International Journal of Technology and Engineering System (IJTES)
Vol 7. No.4 2015 Pp. 337-341
©gopalax Journals, Singapore
available at : www.ijcns.com
ISSN: 0976-1345

PRESERVING LOCATION PRIVACY OF MOBILE USERS IN SOCIAL APPLICATIONS

R.AMIRTHARATHNA
Master of Engineering, Department of Computer Science and Engineering
Krishnasamy College of Engineering & Technology, Cuddalore, India
amirtha800@gmail.com

ABSTRACT

Mobile social networks represent a promising Cyber-Physical System (CPS), which connects mobile nodes within a local physical proximity by using mobile smart phones as well as wireless communication. However, in mobile social networks, the mobile users may face the risk of leaking their personal information and their location privacy. This leads to location aware social networks such as Foursquare [1], Gowaila [2]. In this study, we first model the secure friend discovery process as a generalized privacy-preserving interest and profile matching problem. We identify a new security threat arising from existing secure friend discovery protocols, coined as runaway attack, which can introduce serious unfairness issue. To thwart this new threat, we introduce a novel blind vector transformation technique, which could hide the correlation between the original vector and the transformed results. Based on it, we propose our privacy-preserving and fairness-aware interest and profile matching protocol [4],[5], which allows one party to match its interest with the profile of another, without revealing its real interest and profile and vice versa. Further we introduce the LocX protocol which avoids leaking of the location information. The detailed security analysis as well as real-world implementations demonstrate the effectiveness and the efficiency of the proposed protocol.

Keywords- Privacy Preserving, Fairness Aware Friend Matching, Blind Transformation, LocX Protocol, Profile Interest

I. INTRODUCTION

Mobile social applications represent a promising Cyber-Physical System (CPS), which connects mobile nodes within a local physical proximity by using mobile smart phones as well as wireless communication. However, in mobile social networks, the mobile users may face the risk of leaking their personal information and their location privacy. In this study, we first model the secure friend discovery process as a generalized privacy-preserving interest and profile matching problem [4],[5]. We identify a new security threat arising from existing secure friend discovery protocols, coined as runaway attack [4], which can introduce serious unfairness issue. To that this new threat, we introduce a novel blind vector transformation technique, which could hide the correlation between the original vector and the transformed results. Based on it, we propose our privacy-preserving and fairness-aware interest and profile matching protocol, which allows one party to match its interest with the profile of another, without revealing its real interest and profile and vice versa. Further after the profiles are connected we avoid the leaking of location information by introducing a new protocol called the LocX protocol. The detailed security analysis as well as real-world implementations demonstrate the effectiveness and the efficiency of the proposed protocol. Our future work includes how to provide fine-grained interest/profile matching and investigate more security and privacy issues in mobile social networks. Enhance the usability of mobile social networks; we present a novel Privacy Preserving and Fairness aware Friend Matching Protocol. In the designed protocol, a successful matching only happens in case that the interests of both of the participants could match the profiles of the others. In other words, no one can learn any extra information from the protocol unless another participant is exactly what he is looking for and vice versa.

II. OBJECTIVE

In particular, in mobile social networks, the mobile users may face the risk of leaking of their personal information

and their location privacy. Under this circumstance, the attackers can directly associate the personal profiles with real persons nearby and then launch more advanced attacks. Existing researches show that loss of privacy can expose users to unwanted advertisement and spam/scams, cause social reputation or economic damage, and make them victims of blackmail or even physical violence [3].The objective is to ensure the fairness and privacy preserving interest and profile matching process in social applications and also to improve the location privacy of users.

III. MOBILE COMPUTING

Mobile computing is human-computer interaction by which a computer is expected to be transported during normal usage. Mobile computing involves mobile communication, mobile hardware and mobile software. Communication issues include ad-hoc and infrastructure networks as well as a communication properties, protocols, formats and concrete technologies. Hardware includes mobile devices or device components. Mobile software deals with the characteristics and requirement of mobile applications.

A. Benefits of Mobile Computing

- Improve business productivity by streamlining interaction and taking advantage of immediate access.
- Reduce business operations costs by increasing supply chain visibility, optimizing logistics and accelerating processes.
- Strengthens customer relationships by creating more opportunities to connect, providing information at their fingertips when they need it most.
- Gain competitive advantage by creating brand differentiation and expanding customer experiences.
- Increase work force effectiveness and capability by providing on-the-go process.
- Improve business cycle processes by redesigning work flow to utilize mobile device that interface with legacy applications.

B. Revising the technical architecture

Mobile users are the demanding. They are important to business world. To provide complete connectivity among users the current communication technology must revised to incorporate mobile connectivity. Additionally, application and data architectures must also revised to support the demands put upon them by the mobile connectivity.

C. Reliability, coverage, capacity and cost

At present wireless network is less reliable, have less geographic coverage and reduce bandwidth, are slower, and cost more than the wired-line network services. It is important to find ways to use this new resource more efficiently by designing innovative applications.

