IJCAT International Journal of Computing and Technology, Volume 1, Issue 7, August 2014
ISSN : 2348 - 6090
www.IJCAT.org

A Privacy Preservation and Application-Level Performance for Profile Matching in Mobile Social Networks

[1] B. Tejaswini , [2] A. Srinivasan

[1] Post-Graduate Student,
Department of Computer Science and Engineering,
SITAMS, CHITTOOR, India

[2] Associate Professor,
Department of computer Science and Engineering,
SITAMS, CHITTOOR, India

Abstract - Social network makes digital communication technologies sharpening tools for extending the social circle connected with people. Privacy preservation is usually a significant research issue in social networking. Here user account matching with privacy-preservation in mobile social networks (MSNs) is studied as well as a category of profile matching protocols is introduced. An explicit Comparison-based Profile matching protocol (eCPM) which runs between two parties, an initiator along with a responder is proposed which enables the initiator to search for the comparison-based matching result with regards to a specified attribute within their profiles, while preventing their attribute values from disclosure. An implicit Comparison-based Profile matching protocol (iCPM) will be proposed that permits the initiator to directly obtain some messages rather than the comparison result from the responder.

The messages unrelated to user account might be separated into multiple categories through the responder. The initiator implicitly chooses the interested category which can be unknown for the responder. Two messages in each category are prepared through the responder, in support of one message can be acquired through the initiator based on the comparison result about the same attribute. iCPM is further generalized into an implicit Predicate-based Profile matching protocol (iPPM) that allows complex comparison criteria spanning multiple attributes. We analyze the communication overhead as well as the anonymity strength from the protocols. You have to present an enhanced version with the called by combining the having a novel prediction-based adaptive pseudonym change strategy. The performance comparatively studied through extensive trace-based simulations. Simulation results demonstrate which they achieve significantly higher anonymity strength with slightly larger variety of pseudonym.

***Keywords* - Networking, Social Networking, Mobile Social Networks, *Privacy Preserving*.**

1. Introduction

Social networking makes digital communication technologies sharpening tools for extending the social circle of people. It offers already become an essential integral a part of our daily lives, enabling us to make contact with our friends and families in time. Social networking sites including Face book and Twitter reach 82 percent around the world's online population, representing 1.2 billion users all over the world. For the time being, fuelled through the pervasive adoption of advanced handheld devices as well as the ubiquitous connections of Bluetooth/Wi-Fi/GSM/LTE networks, the usage of Mobile Social Networking (MSNs) has surged.

In the MSNs, users can not just surf the Internet and also communicate with peers in close vicinity using short-range wireless communications. Because of its geographical nature, the MSNs support many promising and novel applications For instance, through Bluetooth communications, People Net enables efficient information search among neighbouring mobile phone devices; a message-relay approach is suggested directly into facilitate carpool and ride sharing within a local region. Realizing the potential benefits through the MSNs, recent research efforts happen to be placed on how you can enhance the effectiveness and efficiency from the communications one of the MSN users. They developed

specialized data routing and forwarding protocols from the social features exhibited through the behaviour of users, such as, social friendship, social selfishness, and social morality. It can be encouraging how the traditional solutions might be further extended in order to resolve the MSN problems by thinking about the unique social features.

Privacy preservation can be a significant research issue in social networking. Since more personalized data is distributed to everyone, violating the privacy of any target user become much simpler. Research efforts are already put on identity presentation and privacy concerns in social networking sites. Gross and Acquits argued that users are putting themselves at risk both offline (e.g., stalking) and online (e.g., identity theft) with different behavior analysis in excess of 4,000 students who may have joined a well known social networking site. Stutsman presented a quantitative analysis of identity information disclosure in social network communities and subjective opinions from students regarding identity protection and information disclosure. Once the social networking platforms are extended in to the mobile environment, users require more extensive privacy-preservation because they're not really acquainted with the neighbours in close vicinity who may eavesdrop, store, and correlate their personal information at different time periods and locations. After the private information is correlated towards the location information, the behaviour of users will probably be completely disclosed towards the public.

2. Related Work

Profile matching means two users comparison their personal profiles and is particularly usually the initial step towards effective PMSN. It, however, conflicts with users ‘growing privacy concerns about disclosing their personal profiles to try and do strangers before choosing to communicate with them.

2.1 Privacy Preservation

The privacy is ―the ability to be let by itself‖ and it's the authority to maintain the disclosure of private information safe from others. Privacy implications regarding online social networking be determined by the quality of identifiability with the information provided, it‘s possible recipients, and its particular possible uses. It can be relatively simple for any person to achieve usage of 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.

