*International Journal of Multidisciplinary Research and Modern Education (IJMRME)*
*ISSN (Online): 2454 - 6119*
*(www.rdmodernresearch.com) Volume II, Issue II, 2016*

# STUDY OF A SECURE AND PRIVACY-PRESERVING OPPORTUNISTIC COMPUTING FRAMEWORK FOR MOBILE-HEALTHCARE EMERGENCY

**Pramod B. Deshmukh*, Nilesh N. Wani*, Laxmikant S. Malphedwar* & Deepali A. Ghanwat****

* Assistant Professor, D.Y Patil College of Engineering, Akurdi, Pune, Maharashtra
** Assistant Professor, Shri Chhatrapati Shivaji Maharaj COE, Nepti, Ahmadnagar, Maharashtra

**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.*

**Key Words*:*** Security, Healthcare, Opportunistically, PHI & SPOC

## 1. Introduction:

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 smart phones are utilized to provide remote healthcare monitoring to people who have chronic medical conditions such as diabetes and heart disease [1], [2], [3], [4], [5].

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 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, as shown in Figure 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 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 [6].

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.


Figure 1: Pervasive health monitoring in m-Healthcare system.

Recently, opportunistic computing, as a new pervasive computing paradigm, has received much attention [7], [8], [9], [10]. 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 [7].

Obviously, opportunistic computing paradigm cans 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. 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 sand minimizing PHI privacy disclosure in m-Healthcare emergency. Specifically, the main contributions of this paper are threefold.

First, we propose SPOC, a secure and privacy-preserving opportunistic computing framework form-Healthcare emergency. With SPOC, 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, SPOC introduces a user-centric two-phase privacy access control to only allow those medical users who have similar symptoms to participate in opportunistic computing. Second, to achieve user-centric privacy access control in opportunistic computing, we present an efficient attribute-based access control and a novel nonhomomorphic 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 [7], [8], [9], [10]. Yet most of them are relyingon time consuming homomorphic encryption technique [14], [15]. 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. Third, to validate the effectiveness of the proposed SPOC framework in m-Healthcare emergency, we also develop a custom simulator built in Java. Extensive simulation results show that the proposed SPOC framework can help medical users to balance the high reliability of PHI process and minimizing the PHI privacy disclosure in m-Healthcare emergency.

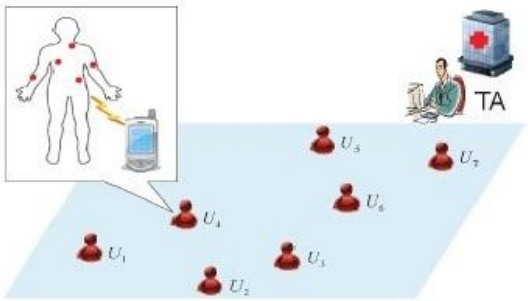


Figure 2: System model under consideration.

**2. Models and Design Goal:**

In this section, we formalize the system model and security model, and identify our design goal as well.

**A. System Model:**

In our system model, we consider a trusted authority (TA) and a group of l medical users U ¼ f U1; U2; . . . ; U9, as U shown in Fig. 2. 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 Ui 2 U is equipped with personal BSN and smart-U Phone, 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 [16], [17], [18], medical users U in our model are considered as mobile ones, i.e., walking outside [19]. BSN and Smartphone are two key

components for the success of m-Healthcare system. In order 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 In general, 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. However, since the Smartphone could be used for other purposes, e.g., phoning friends, surfing webpage's, when an emergency suddenly takes place, the residual power of smart-phone may be insufficient for high-intensive PHI process and transmission. To deal with this embarrassing situation, opportunistic computing provides a promising solution in m-Healthcare system, i.e., when other medical users find out one medical user Ui 2 U is in emergency, they will contribute their Smartphone's' resources to help Ui with processing and transmitting PHI.

**B. Security Model2.2 Security Model:**

Opportunistic computing 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 his PHI to all passing-by medical users. Instead, he may only disclose his PHI to those medical users who have some similar symptoms with him. In this case, the emergency situation can be handled by opportunistic computing with minimal privacy disclosure. Specifically, in our security model, we 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, as shown in Figure 3.

