International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622
NATIONAL CONFERENCE on Developments, Advances & Trends in Engineering Sciences (NCDATES- 09th & 10th January 2015)

RESEARCH ARTICLE OPEN ACCESS

A Secure and Privacy Preserving Opportunities Computing Framework for Mobile Health Care Emergency

*Mr.D.Devendar, **Mr.M. Narendra
*M.Tech scholar, CMR Engineering College
**Asst.Professor, Dept. of CSE, CMR Engineering College,Hydearbad,
E-Mail: narendramupparaju06@gmail.com

Abstract
With the pervasiveness of smart phones and the advance of wireless body sensor networks (BSNs), mobile Healthcare (m-Healthcare), which extends the operation of Healthcare provider into a pervasive environment for better health monitoring, has attracted considerable interest recently. However, the flourish of m-Healthcare still faces many challenges including information security and privacy preservation. In this paper, we propose a secure and privacy-preserving opportunistic computing framework, called SPOC, for m-Healthcare emergency. 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. In specific, to leverage the PHI privacy disclosure and the high reliability of PHI process and transmission in m-Healthcare emergency, we introduce an efficient user-centric privacy access control in SPOC framework, 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 his overwhelming PHI data. Detailed security analysis shows that the proposed SPOC framework can efficiently achieve user-centric privacy access control in m-Healthcare emergency. In 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 m-Healthcare emergency

Introduction:

In our aging society, mobile Healthcare (m-Healthcare) system has been envisioned as an important application of pervasive computing to improve health care quality and save lives, where miniaturized wearable and implantable body sensor nodes and smartphones are utilized to provide remote healthcare monitoring to people who have chronic medical conditions such as diabetes and heart disease. 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 (BSN) formed by body sensor nodes, medical users can walk outside and receive the high-quality healthcare monitoring from medical professionals anytime and anywhere. 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 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 user 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.

Recently, OPPORTUNISTIC computing, as a new pervasive computing paradigm, has received much attention. Essentially, opportunistic computing is characterized by exploiting all available computing resources in an opportunistic environment to provide a platform for the distributed execution of a computing-intensive task. For example once the execution of a task exceeds the energy and computing power available on a single node, other opportunistically contacted nodes can contribute to the execution of the original task by running a subset of task, so that the original task can be reliably performed. Obviously, opportunistic computing paradigm can be applied in m-Healthcare emergency to resolve the challenging reliability issue in PHI process. However, PHI are 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. In this paper, we propose a new secure and privacy preserving opportunistic computing framework, called SPOC, to address this challenge. With the proposed SPOC 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.

Literature Survey

Literature survey is the most important step in software development process. Before developing the tool it is necessary to determine the time factor, economy n company strength. Once these things r satisfied, ten next steps is to determine which operating system and language can be used for developing the tool. Once the programmers start building the tool the programmers need lot of external support. This support can be obtained from senior programmers, from book or from websites. Before building the system the above consideration r taken into account for developing the proposed system.

Distributed systems are groups of networked computers, which have the same goal for their work. The terms "concurrent computing", "parallel computing", and "distributed computing" have a lot of overlap, and no clear distinction exists between them.[13] The same system may be characterized both as "parallel" and "distributed"; the processors in a typical distributed system run concurrently in parallel.[14] Parallel computing may be seen as a particular tightly-coupled form of distributed computing,[15] and distributed computing may be seen as a loosely-coupled form of parallel computing.[5] Nevertheless, it is possible to roughly classify concurrent systems as "parallel" or "distributed" using the following criteria:

- In parallel computing, all processors have access to a shared memory. Shared memory can be used to exchange information between processors.[16]
- In distributed computing, each processor has its own private memory (distributed memory). Information is exchanged by passing messages between the processors.[17]

The figure on the right illustrates the difference between distributed and parallel systems. Figure (a) is a schematic view of a typical distributed system; as usual, the system is represented as a network topology in which each node is a computer and each line connecting the nodes is a communication link. Figure (b) shows the same distributed system in more detail: each computer has its own local memory, and information can be exchanged only by passing messages from one node to another by using the available communication links. Figure (c) shows a parallel system in which each processor has a direct access to a shared memory.

