IJournals International Journal of Software & Hardware Research in Engineering
ISSN No: 2347-4890 Volume 2 Issue 12, December-

Fully Anonymous Profile Matching in Mobile Social Networks

Authors: Kundan M. Shewale, Sachin D. Babar

Department of Computer Engineering,
University of Pune

Sinhgad Institute of Technolgy, Lonawala,Pune,
Maharashtra, India

ABSTRACT:

Social networking makes digital communication technologies sharpening tools for extending the social circle of people. Privacy preservation is a significant research issue in social networking. Here user profile matching with privacy- preservation in mobile social networks (MSNs) is studied and a family of profile matching protocols is introduced. An explicit Comparison-based Profile Matching protocol (eCPM) which runs between two parties, an initiator and a responder is proposed which enables the initiator to obtain the comparison-based matching result about a specified attribute in their profiles, while preventing their attribute values from disclosure. An implicit Comparison-based Profile Matching protocol (iCPM) is then proposed which allows the initiator to directly obtain some messages instead of the comparison result from the responder. The messages unrelated to user profile can be divided into multiple categories by the responder. The initiator implicitly chooses the interested category which is unknown to the responder. Two messages in each category are prepared by the responder, and only one message can be obtained by the initiator according to the comparison result on a single attribute. iCPM is further generalized into an implicit Predicate-based Profile Matching protocol (iPPM) which allows complex comparison criteria spanning multiple attributes.

Index Terms—Mobile social network, profile matching, privacy preservation, homomorphic encryption, oblivious transfer.

I. INTRODUCTION :

Mobile Social networking is where individuals with similar interests connect with each other through their mobile/tablet. They form virtual communities. For example Facebook, Twitter, LinkedIn etc. What makes social network sites unique is not that they allow individuals to meet strangers, but rather that they enable users to articulate and make visible their social networks.[1] On many of the large SNSs, participants are not necessarily "networking" or looking to meet new people; instead, they are primarily communicating with people who are already a part of their extended social network.

Mobile Social Networks is a means of transmitting information (communicating) using a Mixture of voice and data devices over networks including cellular technology and elements of private and public IP infrastructure (such as the Internet). Mobile Social Networking' (MSN) refers to all of the enabling elements necessary for the contribution (posting' and uploading) and consumption (viewing/experiencing) of social media across a mobile network.[1] Key to the definition is the user's implicit or explicit choice of network technologies. If the user accesses a community service platform by way of any device that uses a cellular network, alone or in combination with a commercially-accessible wireless network that has access to cellular network operator-owned resources. mobile community operators and participants are, and can be, influenced by the platforms, trends and members of communities on the Internet[2].

II. PROBLEM DEFINITION:

Aim to determine the overall similarity of two profiles rather than their relation in Specific attributes. They commonly check whether the proximity measure of the two profiles is larger, equal, or smaller than a pre-defined threshold value. The proximity measurement can be the size of the intersection of two sets or the distance of two vectors where sets and vectors are used to represent profiles. They do not consider the larger, equal, or smaller relations of the attribute values as the matching metrics[3].

Our system consists of N users (parties) denoted as $P_1, \ldots, P_N$, each possessing a portable device. We denote the initiating party (*initiator*) as P_1. P_1 launches the matching process and its goal is to find one party that best *"matches"* with it, from the rest of the parties $P_2, \ldots, P_N$ which are called *candidates*. Each party P_i's profile consists of a set

of attributes S_i, which can be strings up to a certain length. P_1 defines a matching query to be a subset of S_1 , and in the following we use S_1 to denote the query set unless specified. we assume that the system adopts some standard way to describe every attribute, so that two attributes are exactly the same if they are the same semantically.[2]

III. RELATED WORK

Mobile social networks as emerging social communication platforms have attracted great attention recently, and their mobile applications have been developed and imple- mented pervasively. In mobile social networking applications, profile matching acts as a critical initial step to help users, especially strangers, initialize conversation with each other in a distributed manner. Yang et al. introduced a distributed mobile communication system, called E-SmallTalker, which facilitates social networking in physical proximity. E- SmallTalker automatically discovers and suggests common topics between users for easy conversation. studied e-healthcare cases by proposing a symptom matching scheme for mobile health social networks. They considered that such matching scheme is valuable to the patients who have the same symptom to exchange their experiences, mutual support, and inspiration with each other[3].

