Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 5, May 2014, pg.617 – 622

RESEARCH ARTICLE

Secure Profile Matching and Privacy Preserving In Mobile Social Network

Ms. Deepa Kale[1], Prof. Rushi Longadge[2]

Department of CSE, G.H.Raisoni Academy of Engineering and Technology, Nagpur University, Maharashtra, India

Department of CSE, G.H.Raisoni Academy of Engineering and Technology, Nagpur University, Maharashtra, India

deeparkale@gmail.com [1], rushilongadge@gmail.com [2]

Abstract: As the increasing use of mobile devices, mobile social networks (MSNs) are becoming an inseparable part of peoples' lives. In existing systems for such services, usually all the users directly publish their complete profiles for others to search. However in this paper we create a profile matching application which helps user to find the people whose profile best matches with others people. In this paper we propose the security protocol which helps from profiling, and we have tried to increase the privacy so that less information about the user profile is revealed.

Keywords: Profile Matching; Secure communication; Private Set Intersection; Private cardinality of set Intersection; decentralized mobile social network

---

I. INTRODUCTION

Social networking is the grouping of individuals into specific groups, like small rural communities or a neighborhood subdivision. Although social networking is possible in person, especially in the workplace, universities, etc, it is most popular online. This is because the internet is filled with millions of individuals who are looking to meet other people, to gather and share first-hand information and experiences. When it comes to online social networking, websites are commonly used. Once you are granted access to a social networking website you can begin to socialize. This socialization may include reading the profile pages of other members and possibly even contacting them. As mentioned social networking involves grouping specific individual and organization together. While there are number of websites focus on particular interests which means any one can become member, no matter what their hobbies or interest are, once you are inside the community you can make friends of common interest and can eliminate those friends.

What is mobile social network? **Mobile social networking** is social networking where individuals with similar interests converse and connect with one another through their mobile phone and/or tablet. Much like web-based social networking, a current trend for social networking websites is to create mobile apps to give their users instant and real-time access from their device mobile and web-based social networking systems often work symbiotically to spread content, increase accessibility and connect users from wherever they are. While using MSN good level of security measures have also taken into consideration. Face-to-face interaction plays an irreplaceable role in our daily lives, especially for social networking purposes the initiator and its best matching user directly and privately find out and connect to each other, without knowing anything about other users' profile attributes, Making new connections according to personal preferences to matching users profile is the crucial task, while

the rest of the users should also learn nothing about the two user's matching attributes. However in several applications, the users' personal profiles may contain sensitive information that they do not want to make public. In this paper, we propose a set of privacy-preserving profile matching schemes in MSN .We have defined several privacy levels for secure profile matching. However, it is challenging to find out the matching users privately while efficiently. Recently, Yang *et. al*. proposed E-Small Talker [4]which suffers from the dictionary attack which does not fully protect the non-match attributes between two users. We propose privacy-preserving profile matching schemes, known as private set intersection (PSI) protocol solutions based on existing PSI schemes are efficient.

II. LITERATURE SURVEY

A. Shamir Secret Sharing based on SMC

Share of secret *s* under Shamir secret sharing (SS) scheme, [1] shares secret *s* among *w* parties by giving each party *Pi* the value $[s]_i^{t,w}$, and if any at most *t* parties collude they cannot gain any information about *s*. Thus their protocol realizes randomization and degree-reduction in one round by letting each *Pi* pick a random *t*-degree polynomial and re-share $[\alpha]_i^{t,w}$ $[\beta]_i^{t,w}$ to others.

Round 1. Each party *Pi* shares the value $[\alpha]_i^{t,w}$ $[\beta]_i^{t,w}$ by choosing a *t*-degree random polynomial $hi(x)$, s. t. $hi(0) = [\alpha]_i^{t,w}$ $[\beta]_i^{t,w}$. He sends the value $hi(j)$ to party *Pj* , $1 \leq j \leq w$.

Round 2: Every party *Pj* computes his share of $\alpha\beta$, i.e., the value $H(j) = [\alpha\beta]t,w\ j$ under a *t*-degree random polynomial *H*, by locally computing the linear combination $H(j) = \Sigma^{w}_{i=1}\ \lambda i hi(j)$, where $\lambda 1, \ldots, \lambda w$ are known constants.

