ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Monthly Peer Reviewed Open Access International e-Journal

Privacy Protection during Profile Match Making over Online Mobile Social Networking Sites.

Tanguturi Rajesh
M.Tech,Student,
Computer Science Engineering Department,
Rao & Naidu Engineering College, Ongole.

K.Surya Kiran Kumar
M.Tech, Asst Professor,
Computer Science Engineering Department,
Rao & Naidu Engineering College, Ongole

Abstract:

Mobile social networking is social networking where individuals with similar interests converse and connect with one another through their mobile phone and/or tablet. Much like web-based social networking, mobile social networking occurs in virtual communities. A current trend for social networking websites, such as Facebook, is to create mobile apps to give their users instant and real-time access from their device.

Safety issues (including security, privacy, and trust) in mobile social networks are concerned about the condition of being protected against different types of failure, damage, error, accidents, harm or any other non-desirable event, while mobile carriers contact each other in mobile environments. However, lack of a protective infrastructure in these networks has turned them in to convenient targets for various perils. This is the main impulse why MSNs carry disparate and intricate safety concerns and embrace divergent safety challenging problems.

The rationale behind this work paper is to investigate the threats to privacy that come up while users not have a good judgment of privacy consciousness and apprehension when using social networking sites. At this juncture the dilemma of matching user profiles depending on profile's features is addressed in this paper.

Profile matching is process in which to two users are paired evaluated based on their individual profiles. This particular approach, though, clashes with users' increasing privacy concerns regarding revealing their individual profiles to absolute unfamiliar persons. Our work is as well regarding matching profiles that facilitate two users to execute profile matching with no need of reveling any kind of information about their individual profiles.

Keywords:

Mobile Social Networks(MSNs), Privacy, Matching, Individual Profiles, Privacy Protection, Information encryption.

Introduction:

A social networking service is a platform to build social networks or social relations among people who share interests, activities, backgrounds or real-life connections. A social network service consists of a representation of each user (often a profile), his or her social links, and a variety of additional services. Social networks are web-based services that allow individuals to create a public profile, to create a list of users with whom to share connections, and view and cross the connections within the system.

Most social network services are web-based and provide means for users to interact over the Internet, such as e-mail and instant messaging. Social network sites are varied and they incorporate new information and communication tools such as mobile connectivity, photo/video/sharing and blogging.

More and more, the line between mobile and web is being blurred as mobile apps use existing social networks to create native communities and promote discovery, and web-based social networks take advantage of mobile features and accessibility. As mobile web evolved from proprietary mobile technologies and networks, to full mobile access to the Internet, the distinction changed to the following types: 1) Web based social networks being extended for mobile access through mobile browsers and smartphone apps, and 2) Native mobile social networks with dedicated focus on mobile use like mobile communication,location-based services, and augmented reality, requiring mobile devices and technology.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Monthly Peer Reviewed Open Access International e-Journal

However, mobile and web-based social networking systems often work symbiotically to spread content, increase accessibility and connect users from wherever they are.

Privacy concerns with social networking services have been raised growing concerns amongst users on the dangers of giving out too much personal information and the threat of sexual predators. Users of these services also need to be aware of data theft or viruses. However, large services, such as MySpace and Netlog, often work with law enforcement to try to prevent such incidents.

In addition, there is a perceived privacy threat in relation to placing too much personal information in the hands of large corporations or governmental bodies, allowing a profile to be produced on an individual's behavior on which decisions, detrimental to an individual, may be taken.

Furthermore, there is an issue over the control of data—information that was altered or removed by the user may in fact be retained and passed to third parties. This danger was highlighted when the controversial social networking site Quechup harvested e-mail addresses from users' e-mail accounts for use in a spamming operation.

Privacy on social networking sites can be undermined by many factors. For example, users may disclose personal information, sites may not take adequate steps to protect user privacy, and third parties frequently use information posted on social networks for a variety of purposes.

"For the Net generation, social networking sites have become the preferred forum for social interactions, from posturing and role playing to simply sounding off. However, because such forums are relatively easy to access, posted content can be reviewed by anyone with an interest in the users' personal information".

