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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 3, March 2019

Efficient Private Matching and Privacy-Preserving in Mobile Cloud

G.Vijayalakshmi[1], S.Akhilendra Nath[2], Bimalkumar [3]

M.Tech Student, Dept. of CSE, Shirdi Sai Institute of Technology, Affiliated to JNTUA, Andhra Pradesh, India [1]

Assistant Professor, Dept. of CSE, Shirdi Sai Institute of Technology, Affiliated to JNTUA, Andhra Pradesh, India[2]

Associate Professor, Dept. of CSE, Shirdi Sai Institute of Technology, Affiliated to JNTUA, Andhra Pradesh, India[3]

ABSTRACT: The growth of Internet services and popularity of social networking sites has actively increased over the past few years. The existing mobile social network systems pay little heed to the privacy concerns associated with friend matching and recommendation based on users' personal information. In this study, a novel Scalable and Privacy-preserving Friend Matching protocol, or SPFM is proposed, which aims to provide a scalable friend matching and recommendation solutions without revealing the user's data to the cloud. The approach is 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.

KEYWORDS: Friend matching, Privacy preserving, Cloud security, XOR.

I.INTRODUCTION

Mobile social networks extend social networks in the cyberspace into the real world by allowing mobile users to discover and interact with existing and potential friends who happen to be in their physical vicinity. Despite their promise to enable many exciting applications, serious security and privacy concerns have hindered wide adoption of these networks. The average daily time spent on social networking has also expanded in the past few years, as has the influence interactions on social networks might have on anything from one's politics to musical tastes, leisure or purchase reviews, feelings and emotional sharing. Users employ OSNs as a tool to connect with family, friends, colleagues, associates, or people with the same interests for different purposes such as professional networking, advertising their brands and businesses, job searches, making profit, or entertainment. Some networks, such as Facebook, started out as web-based and then extended towards access through mobile browsers and smart phone apps, while other networks, such as Instagram, were initially mobile -only and later extended into cross-platform availability as well with the help of web apps. An increasing number of social networks are therefore accessible through multiple platforms in order to offer users access to different features according to their needs, time and preferred device. Along with the popularity of the smart phone and ubiquitous wireless access, mobile clouds are becoming an inseparable part of our life. People use different clouds provided by different applications to store their private data such as contacts, mail address lists or bank accounts while mobile applications use these data to provide a wide range of service such as friend recommendation. Profile (e.g., contact list, interest, mobility) matching is more than important for fostering the wide use of mobile social networks because recommending the individuals of the common contacts list/similar interests is always the first step for any social networking. The social networks such as Facebook, Line or WeChat recommend the friends for the users based on contact list or mobility traces. The existing mobile social network systems pay little attention to the privacy concerns associated with friend matching and recommendation based on users' personal information. For example, in Facebook, it provides the feature of People You May Know, which recommend

s the friends based on the education information, the contact lists obtained from users' smart phone, and other users' personal information. The basic motivation is that each user obfuscates every bit of the original personal data (e.g., contact list) before uploading by performing XOR operations with a masking sequence which is generated with a

DOI: 10.15680/IJIRCCE.2019. 0703060

certain probability. The design can ensure that the same data maintain a statistical similarity after obfuscation while different data can be statistically classified without leaking the original data.

II. LITERATURE SURVEY

1) D. Lewis, "icloud data breach: Hacking and celebrity photos,"

A few days ago a group calling themselves hackappcom posted a proof of concept script on the popular code repository called Github that would allow for a user to attempt to breach iCloud and access a user account. This script would query iCloud services via the "Find My iPhone" API to guess username and password combinations. The problem here was that apparently Apple AAPL +1.65% was not limiting the number of queries. This allowed for attackers to have numerous chances to guess password combinations without the fear of being locked out.

This script was an output from a talk that was given by Andrey Belenko and Alexey Troshichev called, "iCloud Keychain and iOS 7 Data Protection" at the Russian Defcon Group DCG#7812. Based on the note that they posted after the news of the breach started to circulate, they were rather upset that their script was being used to a malicious end.

In justification I can only mention, that we only described the way HOW to hack AppleID. Stealing private "hot" data is outside of our scope of interests. We discuss such methods of hacks in our's narrow range, just to identify all the ways how privacy can by abused.

For everyone, who was involved in this incident, I want to remind, that today we are living in Brave New Global World, when privacy protection wasn't ever so weak, and you have to consider, that all you data from "smart" devices could be accessible from internet,which is the place of anarchy, and, as result, could be source of undesirable and unfriendly activity.

