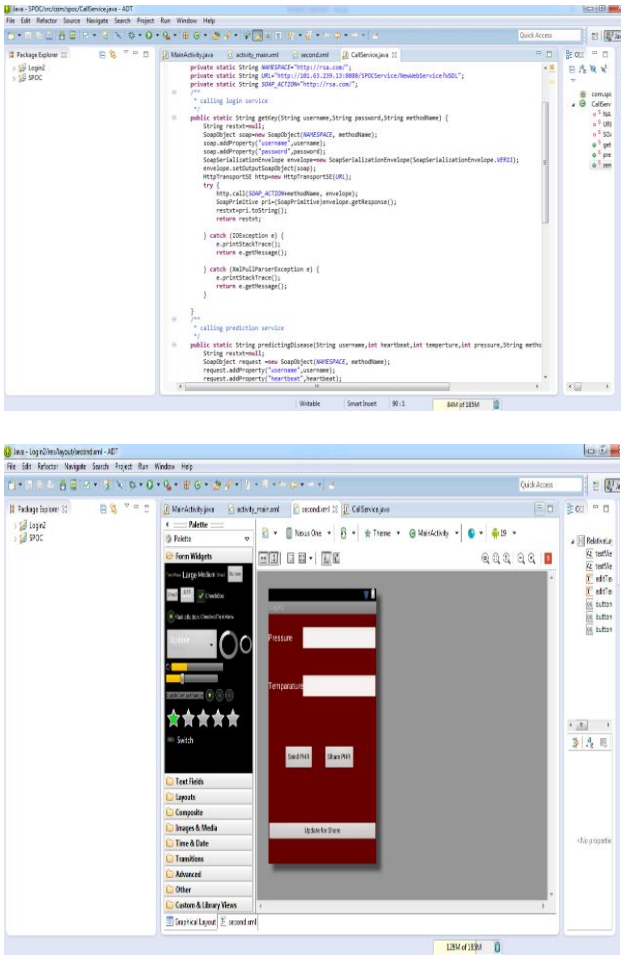


Fig 6 simulation output

Managing AVD

An AVD is a device configuration for the android emulator that allows model different configurations of android powered devices.