IV. PROFILE MATCHING:

Profile matching means two users comparing their personal profiles and is often the first step towards effective PMSN. It, however, conflicts with users growing privacy concerns about disclosing their personal profiles to complete strangers before deciding to interact with them[1].

The Concept of Profile Matching is as Follows:

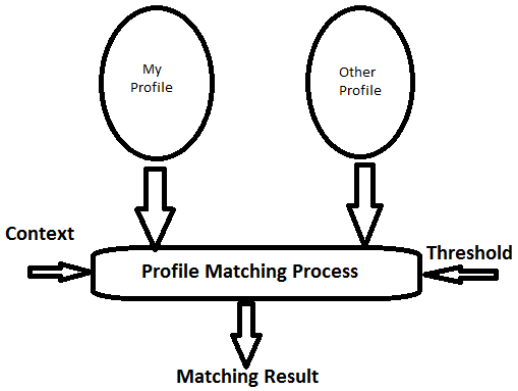

Fig. 1: Profile Matching

V. PRIMITIVES:

A. Privacy Preservation :

The privacy is the right to be let alone and it is the right to keep the disclosure of personal information safe from others. Privacy implications associated with online social networking depend on the level of identifiability of the information provided, it's possible recipients, and its possible uses.[1][3] It is relatively easy for anyone to gain access to it. By joining the network, hacking the site, or impersonating a user by stealing his password. Stalking to identity theft. Personal data are generously provided and limiting privacy preferences are sparingly used.

B.Homomorphic Encryption:

There are several existing homomorphic encryption schemes that support different operations such as addition and multiplication on ciphertexts. By using these schemes, a user is able to process the encrypted plaintext without knowing the secret keys. Due to this property, homomorphic encryption schemes are widely used in data aggregation and computation specifically for privacy-sensitive content. Here the homomorphic encryption scheme that serves a building block of our proposed profile matching protocols is reviewed[3].

VI. EXPLICIT COMPARISON BASED APPROACH (eCPM):

eCPM protocol allows two users to compare their attribute values on a specified attribute without disclosing the values to each other. But, the protocol reveals the comparison result to the initiator, and therefore offers conditional anonymity. [1]The protocol has a fundamental bootstrapping phase, where the TCA generates all system parameters, user pseudonyms, and keying materials.

VII. IMPLICIT COMPARISON BASED APPROACH (iCPM):

The implicit–based profile matching (iCPM) is proposed by adopting the oblivious transfer cryptographic technique. It is considered that users have distinct values for any given attribute. The iCPM consists of three main steps. In the first step, an interested category by setting element to 1 and other elements to 0 in a length, vector. Then

encrypt the vector by using the homomorphic encryption and sends the encrypted vector but still can process on the ciphertext. In the second step, computes the ciphertexts with input of self-defined messages for 1 ≤ message ≤ length[1][2].

VIII. IMPLICIT PREDICTABLE BASED APPROACH: (iPPM):

The eCPM and the iCPM perform profile matching on a single attribute. For a matching involving multiple attributes, they have to be executed multiple times, each time on one attribute. In this section, the iCPM is extended to the multi attribute cases, without jeopardizing its anonymity property, and obtain an implicit Predicate-based Profile Matching protocol, i.e., iPPM. This protocol relies on a predicate which is a logical expression made of multiple comparisons spanning distinct attributes and thus supports sophisticated matching criteria within a single protocol run[1][2].

IX. THREE CLASSES OF ANONYMITY:

Consider a user has υ possible instances of the profile

A. Non-Anonymity:

A profile matching protocol provides non anonymity if after executing multiple runs of the protocol with any user, the probability of correctly guessing the profile of the user is equal to 1[1].

B. Conditional Anonymity:

A profile matching protocol achieves conditional anonymity if after executing multiple runs of the protocol with some user, the probability of correctly guessing the profile of the user is larger than 1/υ[1].

C. Full Anonymity:

A profile matching protocol achieves full anonymity if after executing multiple runs of the protocol with any user, the probability of correctly guessing the profile of the user is always 1/υ[1][3].

