Survey of Privacy Preserving Friend Matching Protocol for Pre-match in Social Networks

Shubhangi S.Ople,
M.E Student, Dept.Of Computer Engineering
STES's, Smt. Kashibai Navale College of Engineering
Vadgaon, Pune-411041, India

Aaradhana A.Deshmukh,
Asso. Professor, Dept.Of Computer Engineering
STES's, Smt. Kashibai Navale College of Engineering
Vadgaon, Pune-411041, India

ABSTRACT

Most popular handheld device is confusing or it become complicated for research activity into new protocol and applications. It can be handling and tackle new characteristics and environment for particular application in mobile social network. New purpose of mobility is defining characteristics of mobility or mobile system in mobile social interaction. Aim of this paper is to find out the bugs or threats. Threats to maintain privacy for matching two user profiles based on profile attributes. It refers comparing and matching two user profiles. If there is a conflict between two profiles matching then privacy concerns about disclosing their personal profile for strangers. This survey is about matching protocols that enable two users to perform profile matching without disclosing any information about their profile.

General Terms

Security, Algorithm, Customer Relationship Management, Interaction, Friend Discovery, Encryption, Decryption.

Keywords

Privacy Preserving; Friend Discovery; CRM;

1. INTRODUCTION

'Friend Discovery' it describes the Customer Relationship Management (CRM) database in an organization with social networks. All friend discovery services are connected to the Customer Relationship Management (CRM) [1][5]. Today Facebook is the most popular exposing in people's social graph of social networking site. Here, when profile is added each other account when mutually two entities share something in common. Friend Discovery Applications are built into organizational websites and with ways of exposing themselves through our various social networks and through third party websites. 'Friend Discovery' is the interaction because it helps user to find friends who also care about a particular organization and its product and service [2]. When we are developing an application according to "Friend Discovery" have consider these steps.

1.1 Do Not Share Any Default Settings-

To reduce the probability of mistakes by user is to make do not share the deserting for all information about customer's interactions with company [7].

1.2 Trust Some Selective Friends More Than Strangers-

When I am sharing some information or updates on Facebook or tweet on Tweeter then in case I don't want to share with all my friend, I just want this information will share with some of my friends. The principle states that customers needs to be able to control which friends in their social graph get access to which type of information[3].

1.3 My Relationship Data Is My Relationship Own Data-

It is created to database information about the organizations relationship with its customer and other stakeholders are belongs in the organization's CRM database. Friends Discovery needs to be able to temporarily combine that data without compromising any condition in it[8].

1.4 Friend Discovery Follows Different Formats-

Popularity used mobile social applications are Facebook, Twitter, Google, Linkedin and so many. And other to chat only are Gtalk, Whatsapp, Wechat, Hike and many more [3][6]. Communication is mainly done between client and server. Then different point mechanism is used for client-server communication. Client-Server, Centralized, Decentralized, Distributed, Multi-Tier these architectures are use to client server communication. Friend Discovery concept not only created to find a friend, exchange profile, select, add and chat. It is used in various areas like social networking sites, call centre for help like healthcare center. Opening an secure email id, company to do large no of transactions.

2. PROBLEM STATEMENT

Explore To propose the private authenticity to user by using Blind Transformation Protocol Algorithm to protect the personal information .In particular, in mobile social network; 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 spams or scams, cause social reputation or economic damage, and make them victims of blackmail or even physical violence.[10]

3. RELATED WORK

The existing mobile social network 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. 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 spams or scams, cause social reputation or economic damage and make them victims of blackmail or even physical violence.

3.1 Find U – Privacy Preserving for Profile Matching In Mobile Social Network-

Here, Friend Discovery are having various boundaries and issues. Proximity based user discovery and key establishment are two important issues for the usability of our profile matching protocols, towards designing light weight protocols [1].

3.2 SPOC-A Secure and Privacy Preserving For Mobile Healthcare Emergency-

Mobile Healthcare still faces many challenges including information security and privacy preservation. A secure and privacy preserving opportunistic computing framework called SPOC, for Mobile Healthcare emergency [2].

Table 1 . Survey for Friend Discovery

Survey	Year	Topic Focused	Protocol Used	Advantage	Disadvantage
Ming Li [1]	Apr 2011	Find U- Privacy Preserving Profile matching in MSN	Light Weight protocol	1)Secure under HBC model 2)Easily extended prevent attack 3)Short range control interfaces	1)Usability of profile matching 2)Privacy preserving manage in MSN
Rongzing Lu [2]	March 2013	SPOC: Mobile Healthcare Emergency	Vector Protocol For Third Party	1)Centralized healthcare system distributed 2)Reduce healthcare expenses	1) Performance to find the track 2)Reliability 3)Privacy 4)Security, Related To mobile health care services.
Haojin Zhu [3]	Oct 2009	SMART: Secure multilayer credit based Delay Tolerance Network	Public key Certificate based protocol	1)Effectiveness, Efficiency, Security, Generality 2)education in Transmission cost	1) Traffic and keep trade of each other. 2) Expensive computing cost.
Haojin Zhu [4]	Oct 2008	SLAB: Secure Localization ,authentication and billing scheme for wireless n/w	Third Way Handshake Protocol	1)High mobility security solution low-cost device 2)Highly desired	Difficult to work when Network size is large
Rui Zhang [5]	Sept 2013	Privacy Preserving Profile Matching For Proximity Based MSN	Fine Grained Private Matching Protocol	Facilitate one communication leading Allows employees to discuss ideas. To maintain consider business contacts Improve business on short client advertisement	1) Possibility for hackers to commit fraud and launch spam and virus attack. 2) Result in lost productivity. 3)Identify theft
Haojin Zhu [5]	Aug 2013	Fairness-aware the privacy preserving friend matching protocol	Friend Matching Protocol/ Novel Protocol	1)Privacy guarantee 2)Fairness assurance 3) Secure multi-party computation (SML) techniques.	1) Mobile user may face the risk of leaking of their personal information and their location privacy. 2) Existing applications fail to consider hide of users profile.

