Compatible and Confidentiality-Preserving Friend Matching in Mobile Cloud

Sowmya H S, Kavitha M, RuhiKhanum, Punitha C C, Asha Rani M*

Department of CSE, GSSSIETW, Mysuru, Karnataka, India

DOI: https://doi.org/10.21467/proceedings.1.21

* Corresponding author email: asharanim@gsss.edu.in

Abstract

The social networks such as Facebook, Line or Wechat recommend the friends for the users based on user's personal data such as common contact list or mobility traces. However, outsourcing users' personal information to the cloud for friend matching will raise a serious privacy concern due to the potential risk of data abusing. In this study, we propose a novel Scalable and Privacy-preserving Friend Matching protocol, or SPFM in short, which aims to provide a scalable friend matching and recommendation solutions without revealing the user's personal data to the cloud. Different from the previous works which involves multiple rounds of protocols, SPFM presents a scalable solution which can prevent honest-but-curious mobile cloud from obtaining the original data and support the friend matching of multiple users simultaneously. We give detailed feasibility and security analysis on SPFM and its accuracy and security have been well demonstrated via extensive simulations. The result show that our scheme works even better when original data is large.

Index Terms- Friend matching, Privacy preserving, Cloud security, XOR

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.

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]. When I am sharing some

© 2018 Copyright held by the author(s). Published by AIJR Publisher in Proceedings of the 3rd National Conference on Image Processing, Computing, Communication, Networking and Data Analytics (NCICCNDA 2018), April 28, 2018.
This is an open access article under Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0) license, which permits any non-commercial use, distribution, adaptation, and reproduction in any medium, as long as the original work is properly cited. ISBN: 978-81-936820-0-5

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 need to be able to control which friends in their social graph get access to which type of information [3]. 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].

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 clientserver communication. Client-Server, Centralized, Decentralized, Distributed, Multi-Tier these architectures are used 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 a secure email id, company to do large no of transactions.

2 LITERATURE SURVEY

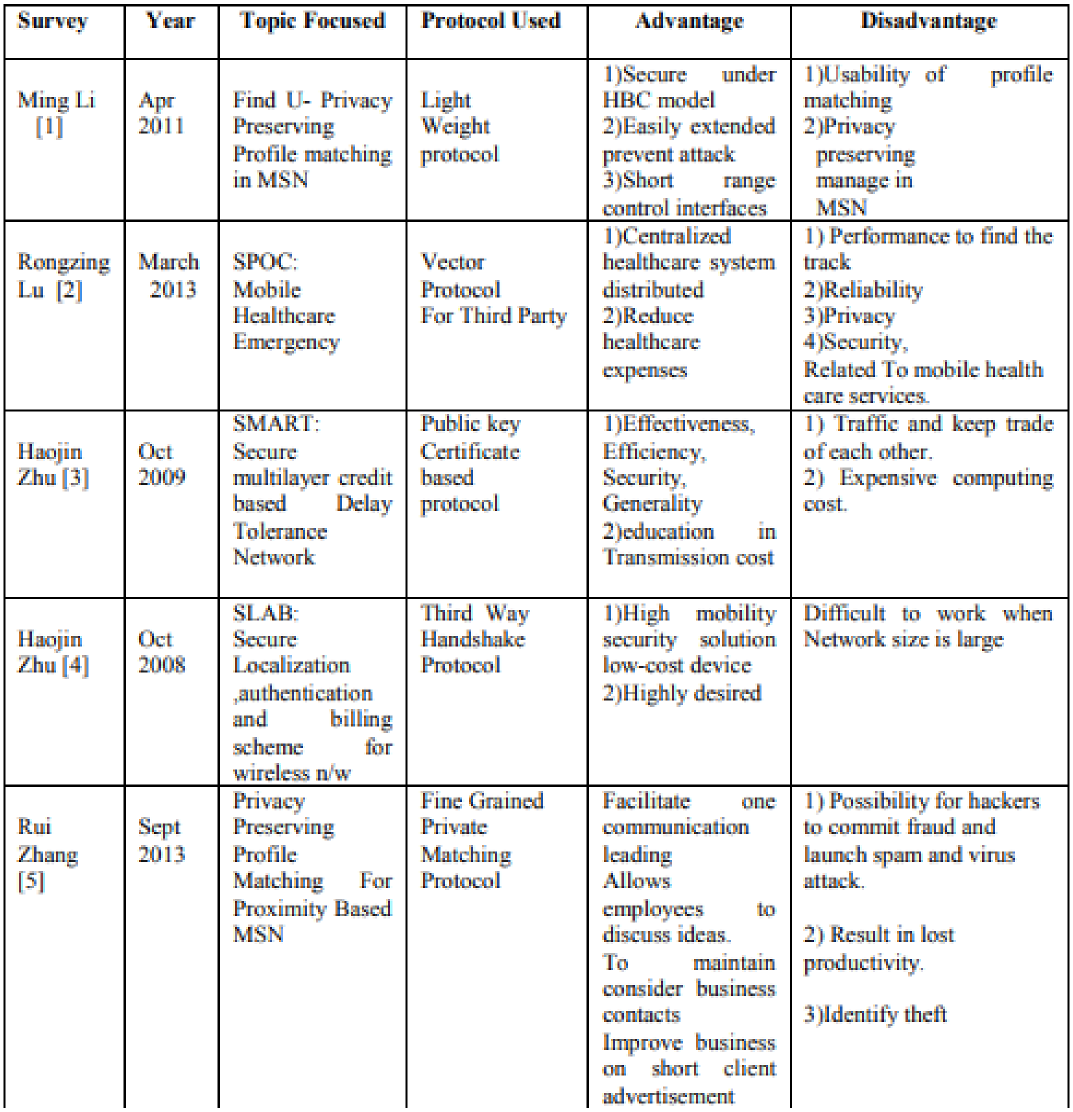
The existing mobile social network systems pay little heed to the security and privacy concerns associated with revealing one's personal social networking preferences and friendship information to the ubiquitous computing environment. In particular, in mobile social networks, the mobile users may face 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.