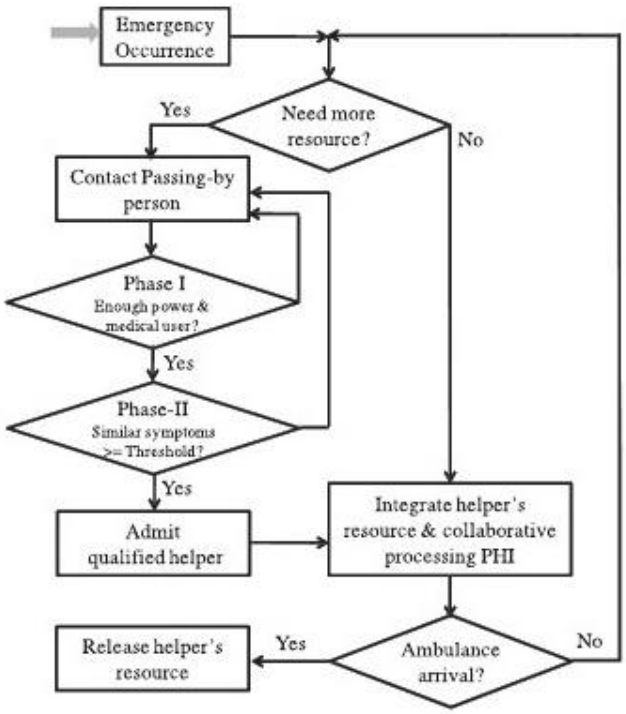


Figure 3: Opportunistic computing with two-phase privacy access control for m-Healthcare emergency.

Phase-I access control. Phase-I access control indicates that although a passing-by person has a smart phone with enough power, as a nonmedical user, he is not welcomed to participate in opportunistic computing. Since the opportunistic computing

requires smart phones that are installed with the same medical software to cooperatively process the PHI, if a passing-by person is not a medical user, the lack of necessary software's does not make him as an ideal helper. Therefore, the phase-I privacy access control is prerequisite. Phase-II access control. Phase-II 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. Note that, the threshold th is a user self-control parameter. When the emergency takes place at a location with high traffic, the threshold the will be set high to minimize the privacy disclosure. However, if the location has low traffic [21], [22], [23], [24], the threshold th should be low so that the high-reliable PHI process and transmission can be first guaranteed. Note that, a passing-by person can still assist in processing some physical cares before the ambulance arrives.

**C. Design Goal:**

Our design goal 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. Specifically, we 1) apply opportunistic computing in m-Healthcare emergency to achieve high reliability of PHI process and transmission; and 2) develop user-centric privacy access control to minimize the PHI privacy disclosure.

**3. Proposed SPOC Framework:**

In this section, we propose our SPOC framework, 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. Before describing them, we first review the bilinear pairing technique which serves as the basis of the proposed SPOC framework.

**A. Bilinear Pairings:**

Let G and $G_T$ be two multiplicative cyclic groups with the same prime order q. suppose G and $G_T$ are equipped with a pairing, i.e., a non degenerated and efficiently computable bilinear map.

Let $G_1, G_2$ be two additive cyclic groups of prime order $q$, and $G_T$ another cyclic group of order $q$ written multiplicatively. A pairing is a map: $e : G_1 \times G_2 \to G_T$, which satisfies the following properties:

1. Bilinearity: $\forall a, b \in F_q^*, \forall P \in G_1, Q \in G_2 : e(aP, bQ) = e(P, Q)^{ab}$
2. Non-degeneracy: $e(P, Q) \neq 1$
3. Computability: there exist an efficient algorithm to compute $e$.

**B. Description of SPOC:**

**System Initialization:**

For a single-authority m-Healthcare system under consideration, we assume a trusted authority located at the healthcare center will bootstrap the whole system. Trusted Authority TA has full access control over whole healthcare system. Each medical user's symptoms are represented through his PHP i.e. a binary vector a={a1,a2,….,an} The medical professionals make medical examination for user and generate PHP i.e. binary vector a. TA chooses body sensor nodes to establish personal BSN and installs specific medical software in users Smartphone. TA computed access control keys and master keys for particular users. User prepares session key for current date and for every 5 min BSN collects raw PHI data Raw PHI data is encrypted using session key and send to Smartphone through which it is transferred to TA.