2.2 K-Anonymity: A Model for Protecting Privacy

Data holders, operating autonomously sufficient reason for limited knowledge, remain with all the difficulty of releasing information that will not compromise privacy, confidentiality or national interests. Most of the time the survival with the database itself depends upon the information holder's capability to produce anonymous data because not releasing such information in any respect may diminish the requirement of the data, throughout another hand, neglecting to provide proper protection inside a release may create circumstances that harm the public varieties. So a standard practice is perfect for organizations to produce and receive person specific data with all of explicit identifiers, for example name, address and telephone number, removed around the assumption that anonymity is maintained since the resulting data look anonymous. However, generally in most of those cases, the residual data can often re-identify individuals by linking or matching the data along with other data or by taking a look at unique characteristics based in the released data.

2.3 Homomorphism Encryption

The development of cloud storage and computing plat-forms allows users to outsource storage and computations on the data, and allows businesses towards the task of maintaining data-centers. An effective way to these privacy concerns is usually to store all data within the cloud encrypted, and perform computations on encrypted data.

To this effect, we start to use an encryption scheme which allows meaningful computation on encrypted data, namely a homomorphism encryption scheme. Homomorphism encryption schemes that permit simple computations on Encrypted data happen to be recognized for a while. We build upon the somewhat homomorphism encryption, and Implement simple statistics such as mean, standard deviation and logistical regression, and set of the performance number.

3. Proposed Approach

It presents an enhanced version with the ecpm, called ecpm+; by combining the ecpm which has a novel prediction based adaptive pseudonym change strategy. The performance from the ecpm as well as the ecpm+ is

comparatively studied through extensive trace-based simulations. The ecpm+ achieves significantly higher anonymity strength with slightly larger variety of pseudonyms compared to ecpm. The msns, users can not simply surf the Internet and also get in touch with peers in close vicinity using short-range wireless communications. The social features exhibited through the behaviour of users, such as, social friendship social selfishness and social morality it really is encouraging which the traditional solutions is usually further extended to resolve the MSN problems by taking into consideration the unique social features. The homomorphism encryption schemes are widely utilized in data.

4. Architecture

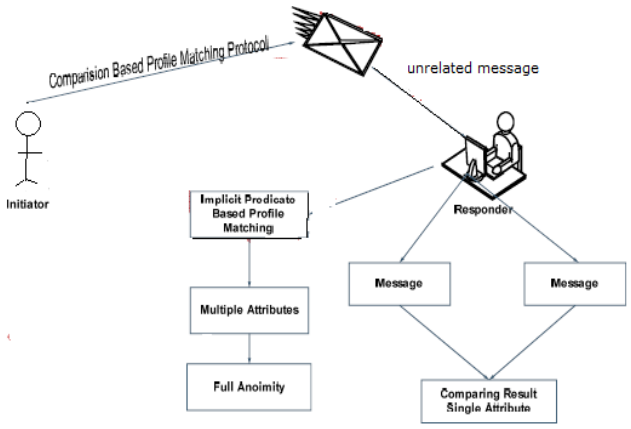

Fig 1: System Architecture

4.1 Profile Creator

The profile creator will be the preliminary module to produce an initiator profile or responder profile. The user profile details (username, password, email, mobile, gender, DOB, occupation, address, location, hobbie/interest).

4.2 Create Attribute Value

An explicit Comparison-based Profile Matching protocol (ECPM) which runs between two parties, an initiator along with a responder. The ecpm enables the initiator to search for the comparison-based matching result in regards to a specified attribute within their profiles, while preventing their attribute values from disclosure the attribute utilized in the comparison (i.e., priority level) as ax, as well as the category T of the's interest as Ty. The attribute values of about the attribute ax are denoted, respectively.

4.3 Initiator/Responder Secret Sharing

The initiator expects how the responder shares one message relevant to the group of its interest, which can be however kept unknown towards the responder. For the time being, the responder really wants to share with the initiator one message which can be based on the comparison results of their attribute values. The comparison and also the groups of messages the initiator first generates vector in which the y-the dimension value is 1 along with other dimension values are 0. Then, encrypts the vector which consists of own public key and sends the cipher texts towards the responder. The cipher texts imply ui's interested category Ty, but uj is not able to know Ty since E (0) and nondistinguishable and not using a decryption key

4.4 Implicit Comparison Based Profile Matching

The Implicit Comparison-based Profile Matching protocol (ICPM) that allows the initiator to directly obtain some messages rather than the comparison result of the responder. The messages unrelated to user profile could be split up into multiple categories through the responder. The initiator implicitly chooses the interested category which can be unknown towards the responder. Two messages in each category are ready through the responder, in support of one message can be acquired through the initiator in line with the comparison result using one attribute. Implicit Comparison-based Profile Matching (ICPM) and Implicit Predicate-based Profile Matching (IPPM). The icpm handles profile matching with different single comparison associated with an attribute even though the ippm is implemented which a logical expression has made from multiple comparisons spanning multiple attributes. The icpm and ippm both enable users to anonymously request messages and respond to the requests based on the profile matching result, without disclosing any profile information.