The situation is further complicated by the traditional uses of the terms parallel and distributed *algorithm* that do not quite match the above definitions of parallel and distributed *systems*; see the section Theoretical foundations below for more detailed discussion. Nevertheless, as a rule of thumb, high-performance parallel computation in a shared-memory multiprocessor uses parallel algorithms while the coordination of a large-scale distributed system uses distributed algorithms.

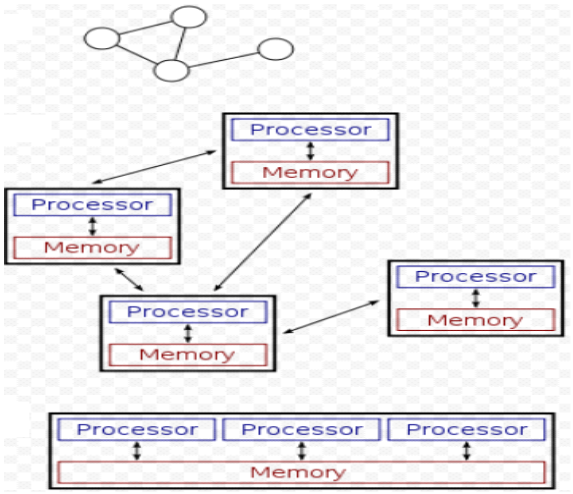


Fig1:

Parallel computing is a form of computation in which many calculations are carried out simultaneously,[1] operating on the principle that large problems can often be divided into smaller ones, which are then solved concurrently ("in parallel"). There are several different forms of parallel computing: bit-level, instruction level, data, and task parallelism. Parallelism has been employed for many years, mainly in high-performance computing, but interest in it has grown lately due to the physical constraints preventing frequency scaling.[2] As power consumption (and consequently heat generation) by computers has become a concern in recent years,[3] parallel computing has become the dominant paradigm in computer architecture, mainly in the form of multicore processors.[4]

Parallel computers can be roughly classified according to the level at which the hardware supports parallelism, with multi-core and multi-processor computers having multiple processing elements within a single machine, while clusters, MPPs, and grids use multiple computers to work on the same task. Specialized parallel computer architectures are sometimes used alongside traditional processors, for accelerating specific tasks.

Parallel computer programs are more difficult to write than sequential ones,[5] because concurrency introduces several new classes of potential software bugs, of which race conditions are the most common. Communication and synchronization between the different subtasks are typically some of the greatest obstacles to getting good parallel program performance.

The maximum possible speed-up of a program as a result of parallelization is observed as Amdahl's law.

System Design

i.Existing System

In Existing System, According to the sensex over the age of 65 is expected to hit 70 million by 2030, having doubled since 2000. Health care expenditures projected to rise to 15.9% by 2010. The cost of health care for the nation's aging population has become a national concern are important for understanding how the opportunistic computing paradigm work when resources available on different nodes can be opportunistically gathered together to provide richer functionality, they have not considered the potential security and privacy issues existing in the opportunistic computing paradigm.

ii Proposed System

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

Advantages Shift from a clinic-oriented, centralized healthcare system to a patient-oriented, distributed healthcare system Reduce healthcare expenses through more efficient use of clinical resources and earlier detection of medical conditions Challenges Performance, Reliability, Scalability, QoS, Privacy, Security and more prone to failures, caused by power exhaustion, software and hardware faults, natural disasters, malicious attacks, and human errors etc.

Implementation.

Implementation is the stage of the project when the theoretical design is turned out into a working system. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective.

The implementation stage involves careful planning, investigation of the existing system and it's constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods.

