International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Survey of Privacy-Preserving Distributed Profile Matching in Mobile Social Network

Atul Atode[1], S. P. Kosbatwar[2]

[1, 2]Department of Computer Engineering, Savitribai Phule University of Pune, India

Abstract: ***Making new association as per individual inclinations is a critical administration in portable interpersonal interaction, where the starting client can locate the coordinating clients inside physical vicinity of him/her. The Profile coordinating means two clients contrasting their own profiles and is frequently the initial move towards successful nearness versatile informal organization. It, in any case, clashes with clients developing security concern s about revealing their own profiles to finish stranger before choosing to cooperate with them. The Protocol empowers two clients to perform profile coordinating without uncovering any data about their profile. Making new associations as indicated by individual inclinations is a urgent administration in versatile systems administration, where a starting client can discover coordinating clients inside physical closeness of them. More often than not in existing frameworks for such administrations, Users can specifically distribute their entire profile for different clients to hunt. Henceforth, in numerous applications, the client's close to home profiles may contain discerning data that they never need to make open. FindU, is a situated of security saving profile coordinating plans for nearness based portable interpersonal organizations. In FindU, the introductory customer can discover from a gathering of clients the one whose profile best matches with them to farthest point the danger of protection revelation, just requires and less data about the private qualities of the taking part customers is trading. Two expanding level of security protection are characterized, with multi-party computation techniques.***

Keywords: Privacy-enhancing personalized web search, Efficient query processing in geographic web search engines, Social network representations, Match -making protocol, PRF and oblivious PRF.

1. Introduction

With the proliferation of mobile devices, mobile social networks (MSNs) are becoming an inseparable part of our lives. Leveraging networked portable devices such as smart phones and PDAs as platforms, MSN not only enables people to use their existing online social networks (OSNs) at anywhere and anytime, but also introduces a myriad of mobility-oriented applications, such as location-bases services and augmented reality. Among them, an important service is to make new social connections/friends within physical proximity based on the matching of personal profiles. Proximity-Based mobile social networking (PMSN) becomes increasingly popular due to the explosive growth of smartphones. In particular, eMarketer estimated the US and worldwide smartphones users to be 73.3 million and 571.1 million in 2011, respectively and almost all smartphones have WiFi and Bluetooth interfaces. PMSN refers to the social interaction among physically proximate mobile users directly through the Bluetooth/Wi-Fi interface on their smartphones or the other mobile devices. For example FindU [2] and MagnetU [20] are MSN applications that matches one with nearby people for dating or making friend based on common interest. In such applications, a user only needs to input some (query) attributes in his/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 hobby, phone contacts and places they have been to. The latter can even be used to find "lost connections" and "familiar strangers".

Online social network providers such as Facebook and Twitter may add PMSN functionalities to their future applications for smartphones and other mobile devices. Private (profile) matching is indispensable for fostering the wide use of PMSN. On the on hand, people normally prefer to socialize with the others having similar interest or background over complete strangers. Such social reality makes profile matching [7] the first step towards effective PMSN, which refers to two users comparing their personal profiles before real interaction. On the other hand, people have growing privacy concerns for disclosing personal profiles to arbitrary persons in physical proximity before deciding to interact with them.

2. Literature Survey

In this section, they briefly discuss some work in several areas which is most germane to our work in this paper. Private matching for PMSN: As mentioned in section private matching scheme proposed in aim to coarse-grained personal profiles and match two users based on a privacy-preserving computation of the intersections (cardinality) of their attributes sets. In contrast our protocols support fine grained personal profiles and thus much finer differentiation, which is important for fostering the much wider use of PMSN.

A. Privacy-Enhancing Personalized Web Search

This approach present a scalable way for users to automatically build user profiles. These profiles summarize user's interest into a hierarchical organization according to specific interests. Two parameters for specifying privacy requirements are proposed to help the user to choose the contented degree of details of the profile information that is exposed to the search engine. Experiments showed that the user profile improved search quality when compared to standard MSN rankings.

B. Efficient Query Processing in Geographic Web Search Engines

In this approach, the problem of efficient query processing in scalable geographic search engines. Query processing is a major bottleneck in standard web search engines, and the main reason for the thousands of machines used by the major engines. Geographic search engine query processing is different in that it requires a combination of text and spatial data processing techniques. They propose several algorithms for efficient query processing in geographic search engines, integrate them into an existing web search query processor, and evaluate them on large sets of real data and query traces.

C. Mining User Preference Using Spy Voting For Search Engine Personalization

This paper addresses search engine personalization. They present a new approach to mining user's preferences on the search results from click through data and using the discovered preferences to adapt the search engine's ranking function for improving search quality. We develop a new preference mining technique called SpyNB, which is based on the practical assumption that the search results clicked on by the user reject the user's preferences, but it does not draw any conclusions about the results that the user did not click on.

D. Personalized Concept-Based Clustering Of Search Engine Queries

In this paper, they introduce an effective approach that captures the user's conceptual preferences in order to provide personalized query suggestions. We achieve this goal with two new strategies. First, we develop online techniques that extract concepts from the web-snippets of the search result returned from a query and use the concepts to identify related queries for that query. Second, we propose a new two phase personalized agglomerative clustering algorithm that is able to generate personalized query clusters.