4.5 Responder Matching Secrets

The initiator can acquire just one message associated with one category for each and every run. Throughout the protocol, the responder is not able to be aware of the group of the initiator's interest. To obtain which message within the category is determined by the comparison result using a specified attribute. The responder will not know which message the initiator receives, even though the initiator cannot derive the comparison be a consequence of the received message. We offer an analysis of the effectiveness from the iCPM, and show which the iCPM achieves full anonymity.

5. Conclusion

A distinctive comparison-based profile matching condition in Mobile Social Networks (*MSNs*) continues to be investigated, and novel protocols are proposed in order to resolve it. The explicit Comparison based Profile Matching (*eCPM*) protocol provides *conditional* anonymity. It reveals the comparison give you the initiator. For the k-anonymity being a user requirement; the anonymity risk level with regards to the pseudonym change for consecutive *eCPM* runs is analyzed. Further an enhanced version from the *eCPM*, i.e., *eCPM+* is introduced, by exploiting the prediction-based strategy and adopting the pre-adaptive pseudonym change. The potency 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*) continues to be devised. The *iCPM* handles profile matching with different single comparison of the attribute even though the *iPPM* is implemented having a logical expression made from multiple comparisons spanning multiple attributes.

References

[1] B. Wang, B. Li, and H. Li, Gmatch: Secure and Private-preserving Group Matching in SocialNetworks, in Proceedings of IEEE Globecom 2012, pp. 744-749, 2012.

[2] M. Li, N. Cao, S. Yu, and W. Lou, FindU: Private-Preserving Personal Profile Matching in Mobile Social Networks, in Proceedings of IEEE INFOCOM 2011, pp. 2435-2443, 2011.

[3] E. Cristofaro and G. Tsudik, Practical Private Set Intersection Protocols with Linear Complexity, in Proceedings of Financial Cryptography 2010, pp. 143-159, 2010.

[4] D. Boneh, C. Gentry, B. Lynn and H. Shacham, Aggregate and Verifiably Encrypted Signatures from Bilinear Maps, in Proceedings of EUROCRYPT 2003, pp. 416-432, 2006.

[5] M. Freedman, K. Nisssim, and B. Pinkas, Efficient Private Matching and Set Intersection, in Proceedings of EUROCRYPT 2004, pp. 1-19, 2004.

[6] P. Paillier, Public Key Cryptosystems Based on Composite Degree Residuosity Classes, in Proceedings of EUROCRYPT 1999, pp. 223-238, 1999.

[7] Z. Yang, B. Zhang, J. Dai, A. Champion, D. Xuan and D. Li, ESmallTalker: A Distributed Mobile System for Social Networking in Physical Proximity, in Proceedings of IEEE ICDCS 2010,pp. 468-477, 2010.

[8] D. Dachman-Soled, T. Malkin, M. Raykova, and M. Yung,"Efficient robust private set intersection," in ACNS '09, 2009,pp. 125–142.

[9] G. S. Narayanan, T. Aishwarya, A. Agrawal, A. Patra, A. Choudhary, and C. P. Rangan, "Multi party distributed private matching, set disjointness and cardinality of set intersection withinformation theoretic security," in CANS '09. Springer - Verlag, Dec. 2009, pp. 21–40.

[10] C. Hazay and Y. Lindell, "Efficient protocols for set intersection and pattern matching with security against malicious and covert adversaries," in TCC'08, 2008, pp. 155–175.

[11] S. Jarecki and X. Liu, "Efficient oblivious pseudorandom function with applications to adaptive ot and secure computation of set intersection," in TCC '09. Berlin, Heidelberg: Springer-Verlag, 2009, pp. 577–594.

[12] W. Dong, V. Dave, L. Qiu, and Y. Zhang, "Secure friend discovery in mobile social networks," in IEEE INFOCOM '11, Apr 2011, pp. 1–9.

[13] E. De Cristofaro, M. Manulis, and B. Poettering, "Private discovery of common social contacts," in Applied Cryptography and Network Security. Springer, 2011, pp. 147–165.

[14] E. De Cristofaro, A. Durussel, and I. Aad, "Reclaiming privacy for smartphone applications," in Pervasive Computing and Communications (PerCom), 2011 IEEE International Conference on,march 2011, pp. 84 –92.

[15] M. Ben-Or, S. Goldwasser, and A. Wigderson, "Completeness theorems for non-cryptographic fault-tolerant distributed computation."

[16] R. Gennaro, M. O. Rabin, and T. Rabin, "Simplified vss and fast-track multiparty computations with applications to threshold cryptography," in ACM PODC '98, 1998, pp. 101–111.

[17] T. Nishide and K. Ohta, "Multiparty computation for interval, equality, and comparison without bit-decomposition protocol," in PKC'07, 2007, pp. 343–360.