An additive homomorphic encryption scheme *E* allows one to compute $E(m1+\ m2)$ given $E(m1)$ and $E(m2)$, without knowing the plain texts. This is used in our protocol for PL-2.

B. Remainder Vector and Hint Matrix:

The author Lan Zhang, Xiang-Yang [2] proposes this mechanism where search is not *flexible* The initiator cannot query any subset of other's profile. A perfect matching is required and *no fuzzy* search is supported. All participants decrypt the message. A *hint matrix* is constructed to support a flexible fuzzy search. It describes the linear constrain relationship among the optional attributes to help calculating unknown attributes from known attributes. The hint matrix helps a matching user exceeding the similarity threshold to recover the required profile vector.

C. Location Attribute and Its Privacy Protection:

In localization enabled mobile social networks, a user usually searches matching users in vicinity. In the existing systems, a user is required to provide his/her own current location information and desired search range. The distance bound to define vicinity, if two users are within each other's vicinity, the intersection of their vicinity regions will have a proportion no less than a threshold. Compared to static attributes like identity information, location is usually a temporal privacy [2].

D. Privacy Preserving Profile Matching Protocols:

In [2] Protocol 1, an unmatched relay user doesn't know anything about the request. The matching user knows the intersection of required profile and his/her own profile in the HBC model. A matching user can decide whether to reply the request according to the profile intersection. The initiator doesn't know anything about any participant until he/she gets a reply.To prevent malicious participants, we design Protocol 2, which is similar to Protocol 1, but it excludes the confirmation information from the encrypted message.

To prevent the dictionary profiling by malicious initiator, we improve Protocol 2 to Protocol 3 which provides a user personal defined privacy protection.

E. Secure Dot Product Protocol:

In this paper Wei Dong, Vacha Dave, ili Qiu, Yin Zhang [6] proposes Authentication and verification which is essential to guard against malicious users who falsify the social coordinates, both parties to obtain the dot product, both Alice and Bob run two separate instances of protocol in parallel. Then, a naive verification approach for Bob may be to first decrypt the result sent by Alice using his private key and encrypt it using Alice's public key and compare it with w that he computed before for consistency. In protocol 0 Alice and bob start exchanging their encrypted vectors EH+A(v, r1) and EH+B(u, r2). Alice computes EH+B(v◦u, r2◦v) and EH+B(r1◦u, r1◦r2) And send them to Bob after self-blinding. Bob computes and sends back for self-blinding. Alice decrypts and gets two numbers as result1 and result 2. Alice computes and compares the vectors; if they are consistent the dot product result is correct.

F. PRF and Oblivious PRF:

In this paper Stainslaw Jarecki and Xiaomin Liu [5] Proposes Pseudorandom function (PRF) is an efficiently computable keyed function $f_k(.)$ whose values are indistinguishable, for a randomly chosen key k, the oblivious PRF is a protocol that allows the sender S on input key k, to let the receiver R compute the value $f_k(x)$ of a PRF $f_k(.)$ on any input x of R's choice without releasing any other information to R and do so obliviously in the sense that sender S learns nothing from the protocol similarly as in oblivious transfer or oblivious polynomial evaluation.