D. Integration with legacy mainframe and emerging client/server applications

Application development paradigms are changing. As a result of the IT industry's original focus on mainframes, a huge inventory of applications using communication interfaces that are basically incompatible with mobile connectivity have been accumulated. Still the application development trend is geared towards wired network platform and little thought has been given to applications necessary for mobile platform. This practice must change for successful integration of mobile connectivity.

E. End-to-end design and performance

Since mobile computing involves multiple network (including wired) and multiple application server platforms, and end-to-end technical compatibility, Server capacity design, and network response time estimates are difficult to achieve.

F. Security

Wireless networks have relatively more security requirements than wired network. A number of approaches have been suggested and also the use of encryption is has been proposed.

IV. EXISTING SYSTEM

The existing mobile social applications systems pay little heed to the security and privacy concerns associated with revealing one's personal social networking preferences and friendship information to the ubiquitous computing environment. In particular, in mobile social networks, the mobile users may face the risk of leaking of their personal information and their location privacy[3]. Under this circumstance, the attackers can directly associate the personal profiles with real persons nearby and then launch more advanced attacks. Existing researches show that loss of privacy can expose users to unwanted advertisement and spam's/scams, cause social reputation or economic damage, and make them victims of blackmail or even physical violence.

A. Disadvantages of Existing System

- The mobile users may face the risk of leaking of their personal information and their location privacy.
- The existing apps fail to consider hide of user's profiles.
- Introducing error into location data.

- Relying on trusted servers or intermediaries to apply anonymization to users and private data.

V. PROPOSED SYSTEM

The proposed system for *Private Profile Matching*, which allow two users to compare their personal profiles without revealing private information to each other [4]. The private profile matching problem [6],[7] could then be converted into Private Set Intersection [8],[9] or Private Set Intersection Cardinality[10],[11]. In particular, two mobile users, each of whom holds a private data set respectively, could jointly compute the intersection or the intersection cardinality of the two sets without leaking any additional information to either side. We introduce a novel blind vector transformation technique, which could hide the correlation between the original vector and the transformed result. Based on it, we propose the privacy-preserving and fairness-aware friend matching protocol, which enables one party to match its interest with the profile of another, and vice versa, without revealing their real interest. It also involves proposing LocX (short for location to index mapping), a approach to achieve privacy while maintaining accuracy in location-based social applications.

A. Advantages Of Proposed System

- Privacy Guarantee
- Fairness Assurance
- secure multi-party computation (SMC) techniques
- User's location is preserved

VI. PAPER DESCRIPTION

In this paper, we first model the privacy-preserving interest and profile matching problem. We identify a new threat arising from existing secure friend discovery protocols, coined as runaway attack, which can introduce serious unfairness issue. We introduce a novel blind vector transformation technique, which could hide the correlation between the original vector and the transformed results. Based on it, we propose our privacy-preserving and fairness-aware interest and profile matching protocol [6],[7], which allows one party to match its interest with the profile of another, without revealing its real interest and profile and vice versa. Also the LocX protocol that does the process of location to index mapping. It allows performing transformations on the location coordinates before storing on untrusted servers. The detailed security analysis as well as real-world implementation demonstrate the effectiveness and the efficiency of the proposed protocol and also uses RC4 Algorithm as an encryption technique.

VII. SYSTEM ARCHITECTURE

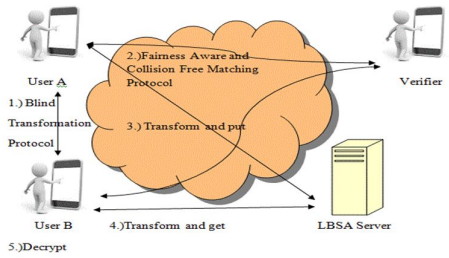

Fig.1 System Architecture

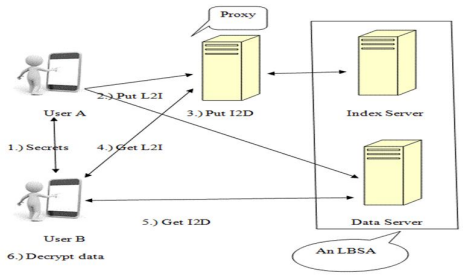

Fig.2 LocX Protocol implementation

A. Privacy Preserving

Mobile online social networks have gained tremendous momentum in the recent years due to both the wide proliferation of mobile devices such as smart phones and tablets as well as the ubiquitous availability of network services. We present a novel Privacy Preserving and Fairness aware Friend Matching Protocol. In the designed protocol, a successful matching only happens in case that the interests of both of the participants could match the profiles of the others. In other words, no one can learn any extra information from the protocol unless another participant is exactly what he is looking for.

B. Secure Friend Discovery in Mobile Social applications

The profile matching directly considers Alice has her personal profile, which includes three attributes: age, girl and movie. She is interested in finding a boy with similar age and hobbies. Conversely, Bob also has his own profile and interests. A successful matching could be achieved in case that Alice's profile matches Bob's interest while, at the same time, Bob's profile matches Alice's interest. Such a mapping process could be well supported by the existing online dating social networks, in which a member may seek another member satisfying some particular requirements [12] (e.g., gender, age ranges or even living location)Further, the existing proposals are one-way only and profile matching requires running a protocol twice [6], [7], with reversed roles in the second run.

