ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

A Survey on Online Friend Matching Protocol

T.B. Shinde[1], P. D. Mohite[1], J. V. Divekar[1], M. A. More[1], Prof.R.V.Chatse[2]

B. E Student, Dept. of Information Technology, SVPM COE, Malegaon Bk., Baramati, Maharashtra, India[1]

Assistant Professor, Dept. of Information Technology, SVPM COE, Malegaon Bk.Baramati, Maharashtra, India[2]

ABSTRACT: Mobile social networking (MSN) constitute an assuring Global Positioning System. Connecting remote host within a local physical distance by the wireless use or mobile phone communication. Anyhow in MSN, smart phone users may face the possibility of releasing their personal details and locality information. Here in the study, we diagnose a new security risk originating from private friend discovery protocols, devised runaway attack, that could introduce extreme unfairness problem. to prevent this problem, We proposed a unique Blind Vector Transformation techniques(BT),which can conceal relation between the existing vector and transformed output. On this basis, we introduce our privacy preserving and fairness aware interest and profile matching protocol, which allow one user to match its interest with the other user without exposing its real interest and profile. The precise security evaluation in addition to real world executions exhibit the adequacy and the productivity of the proposed protocol.

KEYWORDS: Epreserving privacy, Discovery of Friend, Mobile portable Networks.

I. INTRODUCTION

Now In the last decade, the multiple users of online networking sites and mobile phone services has increase rapidly. The popular online social networking site, Facebook, has more than 500 million active users, and more than 50% of its active users log on to Facebook at least once per day. In terms of smart phone services, there were 4.1 billion mobile cellular subscribers in total in March 2009 with the propagation of mobile devices, MSNs are becoming devoted part of our life's. Exploiting networked mobile devices such as smart phones and personal digital assistant (PDA) as platforms, MSN not only enables to use their existing (OSNs) at everywhere, but also introduces infinite numbers of mobility-oriented applications, such as location-based services and augmented reality. Among them, an important service is to make new social connections/friends within local physical distance based on the matching of personal profiles. For example, MagnetU is a MSN application that matches one with nearby people for dating or friend-making based on common interests. In such an paper, a user only needs to input some (query) attributes in her profile, and the system would automatically find the persons around with similar profiles. The scopes of these applications are very broad, since people can input anything as they want, such as hobbies, phone contacts and places they have been to. The latter can even be used to find "lost connections" and "familiar strangers".

Privacy preservation is a significant research issue in social networking. The social net-working platforms are extended into the mobile environment, users require more extensive privacy-preservation because they are unfamiliar with the neighbours in close vicinity who may store, and correlate their personal information at different time periods and locations. Once the personal information is correlated to the location information, the behaviour of users will be completely disclosed to the public