Modules

1. Pervasive health monitoring in M-Healthcare
2. Body Sensor Network
3. Security Analysis
4. Performance Evolution
5. Simulation Setup
6. Report Generation

i Pervasive Health Monitoring in M-Healthcare

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 by BSN, and then

aggregated by smart phone 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.

ii Body Sensor Network

In this module, Body area network (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)

iii.Security Analysis

In this Module 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. Specifically, we
i)apply opportunistic computing in m-Healthcare emergency to achieve high-reliability of PHI process and transmission; and
ii) develop user-centric privacy access control to minimize the PHI privacy disclosure.

iv. Performance Evolution

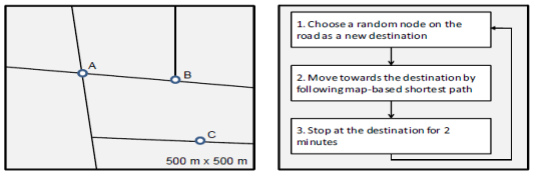
In this module, the performance metrics used in the evaluation are :
1) The average number of qualified helpers (NQH), which indicates how many qualified helpers can participate in the opportunistic computing within a given time period, and
2) The average resource consumption ratio (RCR), which is defined 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.

v. Simulation Setup

In this Module, the simulator implements the application layer under the assumptions that the communications between smart phones and the communications between BSNs and smart phones are always workable when they are within each other's transmission ranges.

vi. Report generation

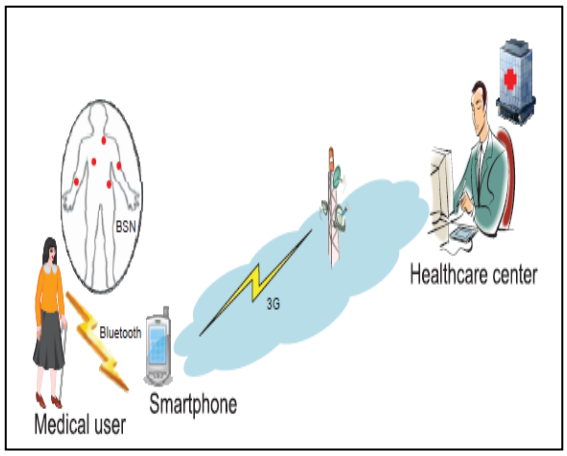
In this module, Health care center generate crystal report from the database collection for future reference.

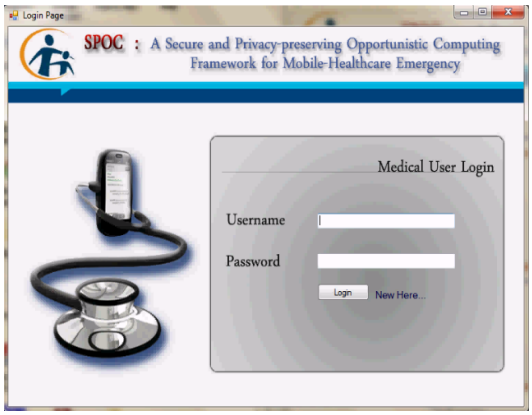


(a) Simulation area (b) Mobility model

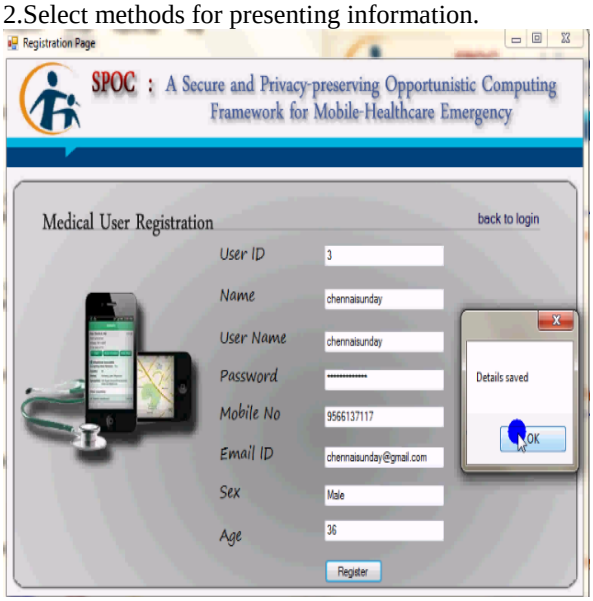
Results:

A quality output is one, which meets the requirements of the end user and presents the information clearly. In any system results of processing are communicated to the users and to other system through outputs. In output design it is determined how the information is to be displaced for immediate need and also the hard copy output. It is the most important and direct source information to the user. Efficient and intelligent output design improves the system's relationship to help user decision-making.
1. Designing computer output should proceed in an organized, well thought out manner; the right output must be developed while ensuring that each output element is designed so that people will find the system can use easily and effectively. When analysis design computer output, they should Identify the specific output that is needed to meet the requirements.