Privacy Threats:

- Privacy implications associated with online social networking depend on the levelof identifiability of the information provided, it's possible recipients, and its possibleuses.
- Face Identification.
- Demographic data.
- It is relatively easy for anyone to gain access to it. By joining the network, hackingthe site, or impersonating a user by stealing his password.
- Stalking to identity theft.
- Personal data is generously provided and limiting privacy preferences are sparinglyused.
- Due to the variety and richness of personal information disclosed in Facebook profiles, their visibility, their public linkages to the members' real identities, and the scope of the network, users may put themselves at risk.
- Building Digital Dossier.

Privacy concerns have been found to differ between users according to gender and personality. Women are less likely to publish information that reveals methods of contacting them. Personality measures openness, extraversion, and conscientiousness were found to positively affect the willingness to disclose data, while neuroticism decreases the willingness to disclose personal information.

Many social networks provide an online environment for people to communicate and exchange personal information for dating purposes. Intentions can vary from looking for a one time date, short-term relationships, and long-term relationships.

Most of these social networks, just like online dating services, require users to give out certain pieces of information. This usually includes a user's age, gender, location, interests, and perhaps a picture. Releasing very personal information is usually discouraged for safety reasons. This allows other users to search or be searched by some sort of criteria, but at the same time people can maintain a degree of anonymity similar to most online dating services. Online dating sites are similar to social networks in the sense that users create profiles to meet and communicate with others, but their activities on such sites are for the sole purpose of finding a person of interest to date.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Monthly Peer Reviewed Open Access International e-Journal

Social networks do not necessarily have to be for dating; many users simply use it for keeping in touch with friends, and colleagues.

However, an important difference between social networks and online dating services is the fact that online dating sites usually require a fee, where social networks are free.

This difference is one of the reasons the online dating industry is seeing a massive decrease in revenue due to many users opting to use social networking services instead.

Many popular online dating services such as Match.com, Yahoo Personals, and eHarmony.com are seeing a decrease in users, where social networks like MySpace and Facebook are experiencing an increase in users.

Profile Matching:

Profile matching can be explained as process in which two users evaluating their personal profiles and is often the first step. Profile matching, although, clashes with users increasing privacy apprehensions about revealing their individual profiles to total unfamiliar persons before deciding to interact with them.

Existing System: Privacy protection is an important study topic in Mobile social networking. The social networking platforms are comprehensive of the mobile environment, users need more widespread privacy-preservation for the reason that they are new with the neighbors in surrounding area who may store, and compare their personal information at different time periods and locations.

Once the private data is associated to the location information, the actions of users will be totally revealed to the general public. To overcome the privacy violation in MSNs, many privacy enhancing techniques have been adopted into the MSN applications.

Threats in Mobile Social Networks:

1.Digital record aggregation: Profiles on MSNs can be downloaded and stored by third parties, creating a digital record of private data.

2.Secondary data collection: Information knowingly revealed in a profile. Various researches propose that such data is being used to significant monetary gain.

3.Face recognition: User-provided digital images are a very popular part of profiles on MSNs. The picture is, in effect, a binary identifier for the user, allowing linking across profiles.

4.Difficulty of complete account deletion: Users aspiring to remove accounts from MSNs discover that it is more or less not possible to delete secondary information linked to their profile such as public comments on other profiles.

5.Difficult to guard from malicious users who are snooping about the personal information of other users.

6.Difficult to safeguard from neighbors in mobile environment who may snoop, store, and compare their personal information.

7.The Internet stores an everlasting record of the conversation which can be tracked.

8.Using non-secure passwords might perhaps be without difficulty guessed by cyber criminals and compromise your MSN account to spam your contacts.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Monthly Peer Reviewed Open Access International e-Journal

Proposed System:

We first worked on an explicit Comparison-based Profile matching protocol (eCPM) which happens among two users, an initiator and a responder. The eCPM allows the initiator to attain the comparison-based matching outcome regarding a particular attribute in their profiles, at the same time as stopping their attribute values from revelation.

Later on we examined an implicit Comparison-based Profile matching protocol (iCPM) which permits the initiator to straight forwardly get various messages as an alternative of the evaluation outcome from the responder.

The messages unrelated to user profile can be divided into multiple categories by the responder. The initiator totally prefers the concerned category which is unfamiliar to the responder.