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

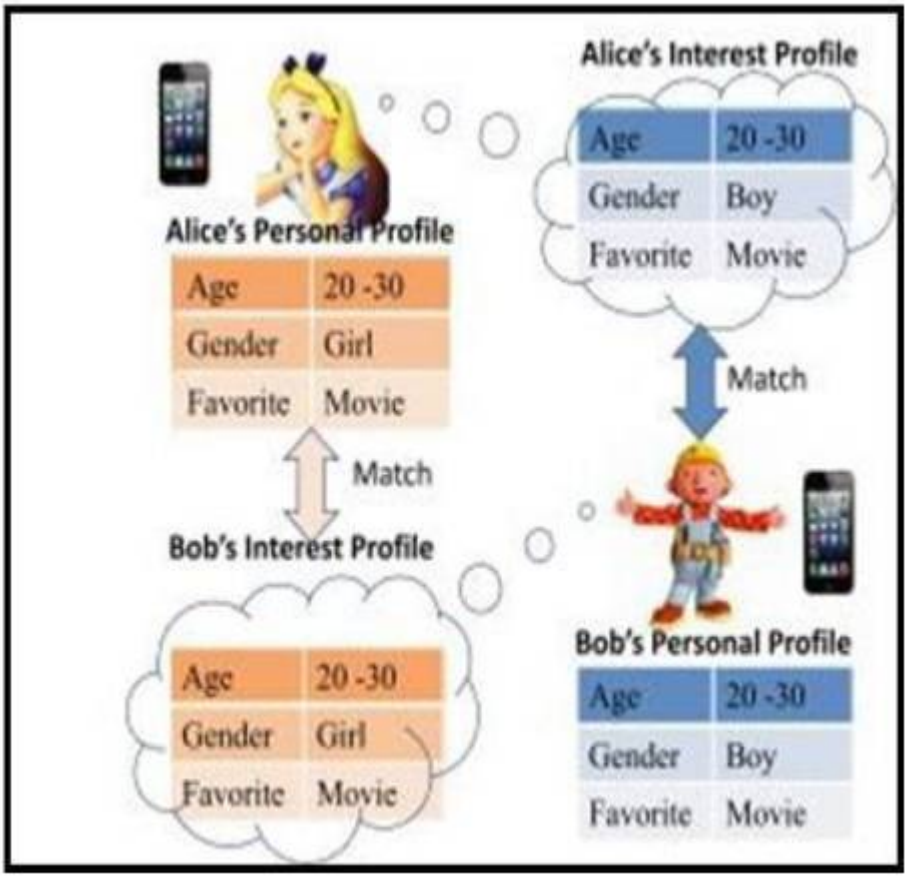

Fig:1.Friend Discovery in Social Network

The content-sharing applications, all of which provide no feedback or control mechanisms to users and may cause inappropriate location and identity information disclosure. Alice has her own profile and Bob has her own. Alice is interested in finding a boy with similar profile and bob is also interested in finding a girl with same profile. 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. The existing model support this type of mapping process. Further, the existing systems are one-way only and profile matching requires running a protocol twice, with reversed roles in the second run. A malicious attacker or disgraced user launch the runaway attack to exploit this two-pass protocol. This runaway attack in-curs a serious unfairness issue. The new system for Secure Profile Matching, which allow multiple users to compare their profiles without leaking private information to each other.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

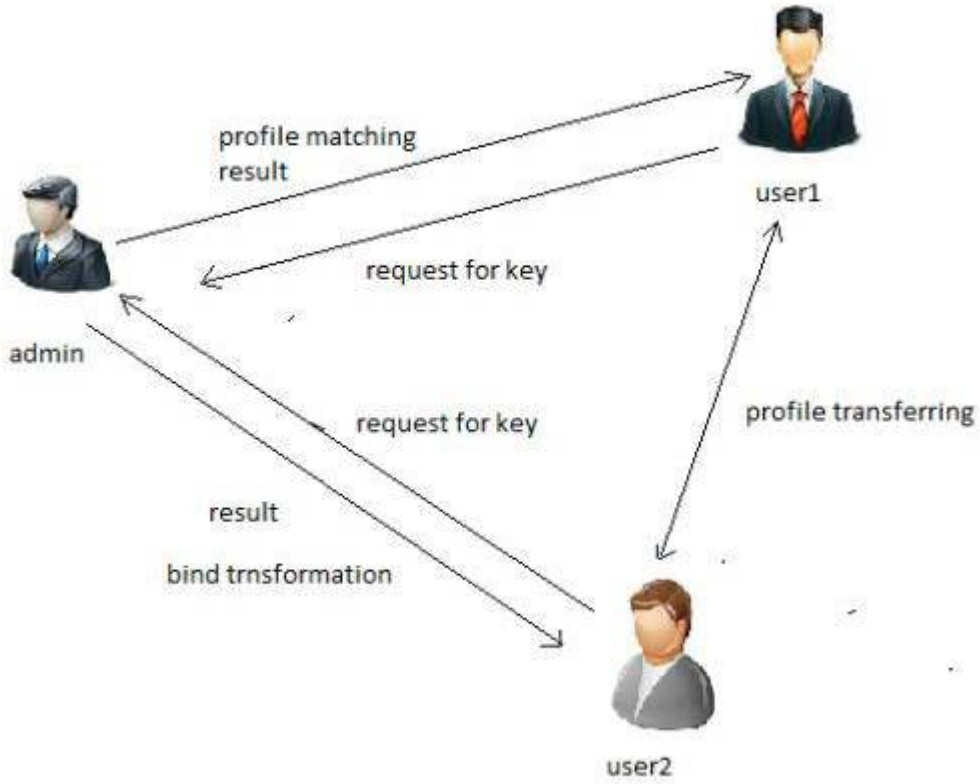

Fig2: System architecture

The secure profile matching problem could then be converted into Private Set Intersection or Private Set Intersection Cardinality. To gain this aim, a novel Blind Vector Transformation Techniques introduce, which could hide the relation between the initial vector and the transformed result. Based on it, the privacy-preserving and fairness-aware friend matching protocol is proposed, which enables one party to match its interest with the profile of another, and vice versa, without revealing their real interest. By the help of Blind Vector Transformation Technique, the interest as well as profile private during match its interests with another's pro-file is kept. To prevent runaway attack, a lightweight verifier checking technique is enable that verify the matching at the minimized overhead and prevent from launching the runaway attack.