**2) User-Centric Privacy Access Control for m-Healthcare Emergency:** When an emergency takes place in m-Healthcare, e.g., user U0 suddenly falls down outside, the healthcare center will monitor the emergency, and immediately dispatch an ambulance and medical personnel to the emergency location. Generally, the ambulance will arrive at the scene around 20 minutes [25]. During the 20 minutes, the medical personnel needs high-intensive PHI to real-time monitor U0. However, the power of U0's smart phone may be not sufficient to support the high-intensive PHI process and transmission. In this case, the opportunistic computing, as shown in Fig. 3, is launched, and the following user-centric privacy access control is performed to minimize the PHI privacy disclosure in opportunistic computing.

**4. Performance Evaluation:**

In this section, we evaluate the performance of the proposed SPOC framework using a custom simulator built in Java. 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. The performance metrics used in the evaluation are 1) the average number of qualified helpers, 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. Both NGH and RCR can be used to examine the effectiveness of the proposed SPOC framework with user-centric privacy access control of opportunistic computing in m-Healthcare emergency.

**A. Simulation Setup:**

In the simulations, total l users U ¼ f$U_0$; $U_1$; . . . ; $U_{l\ 1}$g are first uniformly deployed in an interest area of 500 m 500 m, as shown in Fig. 5a. Each user $U_i$ 2 U is equipped with his personal BSN and a Smartphone with a transmission radius of 20 m, and independently moves along the road with the velocity v 2 ½0:5; 1:2& m=s in the area by following the mobility model described in Fig. 5b. Assume that the symptom character space n ¼ 16, each user is randomly assigned 6-8 symptom characters. Let the emergency of user $U_0$ take place at time t ¼ 0, he sets the threshold th as f3; 5g, and waits the qualified helpers participating in the opportunistic computing before the ambulance arrives in 20 minutes. Note that, in the simulations, we consider all users will stop when they meet $U_0$'s emergency, and only the qualified helpers will participate in the opportunistic computing. To eliminate the influence of initial system state, a warm-up period of first 10 minutes is used. In addition, we consider $U_0$'s emergency takes place at three locations, A, B, and C, in the map to examine how the factors l, th affect the NGH and RCR at different locations. The detailed parameter settings are summarized in Table 1. In the following, we run the simulations with different parameter settings. For each setting, the simulation lasts for 20 minutes (excluding the warm-up time), and the average performance results over 10,000 runs are reported.

**B. Simulation Results:**

In Figure 6, we compare the average NQHs at locations A, B and C varying with time from 2 to 20 minutes under different user number l and threshold th. From the figure, we can see, with the increase of time, the average NQH will also increase, especially for the location A. The reason is that, when all users move in the simulation area by following the same mobility model, location A will have higher traffic than locations B and C.

**5. Related Works:**

Opportunistic computing: 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 [7], [8], [9], [10]. In [7], Avvenuti et al. introduce the opportunistic computing paradigm in wire-less 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 [8], Passarella et al. evaluate the performance of service execution in opportunistic computing. Specifically, they first abstract resources in pervasive computing as services that 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.

Privacy-preserving scalar product computation. Research on privacy-preserving scalar product computation has been conducted for privacy-preserving data mining [28], [12], [11], [29], and as well for secure friend discovery in mobile social networks quite recently [30], [31], [32]. Initially, PPSPC protocol was designed by involving a semi trusted party [28]. Later, to remove the semi trusted party, many PPSPC protocols without a third party were proposed [12], [11], [29], [13]. However, they are relying on time-consuming "homomorphic encryption" [14] and/or "add vector protocol," and are not quite efficient.[2] In our proposed SPOC framework, we present a new PPSPC protocol, which does not use any "homomorphic encryption," but is very efficient in terms of computational and communication costs, i.e., the computational cost only takes 2n multiplications (mul), and the communication cost is only ðn þ 1Þ 1024 þ 256 bits. Let $T_{mul}$ and $T_{exp}$ denote the time needed to execute a modulus multiplication and a modulus exponentiation, respectively. When we roughly estimate $T_{exp}$ $240T_{mul}$ [33], we use Fig. 8 to compare the computation and communication costs of the proposed PPSPC protocol and the popular Paillier Cryptosystem (PC)-based PPSPC protocol described in Fig. 9. From Fig. 8, we can obviously observe that our proposed PPSPC protocol is much efficient, especially in computation costs. To the best of our knowledge, our proposed PPSPC is the most efficient privacy-preserving scalar product computation protocol till now.