3.3 A Secure Multilayer for Delay Tolerant Network –

It shows wide range of applications for end-to-end network connectivity is not available. End-to-End connection is in between source to destination [3].It provide low cost internet service e.g. It's basically used as to open email id and send data form source to destination address.

3.4 SLAB- Secure Localization, Authentication and Building Scheme for Wireless Network-

This secure localized authentication and building (SLAB) scheme is provide the service for address both security guarantee and performance in terms of system compromise receiving capability, workload of the receiving broker (RB).This friend discovery SLAB scheme is for service oriented metropolitan area WMN's [4].

3.5 Privacy Preserving Profile Matching For Proximity Based Mobile Social Networks-

Privacy preserving profile matching for proximity based mobile social network is used fine grained private matching protocol used a wide range of matching metrics at different privacy levels[5]. In this case, private matching in which two users, compare personal profiles without disclosing them to each other. It supports a variety of private matching metrics at different privacy levels [5].

3.6 Fairness Aware Privacy Preserving Friend Matching Protocol-

This is used to improve the navigation effectiveness of website while minimizing two current structures. Transformation and personalization approaches are integrated. In this for two profiles matching fine grained protocol is used [6].In cloud computing the application works on two networks i.e. social network and the mobile network. Survey behind friend discovery is for privacy preserving for different area like mobile, computing, healthcare, education, entertainment. But, main intension behind that is secure communication.

4. PROPOSED SYSTEM

The benefit with the existing Mobile Social Network can get easy access if that person is authorized person. Also the paper suggests that privacy preserving is very sensitive to whether a person is login with their secured ID. So Friend Matching technology is unique in the sense that every person has its unique identity on mobile social networking application. It is different even in the case of identical Twins ID. So to benefit of the technology with the combination of authentication will be very beneficial as well as secure.

Here in above Figure1 Profile A and B created two profiles i.e. Personal Profile having fields Name, Date Of Birth (DOB) and Address and Interest Profile Having fields Hobbies, Movies, Books. Configure Module performing work to match two profile fields to add/ delete each other request. Here module contains IF and NIF both interest profile. For comparing, adding and deleting module uses Blind transformation Protocol. Group module creates two lists Group list and rejected list. Here whatever the operation performed by software controlled by file sharing, it control access for each other [9].

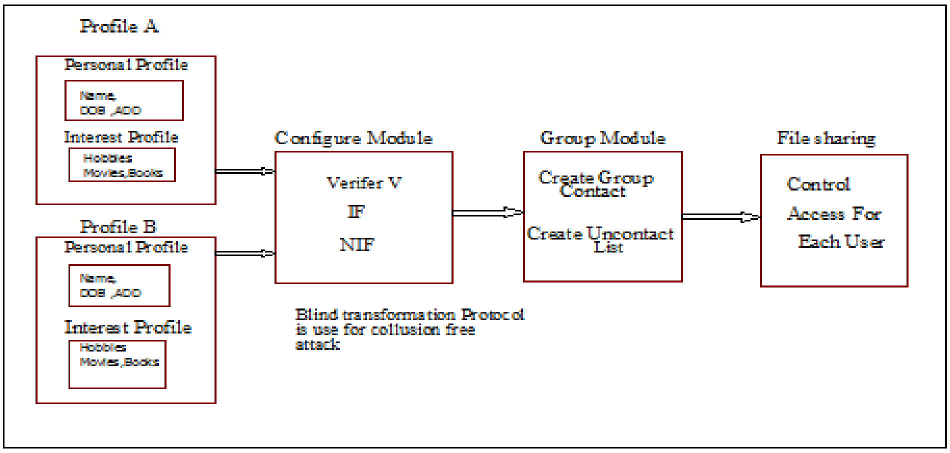


Figure1: System Model for Friend Discovery

Here Blind transformation algorithm is worked throughout the process.

4.1 Blind Transformation Algorithm

1. Separate users profile and interest profile.
2. Encrypted each users profile with his or her public key by using paillier cryptosystem.
3. Vector addition, shuffling, and extensions operations done for profile blind data.
4. Compare each user's encrypted profile for matching profile.
5. Add the interest profile with more matching fields.

