ISSN (Online): 2349-7084
GLOBAL IMPACT FACTOR 0.238
ISRA JIF 0.351

INTERNATIONAL JOURNAL OF COMPUTER ENGINEERING IN RESEARCH TRENDS
VOLUME 2, ISSUE 1, JANUARY 2015, PP 13-17

Profile Matching Scheme in Mobile Social Networks using iCPM Protocol

R.SEETHARAM *
Lecturer in Computer Science Department

Abstract: When the expanding utilization of cell phones in mobile social networks (MSNs) are turning into an interwoven part of individuals' lives there are numerous security protecting profile matching principle. In the event that we consider the client profile distinctive clients will have diverse occurrences of profiles so we will group the profile of clients into their non-anonymity, contingent secrecy, and full obscurity. The primary point is to focus the general likeness of two profiles as opposed to their connection in specific qualities. It checks whether the difference measure of the two profiles is large, equivalent or littler than predefined edge esteem. We can actualize the above matching plan. In existing structure the whole clients straight forwardly circulate their complete profiles for others to interest. In this paper a profile matching application is actualized which helps the customer to find the people whose profile is best matched with different people. It proposes the security convention which helps from profiling, builds the protection with the goal that less data about the client profile is uncovered. To give security to the data some exceptional conventions like ICPM, IPPM, ECPM and ECPM+ are making used.

Keywords: Profile matching, Privacy preservation, mobile social networks.

1. INTRODUCTION

Social network processes and functionalities are required in so many circumstances like data integration, information retrieval, etc., To scope this, user profiles are required and should match. The tendency in social networks is not fully well-matched with this hypothesis since users be disposed to create more than one social network account by having same or different email addresses. In this work, there are some reports that the tricky of matching profiles which range by only if a suitable matching framework is able to consider all the profile attributes.This basis allow users to give more importance to some attributes and give each attribute a different similarity measure. Social networking makes digital communication technologies sharpening tools for extending the social circle of people. It has already become an integral part of our dailylives, enabling us to contact our friends and families on time. To overcome the privacy violation in MSNs, many privacy enhancing techniques are implemented.For example,when two users encounter in the MSNs, privacy-preserving profile matching acts as a critical initial step to help users,especially strangers.The collective goal of these mechanism is to allow the handshake between two users if both users gratify each others condition while eradicating the redundant information leak if they are not.

The web site not only to read information, make business, connect pages, but also it was destined to be a social device for users, social networking has become an vital part of the online activities on the web. In essence, each social network offers particular services and functionalities that target a well-defined community in the real world.The main objective is to provide detailed anonymity analysis and show the relation between pseudonym change and anonymity variation for the iCPM and the iPPM with full anonymity it show that the use of these protocols does not affect user anonymity level and users are able to preserve their privacy. Here, the performance of three proposed protocols eCPM, iCPM, and iPPM are

ISSN (Online): 2349-7084
GLOBAL IMPACT FACTOR 0.238
ISRA JIF 0.351
INTERNATIONAL JOURNAL OF COMPUTER ENGINEERING IN RESEARCH TRENDS
VOLUME 2, ISSUE 1, JANUARY 2015, PP 13-17

studied in terms of statement overhead and anonymity strength. When considering anonymity, the case will be measured that users have different values for any given attribute. Non-distinct attribute values a comparison operations "≥" and "≤" will be considered in future work.As a future work, we are planning to further explore and propose more exciting intersocial Operations and functionalities.

2. LITERATURE SURVEY

Friend based on private profile matching allows two users to match their personal profiles without disclosing them to each other. There are two mainstreams of approaches to solve this problem. One category measures the social proximity by private vector dot product [1], [2], [10]. The another category provides private attributes matching based on private set intersection (PSI) and private cardinality of set intersection (PCSI), [9], [7]. Many social networking services are available on mobile phones (e.g., Juice Caster, Moco Space and Wi-Fi Face [3]) and majority of them are location-aware (e.g., Four Square, Bright Kite and Loopt).They rely on public-key cryptosystem and homomorphism encryption, which results in expensive computation cost and usually requires a trusted third party. Multiple rounds of interactions are required to perform the presetting (e.g. exchange public keys) and private matching between each pair of users. Moreover, most protocols are unverifiable: there lack efficient methods to verify the result. Furthermore, in these approaches, matched users and unmatched users all get involved in the expensive computation and find out their matching results with the initiator. These limitations hold back the adoption of the SMC related private matching methods in MSN. Magnet U [11] matches one with nearby people for dating, friend-making.

