IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 3, March 2016

Fully Anonymous Profile Matching In Social Network

Deepak Thorat[1], Alok Salvi[2], Pradeep Shingade[3], Swapnil Gholap[4]

Student, Computer Engineering, Shivajirao S. Jondhale College of Engineering, Thane, India[1, 2, 3]

Professor, Computer Engineering, Shivajirao S. Jondhale College of Engineering, Thane, India[4]

Abstract: In this paper, we study how the user profile matching is done with privacy-preservation in mobile social networks(MSNs).We propose two techniques for comparison of profile i.e Explicit comparison based profile matching protocol (eCPM) runs between two parties a initiator and a responder. In this method initiator obtain the comparison-based matching result about the specified attributes in their profiles, while preventing their attribute values from disclosure. The profile matching based on implicit comparison protocol (iCPM) allows the initiator to directly obtain some messages instead of the comparison result from the responder.

Keywords: Mobile Social Networks (MSNs), Explicit comparison based profile matching protocol (eCPM), implicit comparison protocol (iCPM).

I. INTRODUCTION

Mobile Social networking is world where individuals with similar interests connect with each other through their mobile/tablet. They form virtual communities. For example Facebook, Twitter, Google+, LinkedIn etc. What makes social network sites popular is not that they allow individuals to meet strangers, but rather that they prompt users to interact and make visible their social networks.[1] On the large social network world users are not necessarily "networking" or searching to meet new person ,instead they are primarily communicating with persons who are already a part of social network. The meaning of Mobile Social Networks is transmitting information or communicating using a mixture of voice and data devices over networks including cell phone technology and elements of private and public network infrastructure such as the world of Internet. Mobile Social Networking (MSN) refers to all of the start up elements necessary for the posting, uploading, viewing and experiencing of social media content across a mobile network.[1] Key to the definition is the user‘s implicit or explicit way of network technologies. If the user accessing a community service platform through any device that uses a cell phone network or in combination with commercially-accessible wireless network that has access to cell phone network operator-owned resources. Mobile community operators and participants are can be influenced by the platforms, trends and members of community on the world of Internet [2].

II. LITERATURE SURVEY

Mobile social networks as fastest growing social communication platforms have attracted great attention in recent time and their mobile apps have been implemented and developed extensively. In mobile social networking apps, profile matching acts as a initial step to help users, especially unknown user, initialize communication with each other in a separated manner. Yang et al introduced aconcept called E-SmallTalker as distributed mobile communication system, which makes social networking easy in physical proximity. E- SmallTalker automatically discovers and suggests similarities between users for easy communication. Case study of e-healthcare cases by proposing a significance matching scheme for mobile health social networks. They realized that such matching scheme is very important to the patients who have the same significance to exchange their treatment experiences, mutual support and motivations with each other[3].

III. PROPOSED SYSTEM

The main aim to determine the similarity of two profiles rather than their relation in specific attributive value .They commonly check whether the similarity measure of the two profiles is greater, equal , or less than a predefined value. The similarity measurement can be the distance of two vectors or the sizes of the intersection of two sets, where vectors and sets are used to represent profiles .They do not consider the greater, equal, or lesser relations of the attributive value as the match metrics [3].

Our system includes N number of users (parties) denoted as P1,...,...,...PN, each having a portable device. We denote the initiator as P1. P1 starts the matching process and his/her goal is to find any one party that best “matches” with it from the rest of the parties P2,...,PN which are called as candidates. Each party Pi ’s profile consists of attributes set Si ,which can be strings up to a certain length .Matching query is defined by P1 to be a subset of S1, and in the following we use S1 to denote the query set specified. We assume that the system adopts some benchmark to describe every attribute, so that two attributes are exactly the similar if they are the same semantically.[2].

IV.PROFILE MATCHING

Profile Matching means comparison of two user profiles from that social network and it is the first step towards

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 3, March 2016

effective profile matching social network .It however struggles with users issuance privacy concerns about sharing their personal profile information to completely unknown person before deciding to start communication with them [1]. Concept of profile matching is as follows:

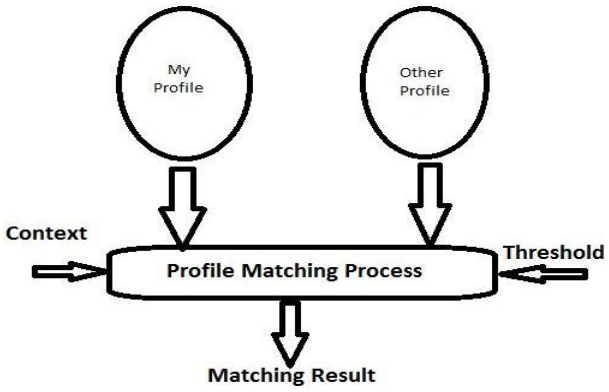

Fig. 1: Profile Matching

V. PRIMITIVES

A. Privacy Preservation

The user has right to kept his information private and hidden from unknown person. Privacy associated with online social networking sites depend on the level of the information provided, it is possible recipients, and it is possible uses. [1][3] It is relatively very easy for anyone to gain access to it by hacking the site, impersonating a user by stealing his password or joining the network. Identify theft by staking. Limiting privacy preferences are sparingly used and personal data are generously provided.