III. PROPOSED ALGORITHM

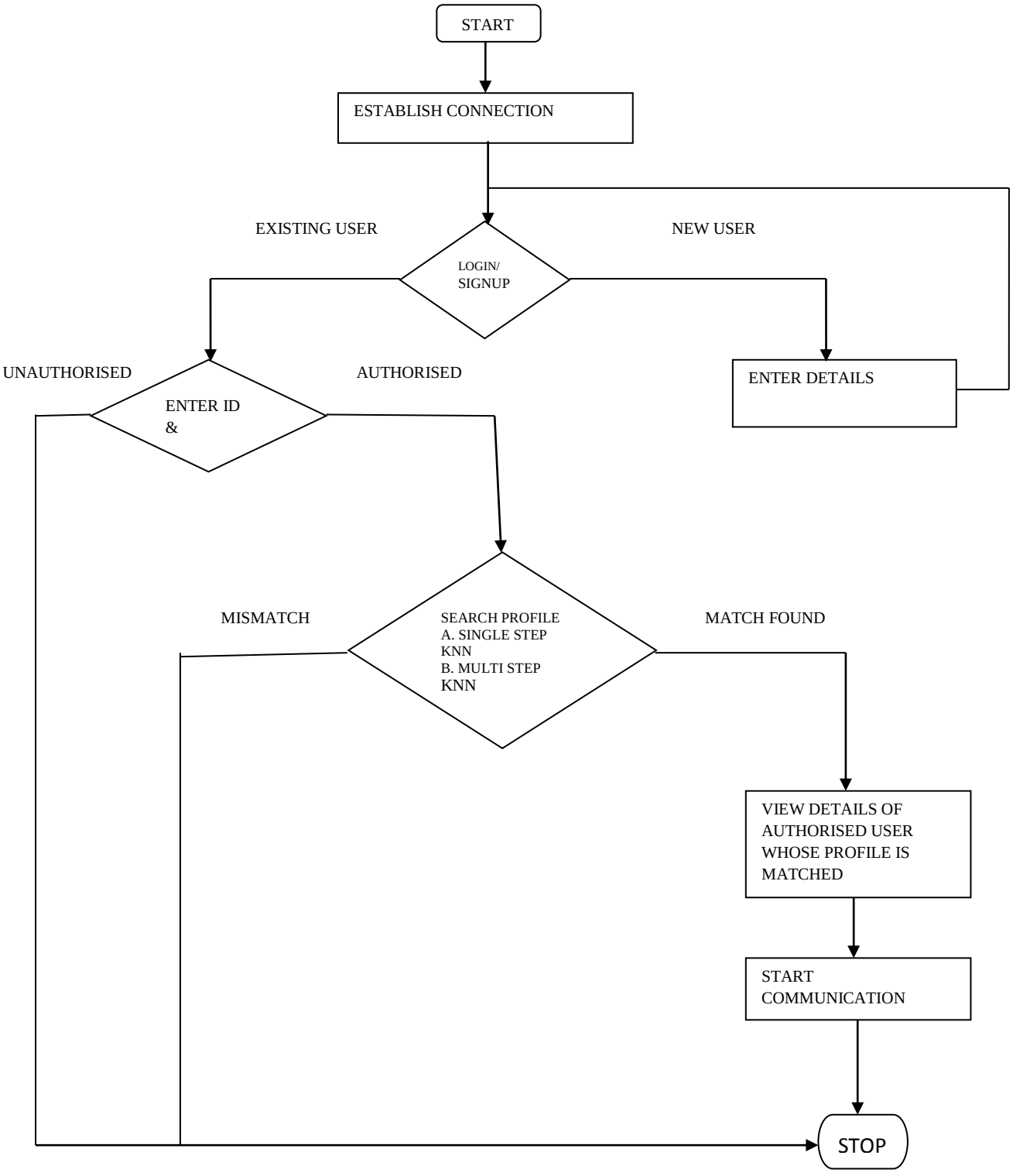

Figure 1. Search Profile Algorithm

A. Algorithm

Step 1: Start
Step 2: Establish Connection
Step 3: Login if existing user or signup for new user
Step 4: Search Profile
  a. Single Step KNN
  b. Multi Step KNN
Step 5: If Profiles are matched view details of authorized user whose profile is matched
Step 6: Start Communication
Step 7: Stop

B. Single Step KNN

1. For Profile Matching we use single step KNN.
2. The number of attributes search is less.
3. The attributes are encrypted using homomorphic encryption E (m1+m2).

C. Multi step KNN

1. In this algorithm multiple or more attributes are searched.
2. The searched data is in encrypted form which provides security from attacks.
3. The encrypted data is decrypted and profile is matched.

IV. RESULT ANALYSIS

Experiment 1: Analysis of execution time observed by user
In the below fig 2 execution time of the protocol is shown on x-axis number of attributes that each user has and on y-axis execution time on less number of attributes.