Two messages in every category are arranged by the responder, and only one message can be obtained by the initiator according to the comparison result on a single attribute.

We additionally generalized the iCPM to an implicit Predicate-based Profile Matching protocol (iPPM) which facilitates multifaceted evaluation criteria across several attributes.

The anonymity investigation demonstrates that all these protocols accomplish the confidentiality of user profiles. Apart from the above, the eCPM reveals the evaluation outcome to the initiator and provides simply conditional anonymity; the iCPM and the iPPM do not disclose the outcome at all and give full secrecy.

Merits of the proposed system:

1)Two commonly unknown users, both holding confidential information, together calculate the possible correlation without revealing any extra data to other user.

2)Make possible open communication, leading to improved information detection and delivery.

3)Permits users to talk about thoughts, ask questions and share links.

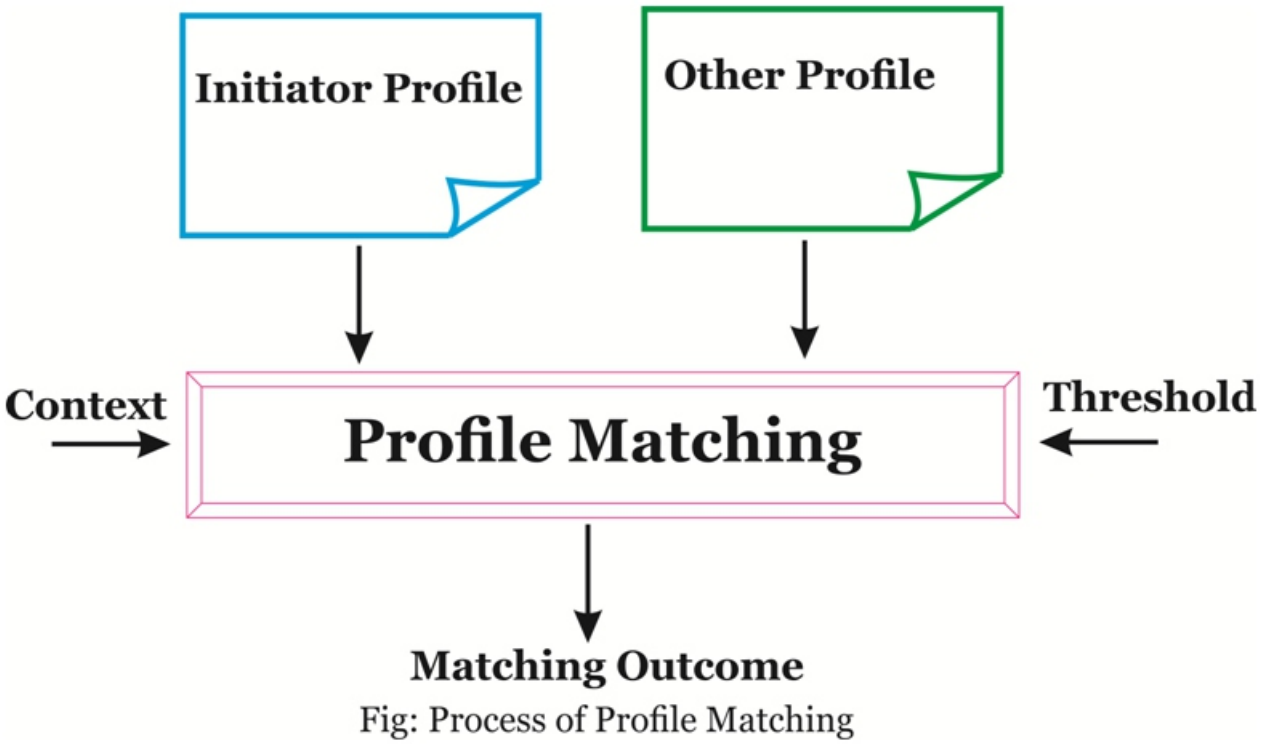
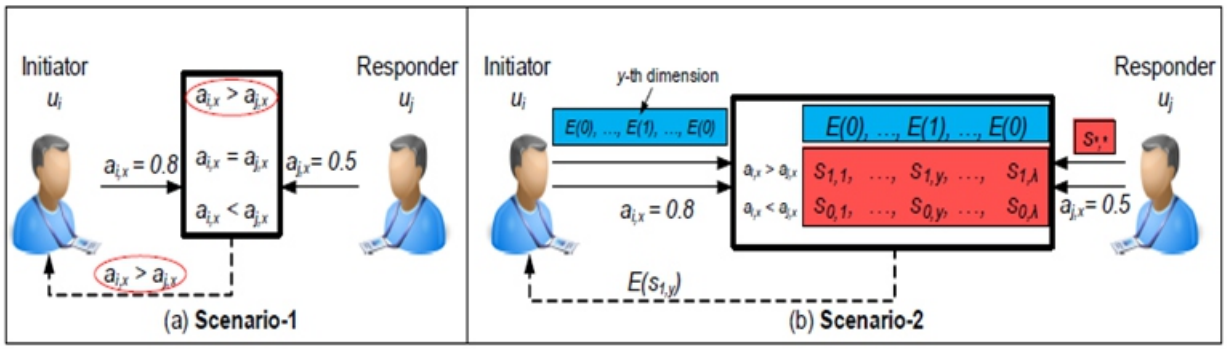


