IJSEAT International Journal of Science Engineering and Advance Technology

Improved Privacy Preserving Profile Matching in Online Social Networks

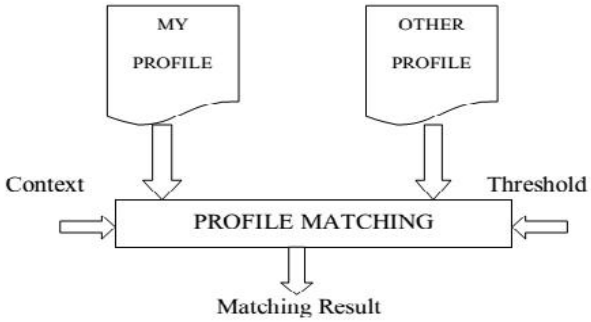
Nageswara Rao Yarlagadda, B. Naresh,
M.Tech research scholar,Asst. Prof in Department Of Computer Science And Engineering,
Srkit,Vijayawada.

Abstract:

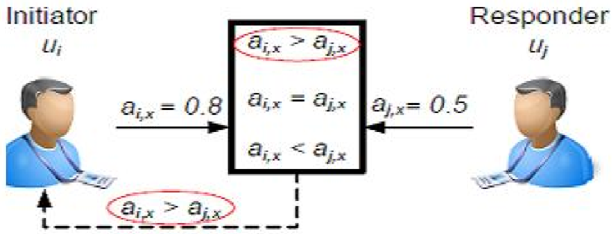
Social networking became popular because of its digital communication technologies tools for extending the social circle of people. Privacy preservation became a significant issue in social networking. This work discussed user profile matching with privacy preservation and introduced a group of profile matching protocols. Online social network with a mixture of public and private user profiles to predict the private attributes of users. We map this problem to a relational classification problem and we propose practical models that use friendship and group membership information (which is often not hidden) to infer sensitive attributes. The key novel idea is that in addition to friendship links, groups can be carriers of significant information. To the best of our knowledge, this is the first work that uses operation-based and group-based classification to study privacy implications in social networks with mixed public and private user profiles.

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

Introduction : Mobile Social networking where individuals with similar interests connect with each other through their mobile/tablet. Social network sites not only allow the user to articulate but also make visible their social networks. 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. The concept of profile matching is as follows



To emphasize this articulated social network as a critical organizing feature of these sites, we label them "social network sites." some web-based SNSs support limited mobile interactions (e.g., Facebook, MySpace, and Cyworld). 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)
The working scenario of eCPM as follows



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

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.

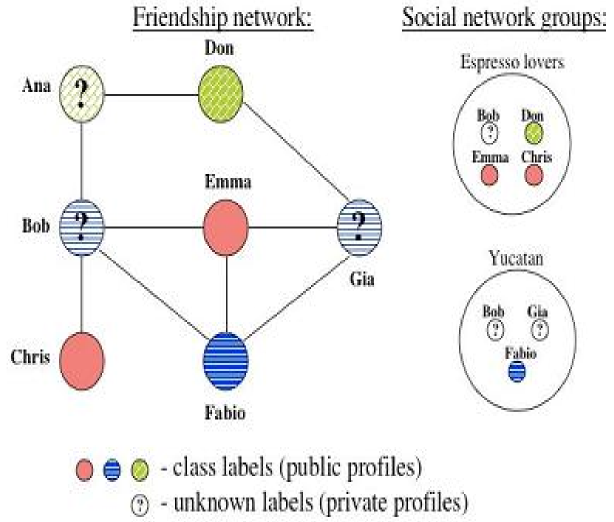
Existing System:

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.

Gathering a suitable trace to analyze the properties of people encounters is very challenging. Such a trace requires tracking many people simultaneously while recording all interactions among them. Collecting the data must not inconvenience the individuals being monitored and tracked. The privacy concerns raised by such experiments makes it particularly difficult to gather the data at scale. For all these reasons, very few large-scale traces of people encounters are available.

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. 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

The problem we consider is sensitive attribute inference in social networks: inferring the private information of users given a social network in which some profiles and all links and group memberships are public (this is a commonly occurring scenario in existing social media sites). We define the problem formally We believe our work is the first one to look at this problem, and to map it to a relational classification problem in network data with groups.



The novelty of our work is that we study the implications of mixing private and public profiles in a social network. For example, in Facebook many users choose to set their profiles to private, so that no one but their friends can see their profile details. Yet, fewer people hide their friendship links and even if they do, their friendship links can be found through the backlinks from their public-profile friends.

