Scientific Journal of Impact Factor (SJIF): 4.72

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 5, Issue 01, January -2018

An Enhanced Auditability and secured privacy preserving Approaches for Cloud Assisted Mobile Access of Health Data

[1]K. Ravikumar, [2] G. Sumithra,

[1]*Asst.professor, Dept. of. Computer Science, Tamil University, Thanjavur-613010*
[2] *Research Scholar, Dept. of. Computer Science, Tamil University, Thanjavur-613010*

Abstract —*This technique is developed with the intention of privacy issues in the current cloud data storage, curbing the adoption of electronic healthcare systems and the wild success of cloud service models, this propose to build privacy into mobile healthcare Systems with the help of the private cloud. This system offers salient features including efficient key management, privacy-preserving data storage, and retrieval, especially for retrieval at emergencies, and auditability for misusing health data. Precisely, this propose to integrate key management from pseudorandom number generator for unlink capability, a secure indexing method for privacy maintaining keyword search which hides both search and access configurations established on redundancy, and integrate the concept of attribute-based encryption with threshold authorization for providing role-based access control with auditability to avoid potential misbehavior, in both normal and emergency cases.*

Keywords: *Access Regulator, Audit Capability, E Health, Confidentiality*

1. INTRODUCTION

The mobile Healthcare (m-Healthcare) system has been intended as a significant application of universal computing to advance health care feature and save lives, where reduced wearable and implantable body sensor nodes and smart phones are used to provide distant healthcare monitoring to people who have long-lasting medical circumstances such as diabetes and heart disease Precisely, in an m-Healthcare system, medical consumers are no longer needed to be monitored within home or hospital environments. Instead, after being prepared with smart phone 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, 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.
Finally, they are further transmitted to the remote healthcare center via 3G networks. Outstretched on these collected PHI data, medical experts at healthcare epicenter can constantly monitor medical operators' health circumstances and as well quickly react to users' lethal situations and save their lives by forwarding ambulance and medical employees to an emergency location in a timely manner.

Even though m-Healthcare system can advantage therapeutic consumers by providing extraordinary quality universal healthcare observing, the decoration of m-Healthcare system still pivots upon how we fully comprehend and achieve the encounters facing in m-Healthcare system, particularly during a medical emergency. To clearly illustrate the challenges in m-Healthcare emergency, itconsiders the following scenario. In overall, a medical consumer's PHI should be reported to the healthcare epicenter every 5 minutes for standard 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 quantity of PHI data will be produced in a very short old-fashioned of time, and they additional should be reported every 10 seconds for high-intensive monitoring before ambulance and medical personnel's arrival.

Though, since mobile phone is not only used for healthcare observing, but also for other submissions, i.e., calling the friends, the Smartphone's liveliness could be inadequate 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 occasion integer will spread 50, which is not insignificant and clearly indicates the reliability of m-Healthcare system is still perplexing in emergency.

Recently, opportunistic calculating, as a new pervasive computing paradigm, has received much attention.
Principally, unscrupulous computing is categorized by exploiting all available calculating resources in an unscrupulous environment to provide a platform for the dispersed execution of a computing-intensive task. For example, once the execution of a task exceeds the energy and computing power Obtainable on a solitary node, other unscrupulously 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, unscrupulous computing paradigm can be applied in m-Healthcare emergency to resolve the perplexing reliability issue in PHI process.

Though, PHI is individual information and very complex to medical consumers, once the raw PHI data are handled in unscrupulous computing, the privacy of PHI would be revealed. Consequently, how to equilibrium the high reliability of PHI process while minimalizing the PHI privacy revelation during the opportunistic computing becomes a perplexing issue in m-Healthcare emergency.

2. RELATED WORK

Existing opportunistic networks are moving from academia to real world scenarios. This will involve, in the near future, the design and production of hardware platforms characterized by low cost and small form factor. As a consequence, the amount of resources available on a single node, i.e. computing power, storage, and energy, will be even more constrained than today. This paper faces the problem of storing and executing an application that exceeds the memory resources available on a single node. The solution is based on the idea of partitioning the application code into a number of opportunistically cooperating modules. 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.

It should be noted that, since these kinds of systems have been designed and manufactured to be used in research projects, both the form factor and production costs are not adequate for their adoption in real ubiquitous computing scenarios. A massive adoption of WSNs requires reducing the size and cost of nodes by an order of magnitude.

Obviously, this also implies a significant reduction of the computing and storage capabilities of nodes. This trend is confirmed by the advent of alternative platforms such as Spec [5], an experimental node architecture designed at Berkeley. Spec is a prototype of “mote on a chip”: microcontroller, wireless radio transceiver, and analog to digital converter are packed all together on a single die of a cubic millimeter. Only few external passive components are necessary. In order to optimize the power consumption, Spec uses dedicated hardware accelerators for low level primitives. The total amount of memory available for both data and programs is 3KBytes.

With opportunistic networking, routing and forwarding schemes are designed to benefit from the randomness and uncertainty of the network topology. The basic idea behind opportunistic networking is that two nodes may be able to communicate even if a completely connected path never exists between them.

Communication is generally obtained through extensive buffering of messages at intermediate nodes, waiting for the chance to get closer to the destination. Opportunistic networking has been successfully used to extend the capacity of the wireless channel beyond the classical theoretical limit [4] and to enhance network coding and out perform traditional routing schemes [7]. Readers interested in a more comprehensive list of works and projects related to opportunistic networking are redirected.

With opportunistic computing, the execution of applications is supported by spare computational resources available somewhere in the network. No assumption is made on the availability and on the position of such resources. Currently, opportunistic computing is mainly applied in wired networks to facilitate the construction of grid-based applications.