Fig: Process of Profile Matching

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Monthly Peer Reviewed Open Access International e-Journal

Flow Diagram:



MODULE DESCRIPTION:

Number of Modules:

After careful analysis the system has been identified to have the following modules:

1.Mobile Social Networking Module.

2.Explicit Comparison-based Profile Matching (eCPM) Module.

3.Implicit Comparison-based Profile Matching (iCPM) Module.

4.Privacy Preserving Module.

1. Mobile Social Networking Module:

The MSNs support many promising and novel applications. In the MSNs, users are able to not only surf the Internet but also communicate with peers in close vicinity using short-range wireless communications Realizing the potential benefits brought by the MSNs, recent research efforts have been put on how to improve the effectiveness and efficiency of the communications among the MSN users.

They developed specialized data routing and forwarding protocols associated with the social features exhibited from the behavior of users, such as, social friendship, social selfishness, and social morality.

2. Explicit Comparison-based Profile Matching (eCPM) Module:

Attribute, the eCPM allows the initiator to know the comparison result, i.e., whether it has a larger, equal, or smaller value than the responder on the attribute.

Due to the exposure of the comparison result, user profile will be leaked and linked in some conditions. We provide a numerical analysis on the conditional anonymity of the eCPM. We study the anonymity risk level in relation to the pseudonym change for the consecutive eCPM runs.

3.Implicit Comparison-based Profile Matching (iCPM) Module:

We propose the iCPM, in this protocol, the responder prepares multiple categories of messages where two messages are generated for each category. The initiator can obtain only one message related to one category for each run. During the protocol, the responder is unable to know the category of the initiator's interest.

To receive which message in the category is dependent on the comparison result on a specified attribute. The responder does not know which message the initiator receives, while the initiator cannot derive the comparison result from the received message. We provide an analysis of the effectiveness of the iCPM, and show that the iCPM achieves full anonymity.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Monthly Peer Reviewed Open Access International e-Journal

4. Privacy Preserving Module:

Privacy preservation is a significant research issue in social networking. Since more personalized information is shared with the public, violating the privacy of a target user become much easier. We propose three different protocols with different anonymity levels. For the eCPM with conditional anonymity, we provide detailed anonymity analysis and show the relation between pseudonym change and anonymity variation.

For the iCPM and the iPPM with full anonymity, we show that the use of these protocols does not affect user anonymity level and users are able to completely preserve their privacy.

Conclusion:

An exceptional comparison-based profile matching difficulty in Mobile Social Networks (MSNs) has been addressed, and new methods are projected to resolve it. The explicit Comparison depending on Profile Matching (eCPM) protocol provides conditional secrecy. It discloses the evaluation outcome to the initiator. Taking into account the k-anonymity as a user condition; the anonymity risk level in relation to the pseudonym change for successive eCPM runs is studied and observed. Two protocols with full anonymity, i.e., implicit Comparison-based Profile Matching (iCPM) and implicit Predicate-based Profile Matching (iPPM) has been simulated and worked upon.