2.Select methods for presenting information.



3. Create document, report, or other formats that contain information produced by the system.

The output form of an information system should accomplish one or more of the following objectives.

- Convey information about past activities, current status or projections of the
- Future.
- Signal important events, opportunities, problems, or warnings.
- Trigger an action.
- Confirm an action.

Conclusion

In this paper, we have proposed a secure and privacy preserving opportunistic computing (SPOC) framework for m-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 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 smart phone 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.

References

[1]. M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "Above the clouds: A berkeley view of cloud computing," University of California, Berkeley, Tech. Rep. USB-EECS-2009-28, Feb 2009.

[2]. "The apache cassandra project," http://cassandra.apache.org/. L. Lamport, "The part-time parliament," ACM Transactionson Computer Systems, vol. 16, pp. 133–169, 1998.

[3]. N. Bonvin, T. G. Papaioannou, and K. Aberer, "Cost-efficient and differentiated data availability guarantees in data clouds," in Proc. of the ICDE, Long Beach, CA, USA, 2010.

[4]. O. Regev and N. Nisan, "The popcorn market. online markets for computational resources," Decision Support Systems,vol. 28, no. 1-2, pp. 177 – 189, 2000.

[5]. A. Helsinger and T. Wright, "Cougaar: A robust configurable multi agent platform," in Proc. of the IEEE Aerospace Conference, 2005.

[6]. J. Brunelle, P. Hurst, J. Huth, L. Kang, C. Ng, D. C. Parkes, M. Seltzer, J. Shank, and S. Youssef, "Egg: an extensible and economics-inspired open grid computing platform," in Proc. of the GECON, Singapore, May 2006.

[7]. J. Norris, K. Coleman, A. Fox, and G. Candea, "Oncall: Defeating spikes with a free-market application cluster," in Proc. of the International Conference on Autonomic Computing, New York, NY, USA, May 2004.

[8]. C. Pautasso, T. Heinis, and G. Alonso, "Autonomic resource provisioning for software business processes," Information and Software Technology, vol. 49, pp. 65–80, 2007.

[9]. A. Dan, D. Davis, R. Kearney, A. Keller, R. King, D. Kuebler, H. Ludwig, M. Polan, M. Spreitzer, and A. Youssef, "Web services on

demand: Wsla-driven automated management," IBM Syst. J., vol. 43, no. 1, pp. 136–158, 2004.

[10]. M. Wang and T. Suda, "The bio-networking architecture: a biologically inspired approach to the design of scalable, adaptive, and survivable/available network applications," in Proc. of the IEEE Symposium on Applications and the Internet, 2001.

[11]. N. Laranjeiro and M. Vieira, "Towards fault tolerance in web services compositions," in Proc. of the workshop on engineering fault tolerant systems, New York, NY, USA, 2007.

[12]. C. Engelmann, S. L. Scott, C. Leangsuksun, and X. He, "Transparent symmetric active/active replication for servicelevel high availability," in Proc. of the CCGrid, 2007.

[13]. J. Salas, F. Perez-Sorrosal, n.-M. M. Pati and R. Jim´enez- Peris, "Ws-replication: a framework for highly available web services," in Proc. of the WWW, New York, NY, USA, 2006,

** **Narendra Mupparaju** Master of Engineering from Hindustan University Chennai B.Tech IT from Prakasam Engineering College. He is having more than 4 years of experience has guided UG & PG students, currently he is working as Asst Prof at CMR of Engineering College,Hyderabad. His research areas include Computer Network, Compiler Design, Operating system, Linux.