Programs for wireless sensor networks are specialized for the particular scenario of operation. Formerly, programs were developed in low level languages, but in the last few years Java and C like languages gained popularity. The use of high level languages gave an impulse to the production of programs with modular structure, where modules represent both parts of the application logic and services of the operating system. Moreover, they stimulated the implementation of large libraries that can be accessed by developers to pick up modules and generate new programs with reduced effort.

The study of opportunistic computing has gained the great interest from the research community recently, and we briefly review some of them related to our work. In Aventis et al. introduce the opportunistic computing paradigm in wireless sensor network to solve the problem of storing and executing an application that exceeds the memory resources available on a single sensor node.

Especially, their 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 Passarella et al. evaluate the performance of service execution in opportunistic computing. Specifically, they first abstract resources in pervasive computing as services, which are opportunistically contributed by providers and invoked by seekers. Then, they present a complete analytical model to depict the service invocation process between seekers and providers, and 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.

Although [13] and [14] 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 [15], [16] different from the above works.

3. PROPOSED DESIGN

This proposed technique is a new secure and privacy preserving opportunistic computing framework, called CBPHS, to address this challenge. With the projected CBPHS 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 USER HEALTH DATA process and minimizing USER HEALTH DATA privacy disclosure in m-Healthcare emergency. Specifically, the main contributions of this system have been developed with multiple attributes.

This technique is to leverage the USER HEALTH DATA privacy disclosure and the high reliability of USER HEALTH DATA process and transmission in m-Healthcare emergency, it introduce an efficient user-centric privacy access control in CBPHS framework, which is based on an attribute-based access control and a new UIN(unique Number) based 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 USER HEALTH DATA data. Comprehensive security investigation shows that the projected CBPHS framework can proficiently achieve user-centric privacy access control in m-Healthcare crisis. In addition, performance evaluations via extensive simulations demonstrate the CBPHS's effectiveness in term of providing high reliable USER HEALTH DATA process and transmission while minimizing the privacy disclosure during m-Healthcare emergency.

3.1. HEALTH CENTER SERVER

In this module new secure and privacy preserving opportunistic computing health server has been installed, to address the m-user data storing and retrieval on a secured process. With the projected CBPHS (CLOUD BASED PERSONAL HEALTH SYSTEM) outline, discretely medical consumer in emergency can achieve the user-centric privacy access control to allow entering into the system only qualified m-users to participate in the opportunistic computing to balance the high reliability of PHI process in m-Healthcare emergency server.

3.2. MOBILE USER DATA PHI METRIC

This module mainly deals with the process of registering the m-user PHI data into the mobile health care server and provides the login credentials for further authentication process, it shows the secure and privacy preserving opportunistic computing framework for m-Healthcare emergency, With CBPHS (CLOUD BASED PERSONAL HEALTH SYSTEM) , the incomes available on other unscrupulously communicated medical users' phones can be collected together to deal with the computing-intensive PHI procedure in emergency situation. Since the PHI will be disclosed during the process in opportunistic computing, to minimize the PHI privacy disclosure, CBPHS (CLOUD BASED PERSONAL HEALTH SYSTEM) announces a user-centric two-phase confidentiality access control to solitary permit those medical users who have similar symptoms to contribute in unscrupulous computing.

3.3. M-HEALTH EMERGENCY REQUEST PROCESSOR

The major process of the system is to provide the PHI data to the particular emergency user by validate the user's request on the basis of timestamp, location based user search ,status of the donors and active directory user search implemented attributed based access control can help the emergency user in emergency 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 shown in figure 1.

Figure 1. Users Symptoms

3.4. SERVICE PROVIDER

The PHI data has send to the particular emergency m-user by the sending the OTP(one time password) code to the donors list after confirm the code the complete PHI m-user list has send to the emergency requester for further communication has been made directly.

4. PROPOSED ALGORITHM: CBPHS

The major process of the system is to provide the PHI data to the particular emergency user by validate the user's request on the basis of timestamp, location based user search ,status of the donors and active directory user search implemented attributed based access control can help the emergency user in emergency and PPSPC protocol can further control only those medical users who have identical symptoms to contribute the opportunistic computing while without directly revealing users' symptoms.

The PHI data has send to the particular emergency m-user by the sending the OTP (one-time password) code to the donors list after confirm the code the complete PHI m-user list has send to the emergency requester for further communication has been made directly.

5. CONCLUSION

This proposed model CBPHS (CLOUD BASED PERSONAL HEALTH SYSTEM) a secure and privacy preserving opportunistic computing 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 CBPHS (CLOUD BASED PERSONAL HEALTH SYSTEM) framework can achieve the efficient user-centric privacy access control. In addition, through extensive performance evaluation, this demonstrated the proposed CBPHS (CLOUD BASED PERSONAL HEALTH SYSTEM) framework can balance the high-intensive PHI process and transmission and minimizing the PHI privacy disclosure in m-Healthcare emergency.

REFERENCES

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

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

[3]. 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.

[4].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.

[5]M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption," IEEE Trans. Parallel and Distributed System, to be published.

[7].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.

[8].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.

[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] 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. 639-644, 2002.

[12].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.

[13].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.

[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] X. Lin, R. Lu, X. Shen, Y. Nemoto, and N. Kato, "Sage: A Strong Privacy-Preserving Scheme against Global Eavesdropping forEhealth Systems," IEEE J. Selected Areas in Comm., vol. 27, no. 4, pp. 365-378, May 2009.