C. Fairness Aware Friend Matching Protocol

For the first time, we separate the user's interest from its profile, which is expected to be a generalization of traditional profile matching problem. We introduce a novel blind vector transformation technique [13], which could hide the correlation between the original vector and the transformed result. Based on it, we propose the privacy-preserving and fairness-aware friend matching protocol, which enables one party to match its interest with the profile of another, and vice versa, without revealing their real interest. We introduce a novel lightweight verifier checking approach to thwart runaway attack and thus achieve the fairness of two participants. We implement our protocols in real experiments. We demonstrate the performance of the proposed scheme via extensive experiment results.

D. Blind Transformation Protocol

In the blind transformation phase, each participant will encrypt his profile by using his public key and provide it to his partner for blind transformation. The basic idea of blind vector transformation protocol[13] is allowing two untrusted parties to transform two vectors into the blind ones by following a series of private and identical steps, e.g., adding a random vector, shuffling in the same order. Since the transformation follows the same step, the matching results (e.g. the number of matched interest and profiles) keep unchanged before and after the transformation, which enable the untrusted participants compare the profile without leaking their real interest or profile information.

E. LocX Protocol

First, in LocX we split the mapping between the location and its data into two pairs: a mapping from the transformed location to an encrypted index (called L2I) and a mapping from the index to the encrypted location data (called I2D).The splitting helps in making our system efficient. Second, users store and retrieve L2Is via untrusted policies. This redirection of data via proxies along with splitting improves privacy in LocX. Thus for efficiency the L2Ds are not proxied yet privacy is preserved. It involves the following activities:

- Proxying L2Is for location privacy
- Storing L2I on the index server
- Storing I2Ds on the data server

F. Generating Encryption Key

By using the RC4 algorithm the key is generated for viewing the user complete profile.

VIII. Future Enhancement

In this paper, the privacy of privacy preserving interest and profile matching process can be done. In our future work these can be improved by applying some of the more efficient strategy or technique. This can be also applied to some of the real time application like YouTube. In this algorithms like RC5 algorithm can be applied. This will reduce the chance of hacking the information or revealing the information to unauthorized user.

IX. Conclusion

Users in online social applications such as Gowaila face the problem of risk of leaking the personal information and their location. This causes the loss of security and privacy. To overcome this problem, several tasks could be done such as Fairness aware, privacy of privacy preserving interest, profile matching process, energy efficient virtual energy based dynamic keying and also by LocX mechanism the location data of the users are preserved. Profile matching process is done based upon the user having same interest. And in addition RC4 algorithm is done for key generation. By using this algorithm the users who know the generated key can able to access or view the information. This will ensure the privacy and security.

References

[1] *"Foursquare,"* 2012. [Online]. Available: https://foursquare.com/.

[2] *"Gowaila,"* 2012. [Online]. Available: http://gowaila.com/.

[3] R. Shokri, G. Theodorakopoulos, C. Troncoso, J.-P. Hubaux and J.-Y. Le Boudec. *''Protecting location privacy: Optimal strategy against localization attacks.''* in Proc. of *ACM CCS'12*, pp.617-627, 2012.

[4] M. Li, N. Cao, S. Yu, and W. Lou, *"FindU: Privacy-preserving personal profile matching in mobile social networks,"* in Proc. Of *IEEE INFOCOM'11*, Shanghai, China, April 2011.

[5] Lili Qiu, Wei Dong, Vacha Dave, and Yin Zhang, *"Secure Friend Discovery in Mobile Social Networks."* In Proc. of *IEEE INFOCOM' 11*, Shanghai, China, April 2011.

[6] 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, pp. 1-12*, 2010.

[7] M. Von Arb, M. Bader, M. Kuhn, and R. Wattenhofer, *"Veneta: Serverless friend-of-friend detection in mobile social networking,"* in Proc. of *IEEE WIMOB'08, pp. 184-189*, 2008.

[8] L. Kissner and D. Song, *"Privacy-preserving set operations," in Advances in Cryptology'', CRYPTO 2005*. Springer, *pp. 241-257*, 2005.

[9] Q.Ye, H. Wang, and J. Pieprzyk, *"Distributed private matching and set operations," Information Security Practice and Experience, pp. 347-360*, 2008.

[10] M. Freedman, K. Nissim, and B. Pinkas, *"Efficient private matching and set intersection,"* in Advances in

Cryptology, *EUROCRYPT 2004*, Springer, *pp. 1-19*, 2004.
[11] E. D. Cristofaro and G. Tsudik, *"Practical private set intersection protocols with linear computational and bandwidth complexity,"* 2010.
[12] *"Perfect match,"* 2012. [Online]. Available: http://www.perfectmatch.com/
[13] R. Rivest, *"Unconditionally secure commitment and oblivious transfer schemes using private channels and a trusted initialize,"* Unpublished manuscript, 1999.