2) Findu: Privacy-preserving personal profile matching in mobile social networks,"
M. Li, N. Cao, S. Yu, and W. Lou,

Making new connections according to personal preferences is a crucial service in mobile social networking, where the initiating user can find matching users within physical proximity of him/her. In existing systems for such services, usually all the users directly publish their complete profiles for others to search. However, in many applications, the users' personal profiles may contain sensitive information that they do not want to make public. In this paper, we propose FindU, the first privacy-preserving personal profile matching schemes for mobile social networks. In FindU, an initiating user can find from a group of users the one whose profile best matches with his/her; to limit the risk of privacy exposure, only necessary and minimal information about the private attributes of the participating users is exchanged. Several increasing levels of user privacy are defined, with decreasing amounts of exchanged profile information. Leveraging secure multi-party computation (SMC) techniques, we propose novel protocols that realize two of the user privacy levels, which can also be personalized by the users. We provide thorough security analysis and performance evaluation on our schemes, and show their advantages in both security and efficiency over state-of-the-art schemes.

3) "Secure friend discovery in mobile social networks,"
W. Dong, V. Dave, L. Qiu, and Y. Zhang,

Mobile social networks extend social networks in the cyberspace into the real world by allowing mobile users to discover and interact with existing and potential friends who happen to be in their physical vicinity. Despite their promise to enable many exciting applications, serious security and privacy concerns have hindered wide adoption of these networks. To address these concerns, in this paper we develop novel techniques and protocols to compute social proximity between two users to discover potential friends, which is an essential task for mobile social networks. We make three major contributions. First, we identify a range of potential attacks against friend discovery by analyzing real traces. Second, we develop a novel solution for secure proximity estimation, which allows users to identify potential friends by computing social proximity in a privacy-preserving manner. A distinctive feature of our solution is that it provides both privacy and verifiability, which are frequently at odds in secure multiparty computation. Third, we demonstrate the feasibility and effectiveness of our approaches using real implementation on smartphones and show it is efficient in terms of both computation time and power consumption.

4) "Veneta: Serverless friend-of-friend detection in mobile social networking,"
M. Von Arb, M. Bader, M. Kuhn, and R. Wattenhofer
Recently, mobile social software has become an active area of research and development. A multitude of systems have been proposed over the past years that try to follow the success of their Internet bound equivalents. Many mobile solutions try to augment the functionality of existing platforms with location awareness. The price for mobility, however, is typically either the lack of the popular friendship exploration features or the costs involved to access a central server required for this functionality. In this paper, we try to address this issue by introducing a decentralized method that is able to explore the social neighborhood of a user by detecting friends of friends. Rather than only exploiting information about the users of the system, the method relies on real friends, and adequately addresses the arising privacy issues. Moreover, we present VENETA, a mobile social networking platform which, among other features, implements our novel friend of friend detection algorithm.

III. EXISTING SYSTEM

- ❖ The existing mobile social network systems pay little heed to the privacy concerns associated with friend matching and recommendation based on users' personal information. For example, in Facebook, it provides the feature of People You May Know, which recommends the friends based on the education information, the contact lists obtained from users' smart phone, and other users' personal information.
- ❖ Li et al. applies additive homomorphic encryption in privacy preserving in a scenario with many intermediate computing parties.
- ❖ Narayanan et al. and Dong et al. computes social proximity to discover potential friends by leveraging both homomorphic cryptography and obfuscation, which is more efficient.

DISADVANTAGES OF EXISTING SYSTEM:

- ❖ Outsourcing users' personal information to the cloud for friend matching will raise a serious privacy concern
- ❖ Existing researches show that loss of privacy can expose users to unwanted advertisement and spams/scams, cause social reputation or economic damage, and make them victims of blackmail or even physical violence.
- ❖ The existing works may fail to work in practice due to the following two reasons. Firstly, the best practice in industry for friends recommendation is a multiple-users matching problem rather than a two-party matching problem. Some pre-share parameters between users are more likely to leak. Secondly, most of the existing works involve multiple rounds of protocols, which will suffer from a serious performance challenge.

IV.PROPOSED WORK

- ❖ 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.
- ❖ Our basic motivation is that each user obfuscates every bit of the original personal data (e.g., contact list) before uploading by performing XOR operations with a maskings equence which is generated with a certain probability.
- ❖ We propose a Scalable and Privacy-preserving Friend Matching scheme (SPFM) to prevent privacy leakage in friend matching and recommendation system.

ADVANTAGES OF PROPOSED SYSTEM:

- ❖ Our design can ensure that the same data maintain a statistical similarity after obfuscation while different data can be statistically classified without leaking the original data.

- ❖ We provide a detailed feasibility and security analysis as well as the discussion of correctness, True-Negative rate and True-Positive rate.
- ❖ Extensive evaluations have been performed on SPFM to demonstrate the feasibility and security.