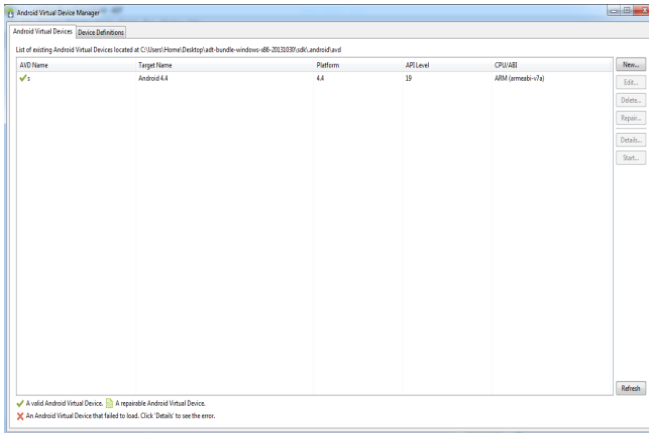


Fig 7 (a) AVD Manager

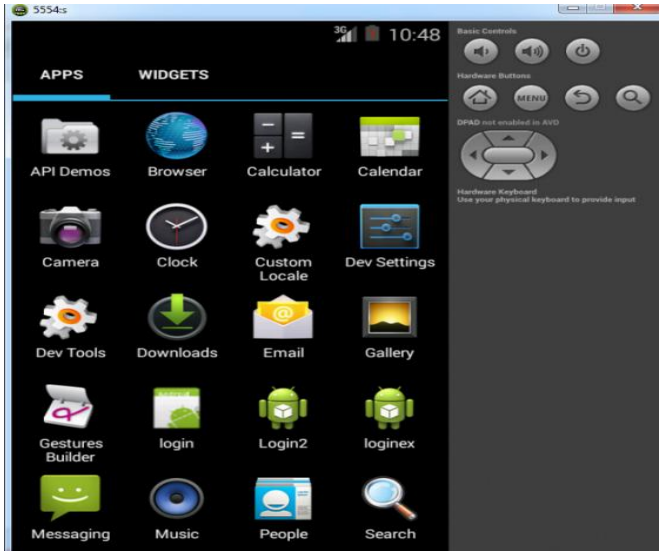


Fig 7 (b) AVD Manager

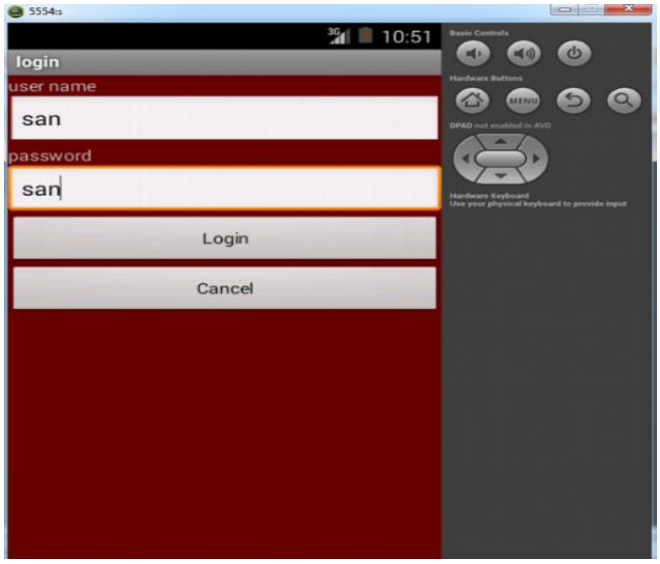


Fig 8 (a) Eclipse- AVD manager output

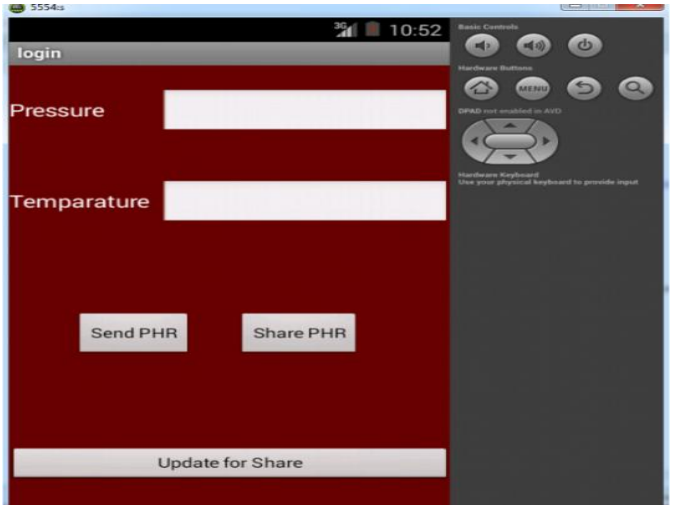


Fig 8 (b) Eclipse- AVD manager output

VI. CONCLUSION AND FUTUREWORK

A. Conclusion

A secure information forwarder for mobile healthcare system using sensors, the Android mobile devices is successfully implemented. An information forwarder are designed and used for the measurement of temperature sensor and blood pressure sensor, while the Android mobile device is used to provide a mobile healthcare service by means of an Android application running on a Samsung device with wireless internet access.Medical users can walk outside and receive the high-quality healthcare monitoring. By combining the 3G network and mobile communication techniques, significant network extension and the higher accessibility of mobile healthcare system has been achieved. We have proposed the ideas of establishing the 3G applications. With the use of comfortable wearable sensors in global areas, the proposed mobile healthcare system promises to improve the flexibility and scalability of healthcare applications. In addition, an Android mobile healthcare application can be deployed on mobile devices, such as smartphones, tablet PCs, and laptops to monitor biomedical temperature and pressure details in real time for healthcare services. With an exponentially increasing number of sensors and opportunities in the marketplace, this field of research has the potential to significantly change and improve the efficiency of the healthcare system. Based on our results, we conclude that, with the evolution of network integration and the management of embedded devices operating multimodal tasks a more precise and universal healthcare service scheme can be realized.