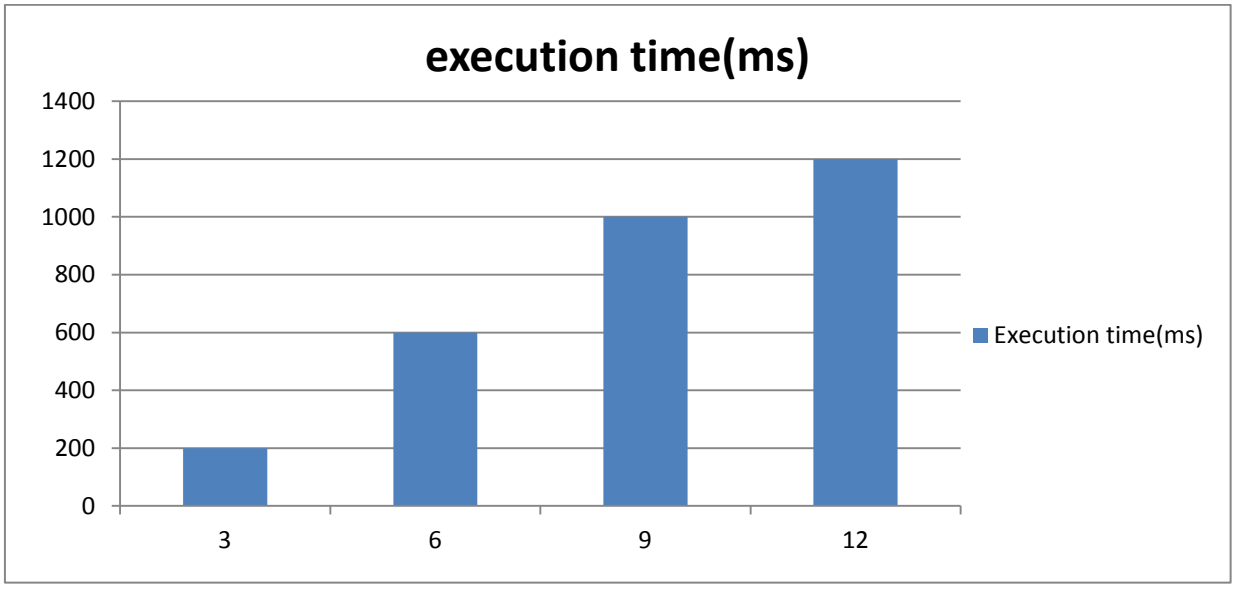

Figure 2: Execution time for single step KNN

Experiment 2: Analysis of execution time observed by user
In the below fig 3 execution time of the protocol is shown on x-axis number of attributes that each user has and on y-axis execution time for more number of attributes.