ARCHITECTURE

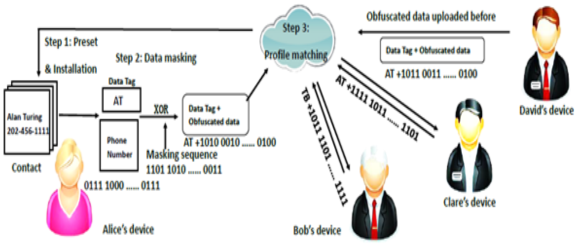

Fig 1: system Architecture

V. IMPLEMENTATION

- **Cloud Server**
  In this module, the Cloud Server has to login by using valid user name and password. After login successful he can perform some operations such as View all users and authorize and view all users in GMap using multiple markers, View all Friend Request and Response ,View all Friends matching based on Location(Mobility),Interest, Hobbies (Display into clusters),View all user image posts with rank,rating,reviews,View all Posts recommended Details(From and To),View all Friend recommended Details(From and To),List No. Of friend matching for each user and give link to view in Chart, View no.of Users in the same Interest and Mobility(Location).

- **Friend Request & Response**
  In this module, the CS can view all the friend requests and responses. Here all the requests and responses will be displayed with their tags such as Id, requested user photo, requested user name, user name request to, status and time & date. If the user accepts the request then the status will be changed to accepted or else the status will remains as waiting.

- **User**
  In this module, there are n numbers of users are present. User should register before performing any operations. Once user registers, their details will be stored to the database. After registration successful, he has to login by using authorized user name and password. Once Login is successful user can perform some operations like Register with Location(Give Combo Box),Interest(Give Combo Box),Hobbies(Give Combo Box),lat and long from GMap, View your profiles with Location, Interest, Hobbies, View Friend Matching based on Location, Interest, Hobbies and view their details and send friend request, Search Friend and Find Friend Request, View all Your Friends Based on Search, find route path using GMap and recommend friend to other by reason, View all Your Friends Based Friend Matching Parameters, find route path using GMap and recommend friend to other by reason, Add Post about images with image name, image desc(enc),image uses, add image, View all your Image posts details with rank and rating, reviews, View all your friends Image post details and recommend to other friends

- **Searching Friends**
  In this module, the user searches for friends in network and sends friend requests to them. The user can search for users in other sites to make friends only if they have permission.

VI. CONCLUSION

In this paper we tackles 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.

.

REFERENCES

[1] Q. Ye, H. Wang, And J. Pieprzyk, "Distributed Private Matching And Set Operations," In Information Security Practice And Experience. Springer, 2008, Pp. 347–360.
[2] M. J. Freedman, K. Nissim, And B. Pinkas, "Efficient Private Matching And Set Intersection," In Advances In Cryptology-Eurocrypt. Springer, 2004, Pp. 1–19.
[3] E. De Cristofaro And G. Tsudik, "Practical Private Set Intersection Protocols With Linear Complexity," In Financial Cryptography And Data Security. Springer, 2010, Pp. 143–159.
[4] R. Agrawal And R. Srikant, "Privacy-Preserving Data Mining," In Acm Sigmod Record, Vol. 29, No. 2. Acm, 2000, Pp. 439–450.
[5] A. Acquisti, L. Brandimarte, And G. Loewenstein, "Privacy And Human Behavior In The Age Of Information," Science, Vol. 347, No. 6221, Pp. 509–514, 2015.
[6] D. Lewis, "Icloud Data Breach: Hacking And CelebrityPhotos," And-Nude-Celebrity-Photos/.
[7] R. Shokri, G. Theodorakopoulos, C. Troncoso, J.-P. Hubaux, And J.-Y. Le Boudec, "Protecting Location Privacy: Optimal Strategy Against Localization Attacks," In Proceedings Of The Acm Conference On Computer And Communications Security. Acm, 2012, Pp. 617–627.
[8] M. Li, N. Cao, S. Yu, And W. Lou, "Findu: Privacy-Preserving Personal Profile Matching In Mobile Social Networks," In Ieee Infocom. Ieee, 2011, Pp. 2435–2443.
[9] W. Dong, V. Dave, L. Qiu, And Y. Zhang, "Secure Friend Discovery In Mobile Social Networks," In Ieee Infocom. Ieee, 2011, Pp. 1647– 1655.
[10] J. He, M. Dong, K. Ota, M. Fan, And G. Wang, "Netseccc: A Scalable And Fault-Tolerant Architecture For Cloud Computing Security," Peer-To- Peer Networking And Applications, Vol. 9, No. 1, Pp. 67–81, 2016.
[11] M. Dong, H. Li, K. Ota, L. T. Yang, And H. Zhu, "Multicloud-Based Evacuation Services For Emergency Management," Cloud Computing, Ieee, Vol. 1, No. 4, Pp. 50–59, 2014.