2.1 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].

2.2 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].



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

2.3 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.

2.4 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].

2.5 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 SYSTEM ARCHITECTURE

Nowadays, it is observed that many mobile social networks (e.g., Facebook, Wechat, Line) have provided the functionality of friend recommendation, which recommends the new friends to a user based on his contact list, education, mobility and other factors. To achieve this service, the various social networks need to collect the personal data of the users. Take Facebook's "People You May Know" as an example. It is stated by Facebook that it shows the potential friends "based on mutual friends, work and education information, networks you're part of, contacts you've imported and many other factors". For some of user personal data such as contact lists, it relies on apps installed on smart phones to collect the data and upload the data to the cloud. The cloud can determine if two users are friends by checking their common attributes such as the same school, common friends or similar mobility patterns. However, the sensitive data uploaded to the cloud may face the risk of leaking users' sensitive data and compromising users' privacy. In this work, we consider a privacy preserving friend matching scenario, in which the users' data will be obfuscated before uploading to the cloud. Thus, in the friend matching process, the server has no idea of the original sensitive data but it can still perform the friend matching and recommendation service.

4 PROPOSED SYSTEM

- In the first step, the system needs to set up masking generation probability pk. pk is a value greater than 0.5, and pk will determine the masking degree. The more pk is close to 0.5, the greater the degree of disturbance and the privacy-protect ability of the whole system is. However, this will reduce the data matching accuracy as well. In practical applications, the system will determine a pk by different needs of security and privacy. The masking generation probability is a common knowledge for the cloud and all users.
- The second step is performed on each user's device. In this step, each user will use masking generation probability pk to deal with private data needed to be uploaded. For each original sequence, a masking sequence of a same length is needed to obfuscate the original sequence. In a binary case, for each bit of a masking sequence, it has probability pk to be a 0,1 − pk to be a 1.
- In the third step, we first introduce two definitions Threshold and Matching Ambiguity in this step to adjust the matching accuracy, we use the threshold nth to

describe matching criteria, and the matching ambiguity Kth to be the ratio of the threshold and the original data's length.

When a user requests for matching, the server will use the obfuscated sequence and Data Tag to match. Now suppose that the server tries to find out whether two users are real friends in reality. The key is to find out how many common friends they have in contacts. The server first does a traversal through two users' Data Tags and fine all of the same Data Tags. For one of these same Data Tag, do XOR operation of their obfuscated sequences. If the number of 0 in the XOR results is more than nth, then server considers that the original data of these two obfuscated sequences are the same. In the application scenario of this paper, server will consider the telephone number stored in two users under this Data Tag are the same. In other words, the Data Tag represents a common friend of these two users. After a thorough traversal of all the Data Tags, server will get the number of common friends between these two users, which can be further used as a judge basis whether the two users are real friends in reality.

5 CONCLUSIONS

We tackle the problem of conflicting phenomenon that arise from variety of mobile cloud storage nowadays. The problem stems from the conflict about exciting functions cloud providing and the potential security issues in cloud. Honest-but-curious server, cloud account loss or cloud attack all may lead to exposure of users' private data, which will be an irreversible disaster. Thus, we develop SPFM to achieve high accuracy matching while not expose accurate private data to cloud. We provide thorough feasibility and security proof and demonstrate the feasibility and security by analyzing experiment performance.

6 References

[1] M.Li, N.Cao, S.Yu, and W. Lou, "FindU – PrivacyPreserving 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 proximitybased 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 PrivacyEnhanced 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.