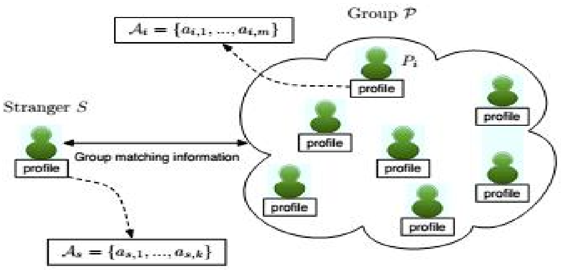
Similarly for group participation information – even if a user makes her profile private, her participation in a public group is shown on the group's membership list. Currently, neither Facebook nor Flickr allow users to hide their group memberships from public groups. Both commercial and governmental entities may employ privacy attacks for targeted marketing, health care screening or political monitoring – just to mention a few. Therefore, social media website providers need to protect their users against undesired eavesdropping and inform them of the possible privacy breaches and providing them with the means to be in full control of their private data.

In order to protect privacy, we sanitize both trait (e.g., deleting some information from a user's on-line profile) and link details (e.g., deleting links between friends) and explore the effect they have on combating possible inference attacks. Our initial results indicate that just sanitizing trait information or link information may not be enough to prevent inference attacks and comprehensive sanitization techniques that involve both aspects are needed in practice

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 [8]. Here the homomorphic encryption scheme that serves a building block of our proposed profile matching protocols is reviewed.

Proposed System:

We represent a social network as a graph G = (V, E, H), where V is a set of n nodes of the same type, E is a set of edges (the friendship links), and H is a set of groups that nodes can belong to. ei,j ∈ E represents a directed link from node vi to node vj . Our model handles undirected links by representing them as pairs of directed links. We describe a group as a hyper-edge h ∈ H among all the nodes who belong to that group; h.U denotes the set of users who are connected through hyper-edge h and v.H denotes the groups that node v belongs to.


Group $\mathcal{P}$
$\mathcal{A}_i = \{a_{i,1}, ..., a_{i,m}\}$
P_i
profile
Stranger S
profile
Group matching information
profile
profile
profile
profile
profile
profile
profile
$\mathcal{A}_s = \{a_{s,1}, ..., a_{s,k}\}$

During group matching, this stranger S wishes to collect group matching information from group P based on his profile. If an attribute in a group member's profile is equal to an attribute in the stranger's profile, it is then referred to as a matched attribute. Otherwise, it is called an unmatched attribute.

During the group matching, our scheme should be able to provide the following desirable privacy properties.

(1)Stranger's Attributes Privacy: The stranger does not reveal any attribute in his profile to any group member.

(2) Group Members' Attributes Privacy: The stranger only obtains matched attributes that both in his profile and some group member's profile, while the unmatched attributes in group members' profiles are not disclosed to the stranger.

(3) Exact Matching Information Privacy: The stranger is able to compute group matching information, while any exact matching information between himself and each group member is not revealed

We assume that each node v has a sensitive attribute v.a which is either observed or hidden in the data. A sensitive attribute is a personal attribute, such as age, political affiliation or location, which some users in the social network are willing to disclose publicly. A sensitive attribute value can take on one of a set of possible values {a1...am}. A user profile has a unique id with which the user forms links and participates in groups. Each profile is associated with a sensitive attribute, either observed or hidden. A private profile is one for which the sensitive attribute value is unknown, and a public profile is the opposite: a profile with an observed sensitive attribute value. We refer to the set of nodes with private profiles as the sensitive set of nodes Vs, and to the rest as the observed set Vo. The adversary's goal is to predict Vs.A, the sensitive attributes of the private profiles.

Here, we study the case where nodes have no other attributes beyond the sensitive attribute. Thus, to make inferences about the sensitive attribute, we need to use some form of relational classifier. While additional attribute information can be helpful and many relational classifiers can make use of it, in our setting this is not possible because all of the private-profile attributes are likely to be hidden

In current version of the iCPM and the iPPM, we implement ">" and "<" operations for profile matching. One future work is to extend them to support more operations, such as "≥" and "≤". And also we used to hide the predicate information in the iPPM. Currently, the responder needs to transmit the threshold value of the predicate to the initiator, which may reveal partial information of the responder's interest. Restricting the disclosure of such parameter will of significance for advancing comparison-based family of profile matching protocols and warrants deep investigation

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.

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.

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.

Abbreviations

MSN Mobile Social Networks
OSN Online Social Network
eCPM explicit Comparison-based Profile Matching
iCPM implicit Comparison -based Profile Matching
iPPM implicit predicate-based Profile Matching

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

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 onVehicular 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.

[11] Q. Li, S. Zhu, and G. Cao, "Routing in socially selfish delay tolerant networks," in Proc. IEEE INFOCOM, 2010, pp. 857–865.

[12] X. Liang, X. Li, T. H. Luan, R. Lu, X. Lin, and X. Shen, "Moralitydriven data forwarding with privacy preservation in mobile social networks," IEEE Transactions on Vehicular Technology, vol. 7, no. 61, pp. 3209–3222, 2012