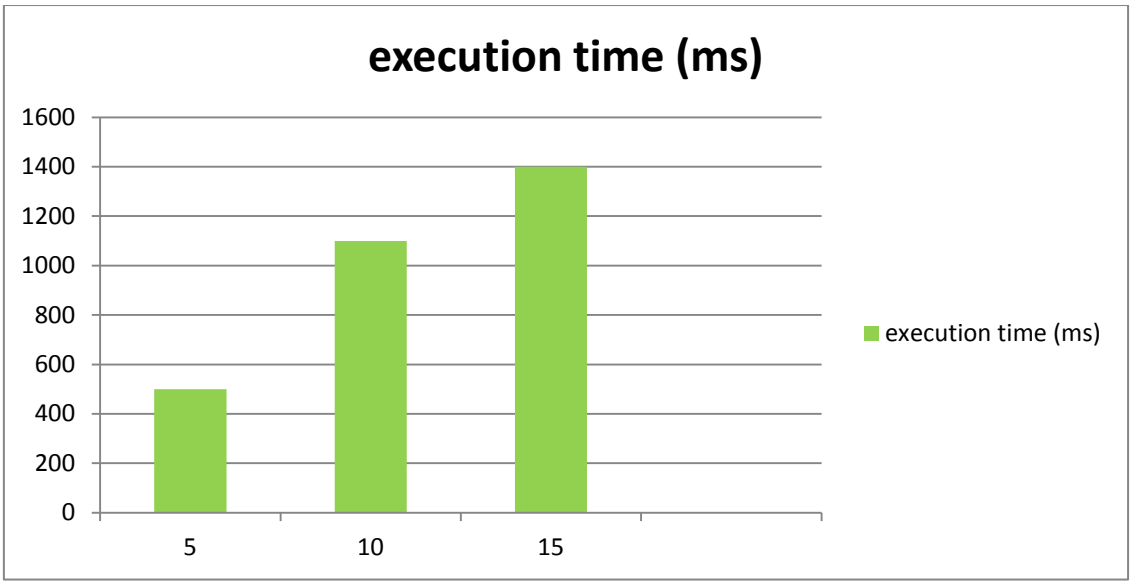

Figure 3: Execution time for multi step KNN

V. CONCLUSION

We presented a security protocol that preserves user's interest information from unnecessary leaks in mobile social networking application .our implementation and evaluation of the protocol show that the protocol is practical for smart phones. This approach is efficient in computation and communication and the security measures we have implemented are useful in preventing attacks. In our scheme the numbers of users is less, and number of query attributes is smaller than the profile attributes.

ACKNOWLEDGEMENT

Ms. Deepa R Kale, received the B. E. degree in Computer Science and Engineering from G.H Raisoni Institute Engineering Technology for women's, Nagpur, India, in 2012. She is currently pursuing M.Tech in Computer Science & Engineering from G. H. Raisoni Academy of Engineering and Technology, Nagpur. Her research interests include Mobile computing & wireless technology. deeparkale@gmail.com

Mr. Rushi Longadge, received the Bachelor of Engineering degree in Information Technology from North Maharashtra University, Jalgon, India, in 2010 and Master of technology in Computer Science & Engineering from G.H. Raisoni College of Engineering, Nagpur. Mr. Rushi Longadge, currently working as Asst. Professor in Department of Computer Science & Engineering, G. H. Raisoni Academy of Engineering and Technology, Nagpur. His Research areas are Data Mining, Machine Learning and Image Processing. rushilongadge@gmail.com

REFERENCES

[1] Ming Li, Shucheng Yu, "Privacy-Preserving Distributed Profile Matching in Proximity-based Mobile Social Networks"in IEEE 2013 VOL:12 NO:5.

[2] " Lan Zhang, Xiang-Yang li, Yunhao Liu "Message in a sealed Bottle:Privacy preserving Friending in Social Networks" in IEEE conference 2013 1063/6927.

[3] Qi Xie and Urs Hengartner ,"Privacy Preserving Matchmaking for mobile social networking secure against Malicious users" international conference 2011 978-1-4577-0584-7/11.

[4] Z. Yang, B. Zhang, J. Dai, A. Champion, D. Xuan, and D. Li, "Esmalltalker: A distributed mobile system for social networking in physical proximity," in *IEEE ICDCS '10*, June. 2010.

[5] S. Jarecki and X. Liu, "Efficient oblivious pseudorandom function with applications to adaptive ot and secure computation of set intersection," in *TCC '09*. Berlin, Heidelberg: Springer-Verlag, 2009, pp. 577–594

[6] Wei Dong, Vacha Dave , ili Qiu ,Yin Zhang "Secure Friend Discovery in Mobile Social Networks" in infocom 2011.

[7] Y. Qi and M. J. Atallah ,"Efficient privacy-preserving k-nearest neighbor search," in *IEEE ICDCS '08*, 2008, pp. 311–319.

[8] L. Kissner and D. Song, "Privacy-preserving set operations," in *CRYPTO '05, LNCS*. Springer, 2005, pp. 241–257.

[9] R. Lu, X. Lin, X. Liang, and X. Shen, "A secure handshake scheme with symptoms-matching for mhealthcare social network," *Mobile Networks and Applications*, pp. 1–12, 2010.

[10] R. Balani, "Energy consumption analysis for Bluetooth, wifi and cellular networks," in *Technical report*, Dec. 2007, pp 1-6.

[11] C. Hazay and Y. Lindell, "Efficient protocols for set intersection and pattern matching with security against malicious and covert adversaries," in *TCC'08*, 2008, pp. 155–175.

[12] R. Cramer, I. Damgard, and J. Nielsen, "Secure multiparty computation," *Book draft*, 2010.

[13] R. Baden, A. Bender, N. Spring, B. Bhattacharjee, and D. Starin. Persona: An online social network with user-defined privacy. In *Proc. of ACM SIGCOMM*, Aug. 2009.

[14] R. Gennaro, M. O. Rabin, and T. Rabin, "Simplified vss and fast-track multiparty computations with applications to threshold cryptography," in *ACM PODC '98*, 1998, pp. 101–111.