A boom in mobile hand-held devices greatly enriches the social networking applications. Many social networking services are available on mobile phones (e.g., Juice Caster, Moco Space and Wi-Fi Face [4]) and majority of them are location-aware .However, most of them are designed for facilitating people connections based on their real life social relationship [5], [6]. There is an increasing difficulty of befriending new people or communicating with strangers while protecting the privacy of real personal information. Friend and communication are two important basic functions of social networks. When people join social networks, they usually begin by creating a profile, and then interact with other users. Profile matching is a common and helpful way to make new friends with common interests or to search for experts [7]. Some applications help a user automatically find users with similar profile within a certain distance. For example, in the social network Color, people in close proximity (within 50 meters) can share photos automatically based on their similarity. Magnet U [11] matches one with nearby people for dating, friend-making. Small-talks [8] connect proximate users based on common interests. These applications use profiles to facilitate friend between proximate strangers and enable privacy preserving people searching to some extent.In existing service , have so many protocols and based on that particular service protocols privacy preserving has been developed like ICPM,ECPM+ in order have less prone attacks and attribute comparision secured protocols are used for further security issues which is higher than existing protocols.

3. 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:

ISSN (Online): 2349-7084
GLOBAL IMPACT FACTOR 0.238
ISRA JIF 0.351

INTERNATIONAL JOURNAL OF COMPUTER ENGINEERING IN RESEARCH TRENDS
VOLUME 2, ISSUE 1, JANUARY 2015, PP 13-17

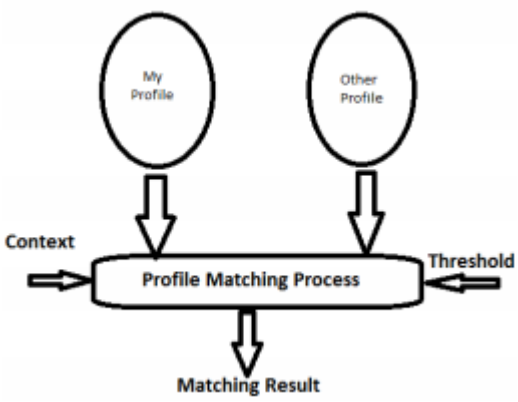


Fig 1.Profile matching

4. 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].

5. FLOWCHART AND ALGORITHM

For security purpose homomorphic encryption is used, there are several encryption schemes which are present that support several operations on cipher texts. Mainly, AES algorithm is used for securing purpose.

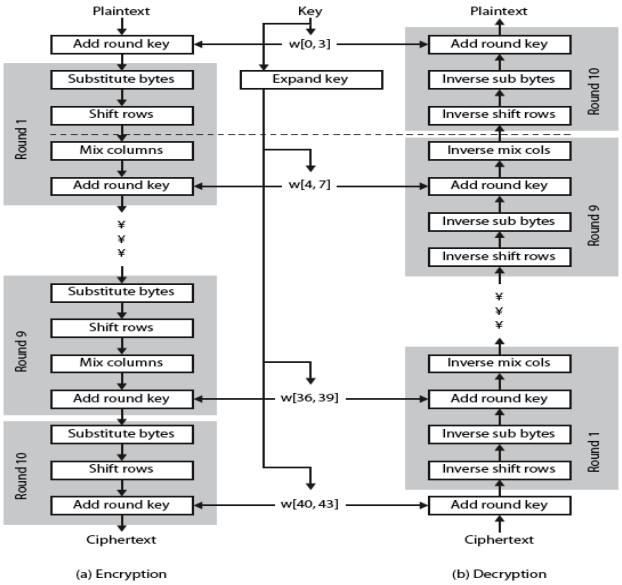


Fig 2. AES Senario

ALGORITHM

Step1: Register for login.

Step 2: New user will create profile.

Step2: Creating attribute values for the new user.

Step3: Profile creation is done.

Step 4: Login for viewing profiles.

Step5: Enter attribute values for matching.

Step 6: View existing profile.

Step 7: Check whether the attributes are matched or not.