**6. Conclusions:**

In this paper, we have proposed 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 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.

**7. References:**

1. 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.
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.
6. 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.
7. 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.
8. 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.
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. W. Du and M. Atallah, "Privacy-Preserving Cooperative Statistical Analysis," Proc. 17th Ann. Computer Security Applications Conf. (ACSAC '01), pp. 102-111, 2001,
12. 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.
13. A. Amirbekyan and V. Estivill-Castro, "A New Efficient Privacy-Preserving Scalar Product Protocol," Proc. Sixth Aus-tralasian Conf. Data Mining and Analytics (AusDM '07), pp. 209-214, 2007.
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 for Ehealth Systems," IEEE J. Selected Areas in Comm., vol. 27, no. 4,
16. 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.

17. 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.
18. "Exercise and Walking is Great for the Alzheimer's and Dementia Patient's Physical and Emotional Health," http://free-alzheimers-support.com/wordpress/2010/06/exercise-and-walking/, June 2010.
19. R. Lu, X. Li, X. Liang, X. Shen, and X. Lin, "GRS: The Green, Reliability, and Security of Emerging Machine to Machine Communications," IEEE Comm. Magazine, vol. 49, no. 4, pp. 28-35, Apr. 2011.
20. D. Boneh and M.K. Franklin, "Identity-Based Encryption from the Weil Pairing," Proc. Ann. Int'l Conf. Cryptology Organized (CRYPTO '01), pp. 213-229, 2001.
21. 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.
22. R. Lu, X. Lin, H. Zhu, and X. Shen, "An Intelligent Secure and Privacy-Preserving Parking Scheme through Vehicular Communications," IEEE Trans. Vehicular Technology, vol. 59, no. 6, 2772-2785, July 2010.
23. R. Lu, X. Lin, H. Luan, X. Liang, and X. Shen, "Pseudonym Changing at Social Spots: An Effective Strategy for Location Privacy in Vanets," IEEE Trans. Vehicular Technology, vol. 61, 86-96, 2012.
24. http://www.uaproperty.com/articles/In-Ukraine-ambulance-come-patient-10-minute s.html, 2012.
25. S. Ross, Introduction to Probability Models, Ninth Ed., 2007.
26. X. Lin, R. Lu, X. Liang, and X. Shen, "STAP: A Social-Tier-Assisted Packet Forwarding Protocol for Achieving Receiver-Location Privacy Preservation in Vanets," Proc. of INFOCOM '11, 2147-2155, 2011
27. W. Du and Z. Zhan, "Building Decision Tree Classifier on Private Data," Proc. of CRPIT '14, ser. CRPIT '14, pp. 1-8, 2002.
28. Ioannidis, A. Grama, and M. Atallah, "A Secure Protocol for Computing Dot-Products in Clustered and Distributed Environ-ments," Proc. of ICPP '02, pp. 379-384, 2002.
29. W. Dong, V. Dave, L. Qiu, and Y. Zhang, "Secure Friend Discovery in Mobile Social Networks," Prof. of INFOCOM '11,
30. 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.
31. M. Li, N. Cao, S. Yu, and W. Lou, "Findu: Privacy-Preserving Personal Profile Matching in Mobile Social Networks," Proc. INFOCOM, pp. 2435-2443, 2011.
32. K.-H. Huang, Y.-F. Chung, C.-H. Liu, F. Lai, and T.-S. Chen, "Efficient Migration for Mobile Computing in Distributed Net-works," Computer Standards and Interfaces, vol. 31, no. 1, pp. 40-47, 2009.