X. The Working Scenarios of eCPM Is as follows:

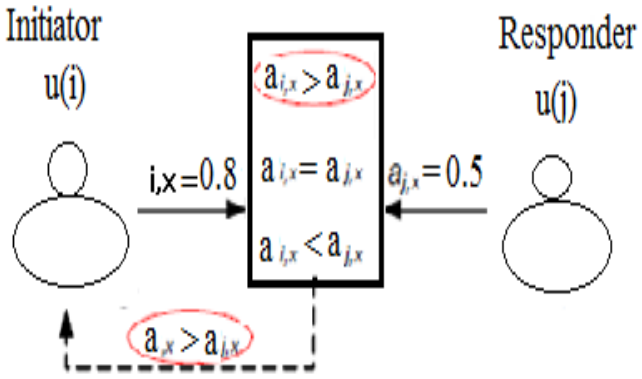

Fig.2: Working scenarios Of explicit comparison based approach

The explicit Comparison-based Profile Matching protocol, i.e., eCPM. This protocol allows two users to compare their attribute values on a specified attribute without disclosing the values to each other. But, the protocol reveals the comparison result to the initiator, and therefore offers conditional anonymity[5].

XI. *Hints Abbreviations and acronyms:*

MSN	Mobile Social Networks
SN	Social Networking Sites.
OSN	Online Social Network.
eCPM	explicit Comparison-based Profile Matching.
iCPM	implicit Comparison-based Profile Matching.
iPPM	Implicit predicate-based Profile Matching .
TCA	Trusted Central Authority.

XII. CONCLUSION:

A unique comparison-based profile matching problem in Mobile Social Networks (MSNs) has been investigated, and novel protocols are

proposed to solve it. The explicit Comparison based Profile Matching (eCPM) protocol provides conditional anonymity. It reveals the comparison result to the initiator. Considering the *k*-anonymity as a user requirement; the anonymity risk level in relation to the pseudonym change for consecutive eCPM runs is analyzed. Further an enhanced version of the eCPM, i.e., eCPM+ is introduced, by exploiting the prediction-based strategy and adopting the pre-adaptive pseudonym change. The effectiveness of the eCPM+ is validated through extensive simulations using real-trace data. Two protocols with full anonymity, i.e., implicit Comparison-based Profile Matching (iCPM) and implicit Predicate-based Profile Matching (iPPM) has been devised. The iCPM handles profile matching based on a single comparison of an attribute while the iPPM is implemented with a logical expression made of multiple comparisons spanning multiple attributes.

XIII. **REFERANCES**:

1) Annet Sahila G, Dr. P.Latha "Privacy Preserving and Fully Anonymous Protocols for Profile Matching in Mobile Social Networks "in International Journal of Computer Science and Mobile Applications,Vol.2 Issue. 2, February-2014

2)Ming Li, Shucheng Yu, Ning Cao, and Wenjing Lou, *Senior Member, IEEE* "Privacy-Preserving Distributed Profile Matching in Proximity-based Mobile Social Networks" in *IEEE INFOCOM '11*, Apr 2011.

3) Xiaohui Liang, Xu Li, Kuan Zhang, Rongxing Lu, Xiaodong Lin, and Xuemin (Sherman) Shen, "Fully Anonymous Profile Matching in Mobile Social Network" in IEEE Transaction On Networking Year 2013.

4) R. Lu, X. Lin, and X. Shen, "Spring: A social-based privacy-preserving packet forwarding protocol for vehicular delay tolerant networks," in *Proc. IEEE INFOCOM*, 2010.

5) W. He, Y. Huang, K. Nahrstedt, and B. Wu, "Message propagation in ad- hoc-based proximity mobile social networks," in *PERCOM workshops*,2010, pp.

6) D. Niyato, P. Wang, W. Saad, and A. Hjørungnes, "Controlled coalitional games for cooperative mobile social networks," *IEEE Transactions on Vehicular Technology*, 1812–1824, 2011.

7) E.Bulut and B.Szymanski, "Exploiting friendship relations for efficient routing in delay tolerant mobile social networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 12, pp. 2254–2265, 2012.

8) Z. Yang, B. Zhang, J. Dai, A. C. Champion, D. Xuan, and D. Li, "E-smalltalker: A distributed mobile system for social networking in physical proximity," in *ICDCS*, 2010, pp. 468–477.

9) R. Lu, X. Lin, X. Liang, and X. Shen, "A secure handshake scheme with symptoms-matching for mhealthcare social net- work," *Mobile Networks and Applications*, pp. 1–12, 2010.

10) C. Zhang, X. Zhu, Y. Song, and Y. Fang, "C4: A new paradigm for providing incentives in multi-hop wireless networks," in *INFOCOM, 2011 Proceedings IEEE*, april 2011, pp. 918 –926.

THIS PAGE IS INTENTIONALLY LEFT BLANK

THIS PAGE IS INTENTIONALLY LEFT BLANK