B. Homomorphic Encryption:

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

VI. EXPLICIT BASED COMPARISON APPROACH (eCPM)

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

VII. IMPLICIT BASED COMPARISON APPROACH: (iCPM)

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

Then encryption is done to vector by using the homomorphic encryption and forwards the encrypted vector but it still can process on the ciphertext. In the second step, computes the ciphertexts with input of self-defined messages for $1 \leq$ message $\leq$ length [1][2].

VIII. IMPLICIT BASED PREDICTABLE APPROACH: (iPPM)

The iCPM and eCPM perform profile matching on a single attribute. For a matching that involving multiple attributes, they have to be executed many times, each time on single attribute. In this section, the iCPM is extended to the multiple attribute cases, without exposing its anonymity property and obtain iPPM an implicit Predicate-based Profile matching protocol.

This protocol depends on a predication which is a logical expression made of many comparisons extending distinct attributes and therefore supports complex matching criteria within a single protocol run[1][2].

IX. THREE CLASSES OF ANONYMITY

Consider a user has possible instances of the profile

A. Non-Anonymity

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

B. Conditional Anonymity

A profile matching protocol gives result as conditional anonymity if after executing many runs of the protocol with some user, the probability of guessing the profile of the user correctly is larger than 1[1].

C. Full Anonymity:

A profile matching protocol gives result as full anonymity if after executing many runs of the protocol with any user, the probability of guessing the profile of the user correctly is always 1[1][3].

X. THE WORKING SCENARIO OF eCPM AND iCPM AS FOLLOES

Scenario 1: The initiator wants to know the result of the comparison, that is, if you have a greater, equal, or lesser specified attribute value than the responder.

Scenario 2: The initiator expected response actions of a message related to the category of interest, yet remains hidden to the responder.

Meanwhile, the responder who wants to share with the originator of a message is determined by the result of the comparison of their attribute values

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 3, March 2016

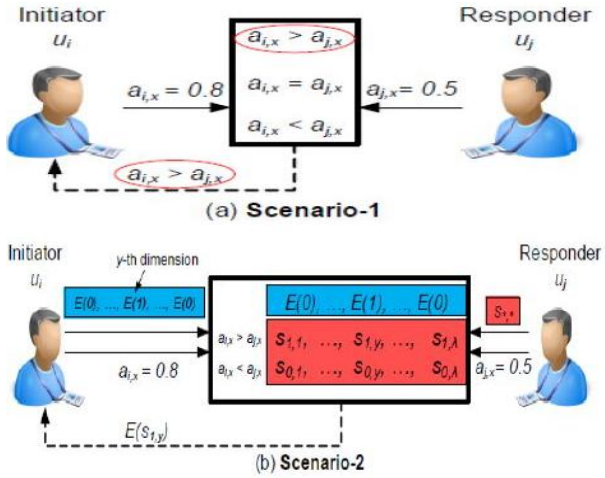

Fig.2: Working Scenarios of Explicit And implicit Comparison Based Approach

XI. HINTS ABBREVIATIONS AND ACRONYMS

SNS - Social Networking Sites
OSN - Online Social Network
MSN - Mobile Social Networks
iCPM - Implicit Comparison-based Profile Matching
eCPM - Explicit Comparison-based Profile Matching
iPPM - Implicit Predicate-based Profile Matching
TCA - Trusted Central Authority

XII. CONCLUSION

A unique comparison-based profile matching problem in (MSNs) Mobile Social Networks has been investigated and desire protocols are proposed to solve it. The (eCPM) explicit Comparison based Profile Matching protocol provides conditional anonymity. It reveals result of the comparison to the initiator. Assuming the k-anonymity as a user requirement; the risk level of anonymity in relation is analyzed to the pseudonym change for consecutive eCPM runs. Further an enhanced version of the eCPM, i.e., eCPM+ is introduced, by using the prediction-based strategy and adopting the pre-adaptive alias change. The effectiveness of the eCPM+ is validated through large recreation using real-trace data. Two protocols with full anonymity, i.e., implicit Predicate-based Profile Matching (iPPM) and implicit Comparison-based Profile Matching (iCPM) 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.

REFERENCES

[1] "Comscore," http://www.comscoredatamine.com/.
[2] A. G. Miklas, K. K. Gollu, K. K. W. Chan, S. Saroiu, P. K. Gummadi, and E. de Lara, "Exploiting social interactions in mobile systems," in Ubicomp, 2007, pp. 409–428.
[3] S. Ioannidis, A. Chaintreau, and L. Massouli´e, "Optimal and scalable distribution of content updates over a mobile social network," in Proc. IEEE INFOCOM, 2009, pp. 1422–1430.
[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, pp. 632–640.
[5] W. He, Y. Huang, K. Nahrstedt, and B. Wu, "Message propagation in adhoc-based proximity mobile social networks," in PERCOM workshops, 2010, pp. 141–146.
[6] D. Niyato, P. Wang, W. Saad, and A. Hjørungnes, "Controlled coalitional games for cooperative mobile social networks," IEEE Transactions on Vehicular Technology, vol. 60, no. 4, pp. 1812–1824, 2011. [7] M. Motani, V. Srinivasan, and P. Nuggehalli, "Peoplenet: engineering a wireless virtual social network," in MobiCom, 2005, pp. 243–257.
[8] M. Brereton, P. Roe, M. Foth, J. M. Bunker, and L. Buys, "Designing participation in agile ridesharing with mobile social software," in OZCHI, 2009, pp. 257–260.
[9] 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.
[10] 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.