The iCPM handles profile matching based on a single comparison of an attribute while the iPPM is implemented with a logical expression consists of multiple comparisons across several attributes. The iCPM and the iPPM both allow users to anonymously request for messages and respond to the requests according to the profile matching result, without disclosing any profile data.

References:

[1]. Xiaohui Liang, Student , Xu Li, Kuan Zhang, Rongxing Lu, Xiaodong Lin and Xuemin (Sherman) Shen, Fully Anonymous Profile Matching in Mobile Social Networks, IEEE TRANASCTIONS ON NETWORKING YEAR 2013

[2]. R.Gross, A. Acquisti, and H. J. H. III, —Information revelation and privacy in online social networks, in WPES, 2005, pp. 71–80.

[3]. Raad, E. ; LE2I, Bourgogne Univ., Dijon, France ; Chbeir, R. ; Dipanda, A.,User Profile Matching in Social Networks, 13th International Conference on Network-Based Information Systems (NBiS), 2010.

[4]. Rui Zhang, Jinxue Zhang, Yanchao Zhang, Jinyuan Sun, and Guanhua Yan, Privacy-preserving profile matching for proximity based mobile social networking, IEEE Journal on Selected Areas in Communications,Special Issue on Emerging Technologies in Communications, 2012.

[5]. Wei Dong ; Univ. of Texas at Austin, Austin, TX, USA ; Dave, V. ; Lili Qiu ; Yin Zhang,Secure friend discovery in mobile social networks,INFOCOM, 2011 Proceedings IEEE.

[6]. Xi Chen Sch., Nanjing Univ., Nanjing, China; Michael, K. Privacy Issues and Solutions in Social Network Sites,IEEE Society on Social Implications of Technology, 2012.

[7] P. Paillier, —Public-key cryptosystems based on composite degree Residuosity classes, in EUROCRYPT, 1999, pp. 223–238.

[8] M. Naehrig, K. Lauter, and V. Vaikuntanathan, —Can homomorphic encryption be practical? in CCSW, 2011, pp. 113–124.

[9] H. Ltkepohl, New introduction to multiple time series analysis. Springer, 2005.

[10] X. Liang, X. Li, Q. Shen, R. Lu, X. Lin, X. Shen, and W. Zhuang, —Exploiting prediction to enable secure and reliable routing in wireless body area networks,in Proc. IEEE INFOCOM, 2012, pp. 388–396.

[11] L. Sweeney, —k-anonymity: A model for protecting privacy,International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, vol. 10, no. 5, pp. 557–570, 2002.

[12] S. Ioannidis, A. Chaintreau, and L. Massouli´e, —Optimal and scalable distribution of content updates over a mobile social network, in Proc.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Monthly Peer Reviewed Open Access International e-Journal

IEEE INFOCOM, 2009, pp. 1422–1430.

[13] 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.

[14] 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.

[15] 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.

[16] R. Zhang, Y. Zhang, J. Sun, and G. Yan, "Fine-grained private matching for proximity-based mobile social networking," in Proc. IEEE INFO-COM, 2012, pp. 1969–1977.

[17] J. Freudiger, M. H. Manshaei, J.-P. Hubaux, and D. C. Parkes, "On non- cooperative location privacy: a game-theoretic analysis," in ACM CCS,2009, pp. 324–337.

[18] R. Lu, X. Lin, H. Luan, X. Liang, and X. Shen, "Pseudonym changing at social spots: An effective strategy for location privacy in vanets," IEEETransactions on Vehicular Technology, vol. 61, no. 1, pp. 86 – 96, 2011.

[19] J. Katz, A. Sahai, and B. Waters, "Predicate encryption supporting dis-junctions, polynomial equations, and inner products," in EUROCRYPT,2008, pp. 146–162.

[20] N. Eagle and A. Pentland, "Social serendipity: mobilizing social soft-ware," IEEE Pervasive Computing, vol. 4, no. 2, pp. 28–34, 2005.

[21] J. Teng, B. Zhang, X. Li, X. Bai, and D. Xuan, "E-shadow: Lubricating social interaction using mobile phones," in ICDCS, 2011, pp. 909–918.

[22] B. Han and A. Srinivasan, "Your friends have more friends than you do: identifying influential mobile users through random walks," in MobiHoc, 2012, pp. 5–14.