II. RELATED WORK

In this part we will present the details of our protocol.

2.1.Protocol Overview

There are two proposed protocols:

1.Blind Vector Transformation

2.Fairness aware and Collusion-free matching protocol

We define five primitive operation as follows:

Encrypt: Given vector performs paillier encryptions with public key pk to getciphertext .This operation denoted by Encrypt

Vec_add:Given two vectors p and q both are encrypted by paillier encryption, The vec_add operation will be excuted to perform add operation

Vec_ext: Given vector ,the operation vec_ext could change real value of by diffusion operation. Append some dummy vector to to obtain p||q

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

Vec_shuffle: Given vector ,the operation vec_shuffle) could change the real value of by performing confusion operation which shuffle the elements in vector .
Vec_rev: Given vector ,the operation Vec_rev could change the real value of by changing value of k element in vector P

Algorithm1:The Blind Transformation Algorithm

Input: P1 □ U1's profile encrypted under his public key pk1, I2 □ interest, n □ the number of interest U2 considers in I2 and s □ a security parameter .

Output:P22□ The Blind-transform profile vector for U1 , I22 □ the transform interest vector for U2 and rb□ the actual matching result for U2.

Function:
Blind-Transformation(P1, pk1, I2, n, s)
r□random vector of length n1 = ||P1||
r1 □Encrypt (r, pk1)
P1' □VecAdd (P1, r1)
I '□VecAdd (I2, r)
y□random vector of length s
y1 □Encrypt (y, pk1)
P11□VecExt (P1', y1)
Rn□random number between [1,s]
yi□VecRev (y, Rn)
I21 □VecExt (Ii, yi)
I22 □VecShuffle(I21)
P22 □VecShuffle(P11)
rb□ n + s - Rn
return P22, I22, rb
end function

2.2 The Proposed Blind Transformation Protocol:

The basic idea of Blind Vector Transformation protocol is allowing two untrustedparties to transform two vectors in the blind one by following series of private and identical steps, eg. Adding random vector, shuffling in same order, VecExt and VecRev.Blind Add: U2 generates random vector r and then perform r1=Encrypt(r,pk1) after the,U2 calculate P1' ecAdd P1,r1) and I2' ecAdd I2,r) by adding r1 and r to P1 and I2 ,respectively.Blind Append: U2 generates random vectory of length s, where s is predeterminedsecurity parameter, then perform y1= Encrypt (y, pk1) to get P11= VecExt(P1', y1).Blind Reverse: U2 randomly selects Rn .{1,2…..s} and perform yi =VecRev (y, Rn) then obtain I21 =VecExt (Ii, yi).Blind Shuffle:U2 performsI22=VecShuffle(I21) and P22 =VecShuffle(P11) with thesame order.2.3 The proposed Fairness-aware and Collusion free Matching Protocol:

In this proposed protocol, instead of directlysending h1, h2 (number of matched entries)to the verifier, an additional blind linear transformation is used To check if two parties'interests match their equivalent profiles, wehave the following verification protocol.First-ly, U1 obtains P'1 Decrypt(P22, sk1) byperforming the decryption operation with hisown secret key sk1. After obtaining P'1, U1compares it with U2's blinded interests I2 toget the number of matched entries s'2 whileU2 could get s'1 similarly. To verify if theirinterests and the profiles match or not,U1sends h1=H(s'1 ||s'2) whereas U2 sends h2=H(s'1||s') to a randomly chosen verifier.The verifier could verify whether h1||h2. Ifh1|| h2, the match succeeds, otherwise, it fails.

III. CONCLUSION

Equalize In this work, we have develop a proposed protocol that will ensure the fairness aware andprivacy preserving profile matching processand also provide more security in socialnetwork.