Mathematical Expression for Proposed Work is defined as below-

The proposed protocols based on the Paillier Homomorphic Encryption. To understand the protocol Paillier Cryptosystem will help.

Key Generation:

The entity's Paillier public and private keys are $< N, g >$ and λ, where <N,g> are public parameters, λ is to calculate multiple of prime integer. Here mainly two encryption and decryption steps are used to encrypt and decrypt data.

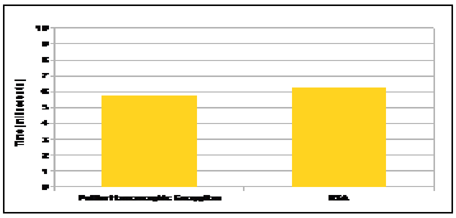
Where g is public parameter, c is cipher text, d is derived parameters, r is string, n is no. of massages.

Encryption: The cipher text could be given by, E (m mod N, r mod N) = gm rn mod N2 ……………………………………………..(1)
E is for encryption
D (E (m1) gm2 mod n2= m…………….. (2)
These equations defining the set of all content which we combine through the message. Cryptosystem is considered, Homomorphic added elements m=m1, m2. Here, we are using Paillier Homomorphic property for key generation method. It works on plaintext and the ciphertext. It supports to hash function to access large and different form of data [11].

5. CONCLUSIONS

Our work to develop the system that will ensure the fairness and the privacy preserving interest and profile matching process in mobile social networks .Future work include how to provide fine grained interest profile matching and investigate more security and privacy issues in mobile social networks. Here conclusion shown in graphical format according to the time and security needed for particular input to the model. Here, x-axis contains Paillier Homomorphic Encrypted input and the RSA elements. And y-axis contains Time and Security factors calculating in Graph 1 and Graph 2 respectively.

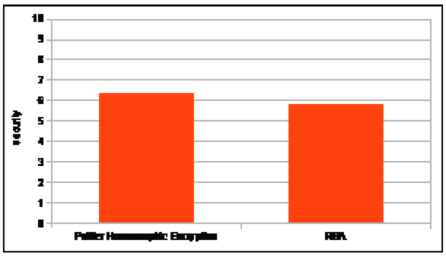
1. Key Generation Time Graph



Graph1. Key Generation Time Graph

Graph1.shows the result how the profile searching particular match through the Paillier homomorphic encryption model and the RSA (Randomly security Access) points for Ciphertext and the Plaintext. It generates results verses time i.e. in milliseconds that counts how many matches are generating for the combination .And the next graph is for providing security to the paillier homomorphic encryption. Time measured in milliseconds for given input.RSA supports to the Ciphertext and Plain text here. It follows the Rivert Shamir Algorithm in the graph for key generation method. Graph 2. Even followed these x-axis operations.

2. Security Graph



Graph 2.Security Graph

Graph2. Shows the result in case of security parameters are used in paillier homomorphic encryption. To developed a novel protocol that will ensure the fairness and the privacy of privacy-preserving network. The profile matching process in mobile social networks provides you security in case of leaking personal information. Our future work includes how to provide fine-grained interest profile matching and investigate more security and privacy issues in mobile social networks. Paillier homomorphic technique helps to access different forms of data and access easily in short time..Large amount of data we can access through this technique.

6. ACKNOWLEDGMENT

This work is performing under the Savitribai Phule Pune University Post Graduation project survey work.

7. REFERENCES

[1] M.Li, N.Cao, S.Yu, and W. Lou, “FindU – Privacy-Preserving Personal Profile Matching In Mobile Social Networks,” .Apr.-2011

[2] Rongzing Lu, SPOC- A Secure and Privacy Preserving Opportunistic Computing Framework for Mobile Healthcare Emergency March-2013

[3] H. Zhu, X. Lin, R. Lu. Fan, and X. Shen, “SMART: A Secure Multilayer credit based Delay Tolerance Network Oct- 2009

[4] H Zhu. X. Lin,R. Lu, P-H. Ho, and X. Shen, “SLAB: Secure Localized authentication and Billing Scheme for wireless mesh networks,” Oct-2008

[5] R. Zhang, J. Zhang, Y. Zhang, J. Sun, and G. Yan, ``Privacy-preserving profile matching for proximity-based mobile social networking," *IEEE* Sep. 2013.

[6] Haojin zhu, Mianxiong Dong, kao Ota,”Fairness – aware Privacy preserving Friend Matching Protocol In MSN”, Sep-2013

[7] LanZhang, Xiang-Yang Li, Yunhao Liu,”Message in a Sealed Bottle:Privacy Preserving Friending in Social Networks” Mar- 2012

[8] Ji Sun Shin, Virgil D. Gligor,”A New Privacy-Enhanced Matchmaking Protocol”. June-2008

[9] Boyang Wang, Baochun Li and Hui Li, ”Gmatch: Secure and Privacy-Preserving Group Matching in Social Networks”. Sept-2009

[10] Qiang Tang,”User-Friendly Matching Protocol for Online Social Networks”. Mar -2011

[11] P.Paiillier, “Public-Key cryptosystem based on composite degree residuosity classes,” - in advance cryptosystem-1999