B. Future Work

An information forwarder for mobile healthcare system, which is connected to the sensors placed on the patient's body to collect health parameters, further transfers the sensor data to the Bluetooth device. The Bluetooth device transfers the data to the Android mobile application. The 3G network device provides reliable communication to transmit a patient's

biomedical data to a healthcare center server via the internet. This program performs an accurate recognition even if the patient is abnormal condition. Receiving all the transmitted data via 3G network communication in the server, the monitoring data stores in a database and plots all the measured biomedical data dynamically. Various algorithms are combined and implemented as mobile application software with the Java Android language to handle all the processes from the server. Using algorithm and filtered the abnormal biomedical data only transfers to a healthcare center server in an android application .The query processes handle the communication between the server and Android mobile device to display the patient current location and nearby hospital on a mobile screen in real time. All the studies and implementation will be done in the next phase and any advancement if possible, is expected to be incorporated with that.

REFERENCES

[1] R. Zhang, Y. Zhang, J. Sun, and G. Yan, "Fine-Grained Private Matching for Proximity-Based Mobile Social Networking," Prof. of INFOCOM '12, pp. 1-9, 2012.

[2] R. Lu, X. Lin, X. Liang, and X. Shen, "A Secure Handshake Scheme with Symptoms Matching for m-Healthcare Social Network," Mobile Networks and Applications special issue on wireless and personal comm., vol. 16, no. 6, pp. 683-694, 2011.

[3] W. Dong, V. Dave, L. Qiu, and Y. Zhang, "Secure Friend Discovery in Mobile Social Networks," Prof. of INFOCOM '11, pp. 1647-1655, 2011.

[4] R. Lu, X. Lin, X. Liang, and X. Shen, "Secure Handshake with Symptoms-Matching: The Essential to the Success of M healthcare Social Network," Proc. Fifth Int'l Conf. Body Area Networks (BodyNets '10), 2010.

[5] Y. Ren, R.W.N. Pazzi, and A. Boukerche, "Monitoring Patients via a Secure and Mobile Healthcare System," IEEE Wireless Comm., vol. 17, no. 1, pp. 59-65, Feb. 2010.

[6] A. Passarella, M. Conti, E. Borgia, and M. Kumar, "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.

[7] 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.

[8] J. Sun and Y. Fang, "Cross-Domain Data Sharing in Distributed Electronic Health Record Systems," IEEE Trans. Parallel Distributed and Systems, vol. 21, no. 6, pp. 754-764, June 2010.

[9] 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

[10] M. Conti and M. Kumar, "Opportunities in Opportunistic Computing," IEEE Computer, vol. 43, no. 1, pp. 42-50, Jan. 2010

[11] A. Toninelli, R. Montanari, and A. Corradi, "Enabling Secure Service Discovery in Mobile Healthcare Enterprise Networks," IEEE Wireless Comm., vol. 16, no. 3, pp. 24-32, June 2009.

[12] 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.

[13] M.R. Yuce, S.W.P. Ng, N.L. Myo, J.Y. Khan, and W. Liu, "Wireless Body Sensor Network Using Medical Implant Band," J. Medical Systems, vol. 31, no. 6, pp. 467-474, 2007.

[14] 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.

[15] X. Lin, X. Sun, P. Ho, and X. Shen, "GSIS: A Secure and Privacy Preserving Protocol for vehicular communications," IEEE Trans. Vehicular Technology, vol. 56, no. 6, pp. 3442-3456, Nov. 2007.

[16] 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.

[17] X. Lin, X. Sun, P. Ho, and X. Shen, "GSIS: A Secure and Privacy Preserving Protocol for vehicular communications," IEEE Trans. Vehicular Technology, vol. 56, no. 6, pp. 3442-3456, Nov. 2007.

[18] J. Vaidya and C. Clifton, "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- 4, 2002.

[19] W. Du and M. Atallah, "Privacy-Preserving Cooperative Statistical Analysis," Proc. 17th Ann. Computer Security Applications Conf. (ACSAC '01), pp. 102-111, 2001.

[20] 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.