REFERENCES

1. Z. Yang, B. Zhang, J. Dai, A. C. Champion, D. Xuan, andD. Li,``ESmallTalker: A distributed mobile system for socialnetworking in physical proximity," in Proc. IEEE ICDCS,Jun. 2010, pp. 468_477.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

2. M. Li, N. Cao, S. Yu, and W. Lou, ``FindU: Privacypreserving personal profile matching in mobile socialnetworks," in Proc. IEEE INFOCOM, Shanghai, China, Apr.2011, pp. 2435_2443.
3. W. Dong, V. Dave, L. Qiu, and Y. Zhang, ``Secure frienddiscovery in mobile social networks," in Proc. IEEEINFOCOM, Shanghai, China, Apr. 2011, pp. 1647_1655.
4. R. Shokri, G. Theodorakopoulos, C. Troncoso, J.-P.Hubaux, and J.-Y. Le Boudec, ``Protecting location privacy:Optimal strategy against localization attacks," in Proc. ACMConf. CCS, 2012, pp. 617_627.
5. PaillierHomomorphic Cryptosystem (JavaImplementation) [Online]. Available:http://www.csee.umbc.edu/kunliu1/research/ Paillier.htmlHubaux, and J.-Y. Le Boudec, ``Protecting location privacy:Optimal strategy against localization attacks," in Proc. ACM
6. Conf. CCS, 2012, pp. 617_627.
7. PaillierHomomorphic Cryptosystem (JavaImplementation) [Online]. Available:http://www.csee.umbc.edu/kunliu1/research/ Paillier.html
8. [6] R. Lu, X. Lin, X. Liang, and X. Shen, ``A securehandshake scheme with symptoms-matching for mhealthcaresocial network," Mobile Netw. Appl., vol. 16, no. 6, pp.683_694, 2010.
9. P. Paillier, ``Public-key cryptosystems based on compositeDegree residuosity classes," in Advances in Cryptology_EUROCRYPT 1999,pp. 223_238.
10. M. Von Arb, M. Bader, M. Kuhn,andR.Wattenhofer,`VENETA:Server-less friend-of-friend detection in mobilesocial networking," in Proc. IEEE WIMOB, Oct. 2008, pp. 184_189.
11. L. Kissner and D. Song, ``Privacy-preserving setoperations," in Advance in Cryptology_CRYPTO 2005, pp.241_257.
12. Q. Ye, H. Wang, and J. Pieprzyk, ``Distributed privatematching and set operations," in Proc. Information SecurityPractice and Experience(ISPEC) Conf., 2008, pp. 347_360.
13. M. Freedman, K. Nissim, and B. Pinkas, ``Efficient privateMatching and set intersection," in Advances inCryptology_EUROCRYPT 2004 pp. 1_19
14. E. D. Cristofaro and G. Tsudik, ``Practical private setintersection protocols with linear computational and bandwidthcomplexity," in Financial Cryptography and Data Security.Berlin, Germany: Springer-Verlag, 2010, pp. 143_159.
15. Perfect-Match [Online]. Available:http://www.perfectmatch.comBhagyashree Deokar, AmbarishHazarnis, " Intrusion Detection System using log files and reinforcement learning", International Journal of Computer Applications (0975 – 8887) ,May 2012
16. Karen Scarfone& Peter Mell, National Institute of Standards and Technology (NIST) Special Publication 800-94 , " Guide to Intrusion Detection and Prevention Systems", Feb 2007.
17. Karen Kent, Tim Grance,Hung Dang, NIST Special Publication 800- 86 , "Guide to Integrating Forensic Techniques into Incident Response" , Aug 2006.

BIOGRAPHY

Miss. T.B. Shinde is Student at Information Technology Department, SVPM COE, Malegaon Bk.,BaramatiMaharashtra

Miss. P. D. Mohite is Student at Information Technology Department, SVPM COE, Malegaon Bk., Baramati Maharashtra

Miss. J. V. Divekaris Student at Information Technology Department, SVPM COE, Malegaon Bk., Baramati, Maharashtra

Miss. M. A. More. Is Student at Information Technology Department, SVPM COE, Malegaon Bk., Baramati, Maharashtra

Prof.R.V.Chatse is Assistant Professor, Information Technology Department, SVPM COE, Malegaon Bk. Baramati , Maharashtra