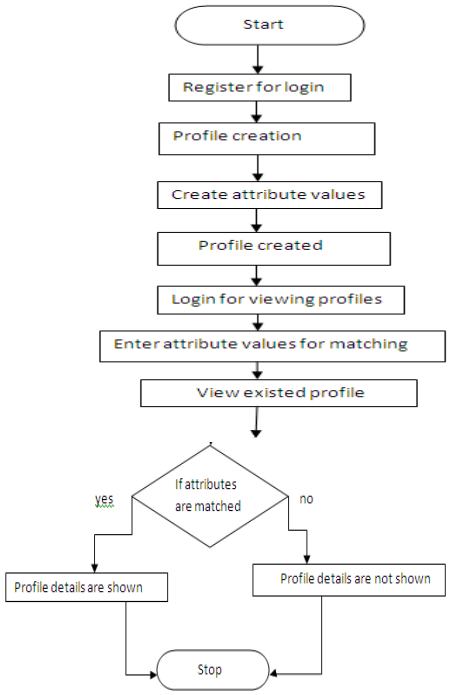
Step 8: when user browses other profile then the profile is completely visible when majority of attributes are matched.

ISSN (Online): 2349-7084
GLOBAL IMPACT FACTOR 0.238
ISRA JIF 0.351

INTERNATIONAL JOURNAL OF COMPUTER ENGINEERING IN RESEARCH TRENDS
VOLUME 2, ISSUE 1, JANUARY 2015, PP 13-17

Step9: if attribute values are not matched the profile is not completely shown.

FLOWCHART



6. PROFILE MATCHING TECHNIQUES

Profile matching mechanism is done by using some techniques like

Location Attribute and Its Privacy Protection

In mobile social networks, a user usually searches matching users in surrounding area. 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 surrounding area, if two users are within each other's surrounding area, the intersection of their surrounding area regions will have a proportion not less than a threshold. Compared to static attributes like identity information, location is usually a temporal privacy.

Privacy Preserving Profile Matching Protocols

By using protocols like iCPM, ECPM can preserve the profiles. The eCPM enables the initiator to obtain the comparison-based matching result about a specified attribute in their profiles, while preventing their attribute values from disclosure. We then propose an implicit Comparison-based Profile Matching protocol (iCPM) 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.

7. CONCLUSIONS

The diverse Profile Matching Techniques are utilized for portable social organize by contrasting and distinctive systems built with respect to their execution. The security is the significant issue for profile matching in versatile interpersonal organization, utilizing upgraded conventions the best strategy is to be actualized which are less inclined to assaults which doesn't uncover profile data and requires less correspondence expense and calculation cost.

REFERENCE:

[1] W. Dong, V. Dave, L. Qiu, and Y. Zhang, "Secure friend discovery in mobile social networks," in Proceedings of IEEE INFOCOM, 2011.

[2] I. Ioannidis, A. Gama, and M. Atallah, "A secure protocol for computing dot-products in clustered and distributed environments," in Proceedingsof IEEE ICPP, 2002.

[3] L. Zhang, X. Ding, Z. Wan, M. Gu, and X. Li, "Wiface: A secure geosocial networking system using

wifi-based multi-hop manet," in ACMMobiSys MCS workshop, 2010.

[4] K. Okamoto, W. Chen, and X.-Y. Li, "Ranking of closeness centrality for large-scale social networks," in FAW, 2008.

[5] S.-J. Tang, J. Yuan, X. Mao, X.-Y. Li, W. Chen, and G. Dai, "Relationship classification in large scale online social networks and its impact on information," in Proceedings of IEEE INFOCOM, 2011.

[6] L. Zhang, X.-Y. Li, J. Lei, J. Sun, Y. Liu, "Mechanism design for finding experts using locally constructed social referral web," in TPDS, 2013

[7] M. Von Arb, M. Bader, M. Kuhn, and R. Wattenhofer, "Veneta: Server less friend-of-friend detection in mobile social networking," in Proceedings of IEEE WIMOB, 2008.

[8] Z. Yang, B. Zhang, J. Dai, A. C. Champion, D. Xuan, and D. Li, "E-small talker: A distributed mobile system for social networking in physical proximity," in Proceedings of IEEE ICDCS, 2010.

[9] M. Li, N. Cao, S. Yu, and W. Lou, "Find u: Privacy-preserving personal profile matching in mobile social networks," in Proceedings of IEEEINFOCOM, 2011..

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

ABOUT THE AUTHOR

R.SEETHARAM, Working as Senior Lecturer in the department of Computer Science , he is having 8+ years of teaching Experience , he completed his Post Graduate M.SC(is) from Osmania University , Hyderabad. His Research areas are Computer Networks, Mobile Computing.