E. Social Network Representations

Social networks offer to users interesting means and ways to connect, communicate, and share information with other members within their platforms. However, those sites have currently different structures/schemas and they represent users' profiles differently. Thus, they prohibit the exchange of information and communication with other

social networks (such as sharing pictures, tags, and comments) making them functioning as "Data Isolated Islands" .

3. Methodology

A. Location Attribute and it's 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.

B. Privacy Preserving Profile Matching Protocols

In Protocol [7], 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, which is similar to Protocol , but it excludes the confirmation information from the encrypted message. To prevent the dictionary profiling by malicious initiator, we improve Protocol to which provides a user personal defined privacy protection.

C. Match -Making Protocol

The paper [8] proposed by Qi Xie and UrsHengartner illustrates several cryptographic protocols for match making. In Initial phase the identity signer and a user guarantees that one user is assigned to only one identifier. Interest Signing Phase: This phase takes place between the personal interest signer (PIS) and a user (e.g., Alice). The PIS generates a safe prime, p, the first time when it starts When a user creates a name for a new interest, the PIS chooses a quadratic residue modulo p as the id of this interest. Matchmaking Phase: Alice and Bob exchange their exponentiated values, as received from the PIS, and the corresponding signatures to ensure authenticity of these values. Alice and Bob sign their messages to ensure non-repudiation in case misbehavior is detected.

D. PRF and Oblivious PRF

In this paper [10] StainslawJarecki and Xiaomin Liu Proposes Pseudorandom function (PRF) is an efficiently computable keyed function fk(.) 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 fk(x) of a PRF fk(.) 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.

4. Conclusion

In this survey paper, for the first time they introduce the problem of privacy-preserving distributed profile matching in MSNs, and propose two concrete schemes that achieve increasing levels of user privacy preservation. Towards designing lightweight protocols, we utilize Shamir secret sharing as the main secure computation technique, while we propose additional enhancements to lower the proposed

schemes' communication costs. Through extensive security analysis and simulation study, we show that:

1) The Schemes are proven secure under the HBC model, and can be easily extended to prevent certain active attacks;
2) The schemes are much more efficient than state-of the- art ones in MSNs where the network size is in the order of tens, and when the number of query attributes is smaller than the number of profile attribute.

References

[1] 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 ICDCS'10, Genoa, Italy, June 2010, pp. 468-477
[2] M. Li, N. Cao, S. Yu, and W. Lou, "FindU: Privacy-preserving personal profile matching in mobile social networks," in INFOCOM'11, Shanghai, China, Apr. 2011.
[3] 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.
[4] W. Dong, V. Dave, L. Qiu, and Y. Zhang, "Secure friend discovery in mobile social networks," in INFOCOM'11, Shanghai, China, Apr. 2011.
[5] A.Shamir, "How to Share a Secret," Comm. ACM, vol. 22, no. 11, pp. 612- 613, 1979.
[6] Giles Hogben, ENISA (2007), ENISA Position Paper No.1 "Security Issues and Recommendations for Online Social Networks"
[7] ElieRaad, Richard Chbeir, and Albert Dipanda," User Profile Matching in Social Networks" in Bourgogne University Dijon, France.
[8] Ralph Gross and Alessandro Acquisti,"Information Revelation and Privacy in Online Social Networks"
[9] Rui Zhang_, Yanchao Zhang_, Jinyuan (Stella) Suny, and GuanhuaYanz,"Fine-grained Private Matching for Proximity-basedMobile Social Networking".
[10] Muyuan Li, ZhaoyuGao, Suguo Du, Haojin Zhu, Mianxiong Dong, Kaoru Ota,"PriMatch: Fairness-aware Secure Friend Discovery Protocol in Mobile Social Network".
[11] Ming Li, Ning Cao, Shucheng Yuand Wenjing Lou,"FindU: Privacy-Preserving Personal ProfileMatching in Mobile Social Networks".
[12] Lan Zhang, Xiang-Yang Li,YunhaoLiu,"Message in a Sealed Bottle: Privacy Preserving Friending in Social Networks"
[13] Ji Sun Shin, Virgil D. Gligor," A New Privacy-Enhanced Matchmaking Protocol".
[14] Elena Zheleva, LiseGetoor," To Join or Not to Join: The Illusion of Privacy in Social Networks with Mixed Public and Private User Profiles".
[15] Rui Zhang, Jinxue Zhang, Yanchao Zhang, Jinyuan Sun, and Guanhua Yan," Privacy- Preserving Profile Matching for Proximity-based Mobile Social Networking".
[16] Boyang Wang, Baochun Li and Hui Li," Gmatch: Secure and Privacy-Preserving Group Matching in Social Networks".
[17] EerikaSavia, TeppoKurki, Sami Jokela," Metadata Based Matching of Documents and User Profiles"
[18] QiangTang, "User-Friendly Matching Protocol for Online Social Networks".
[19] ArjanJeckmans, Qiang Tang, and Pieter Hartel,"Privacy-Preserving Profile Matching Using the Social Graph"
[20] "Magnetu." [Online]. Available: http://magnetu.com