Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 8, August 2014, pg.355 – 360

RESEARCH ARTICLE

Integrally Mysterious Profile Matching Protocols in Mobile Social Networks

Akkanagamma, B.E, (M.Tech), **C.H.Kiran**, B.Tech, M.Tech

Computer Science and Engineering, TITS, JNTU, Hyderabad, TS, India

akku.nara2807@gmail.com , kiran.30.aug@gmail.com

ABSTRACT- In this paper, we study user profile matching with privacy-preservation in mobile social networks (MSNs) and introduce a family of novel profile matching protocols. We first propose an explicit Comparison-based Profile Matching protocol (eCPM) which runs between two parties, an initiator and a responder. 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. We further generalize the iCPM to an implicit Predicate-based Profile Matching protocol (iPPM) which allows complex comparison criteria spanning multiple attributes. The anonymity analysis shows all these protocols achieve the confidentiality of user profiles. In addition, the eCPM reveals the comparison result to the initiator and provides only conditional anonymity; the iCPM and the iPPM do not reveal the result at all and provide full anonymity. We analyze the communication overhead and the anonymity strength of the protocols.

I. INTRODUCTION

Social networking makes digital communication technologies sharpening tools for extending the social circle of people. It has already become an important integral part of our daily lives, enabling us to contact our friends and families on

time. As reported by ComScore, social networking sites such as Facebook and Twitter have reached 82 percent of the world's online population, representing 1.2 billion users around the world. In the meantime, fuelled by the pervasive adoption of advanced handheld devices and the ubiquitous connections of Bluetooth/WiFi/GSM/LTE networks, the use of Mobile Social Networking (MSNs) has surged. 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.

Due to its geographical nature, the MSNs support many promising and novel applications. For example, through Bluetooth communications, People Net enables efficient information search among neighbouring mobile phones; a message-relay approach is suggested in to facilitate carpool and ride sharing in a local region. 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 behaviour of users, such as, social friendship, social selfishness, and social morality. It is encouraging that the traditional solutions can be further extended to solve the MSN problems by considering the unique social features.

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. Research efforts have been put on identity presentation and privacy concerns in social networking sites. Gross and Acquisti argued that users are putting themselves at risk both offline (e.g., stalking) and online (e.g., identity theft) based on a behaviour analysis of more than 4,000 students who have joined a popular social networking site. Stutz man presented a quantitative analysis of identity information disclosure in social network communities and subjective opinions from students regarding identity protection and information disclosure. When the social networking platforms are extended into the mobile environment, users require more extensive privacy-preservation because they are unfamiliar with the neighbours in close vicinity who may eavesdrop, store, and correlate their personal information at different time periods and locations. Once the personal information is correlated to the location information, the behaviour of users will be completely disclosed to the public. Chen and Rahman surveyed various mobile Social Networking Applications (SNAs), such as, neighbourhood exploring applications, mobile-specific SNAs, and content-sharing applications, all of which provide no feedback or control mechanisms to users and may cause inappropriate location and identity information disclosure. To overcome the privacy violation in MSNs, many privacy enhancing techniques have been adopted into the MSN applications. For example, when two users encounter in the MSNs, privacy-preserving profile matching acts as a critical initial step to help users, especially strangers, initialize conversation with each other in a distributed and privacy-preserving manner. Many research efforts on the privacy preserving profile matching have been carried out. The common goal of these works is to enable the handshake between two encountered users if both users satisfy each other's requirement while eliminating the unnecessary information disclosure if they are not. The original idea is from, where an agent of the Central Intelligence Agency (CIA) wants to authenticate herself to a server, but does not want to reveal her CIA credentials unless the server is a genuine CIA outlet. In the meantime, the server does not want to reveal its CIA credentials to anyone but CIA agents.

II. LITERATURE SURVEY

Literature survey is the most important step in software development process. Before developing the tool it is necessary to determine the time factor, economy and company strength. Once these things are satisfied, ten next steps are to determine which operating system and language can be used for developing the tool. Once the programmers start building the

tool the programmers need lot of external support. This support can be obtained from senior programmers, from book or from websites. Before building the system the above consideration r taken into account for developing the proposed system.

III. EXISTING SYSTEM

Privacy preservation is a significant research issue in social networking. The social networking platforms are extended into the mobile environment, users require more extensive privacy-preservation because they are unfamiliar with the neighbors in close vicinity who may store, and correlate their personal information at different time periods and locations. Once the personal information is correlated to the location information, the behavior of users will be completely disclosed to the public. The content-sharing applications, all of which provide no feedback or control mechanisms to users and may cause inappropriate location and identity information disclosure. To overcome the privacy violation in MSNs, many privacy enhancing techniques have been adopted into the MSN applications.

IV. OBJECTIVES

- In this paper, we study user profile matching with privacy-preservation in mobile social networks (MSNs) and introduce a family of novel profile matching protocols.
- The common goal of these works is to enable the handshake between two encountered users if both users satisfy each other's requirement while eliminating the unnecessary information disclosure if they are not.
- We analyze the communication overhead and the anonymity strength of the protocols

V. PROPOSED SYSTEM

We first propose an explicit Comparison-based Profile Matching protocol (eCPM) which runs between two parties, an initiator and a responder. 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. We further generalize the iCPM to an implicit Predicate-based Profile Matching protocol (iPPM) which allows complex comparison criteria spanning multiple attributes. The anonymity analysis shows all these protocols achieve the confidentiality of user profiles. In addition, the eCPM reveals the comparison result to the initiator and provides only conditional anonymity; the iCPM and the iPPM do not reveal the result at all and provide full anonymity. We analyze the communication overhead and the anonymity strength of the protocols.

VI. SYSTEM ANALYSIS

6.1. Feasibility study

The feasibility of the project is analyzed in this phase and business proposal is put forth with a very general plan for the project and some cost estimates. During system analysis the feasibility study of the proposed system is to be carried out. This is to ensure that the proposed system is not a burden to the company. For feasibility analysis, some understanding of the major requirements for the system is essential.

Three key considerations involved in the feasibility analysis are

6.1.1. Technical feasibility study

This study is carried out to check the economic impact that the system will have on the organization. The amount of fund that the company can pour into the research and development of the system is limited. The expenditures must be justified. Thus the developed system as well within the budget and this was achieved because most of the technologies used are freely available. Only the customized products had to be purchased.

6.1.2. Economical feasibility study

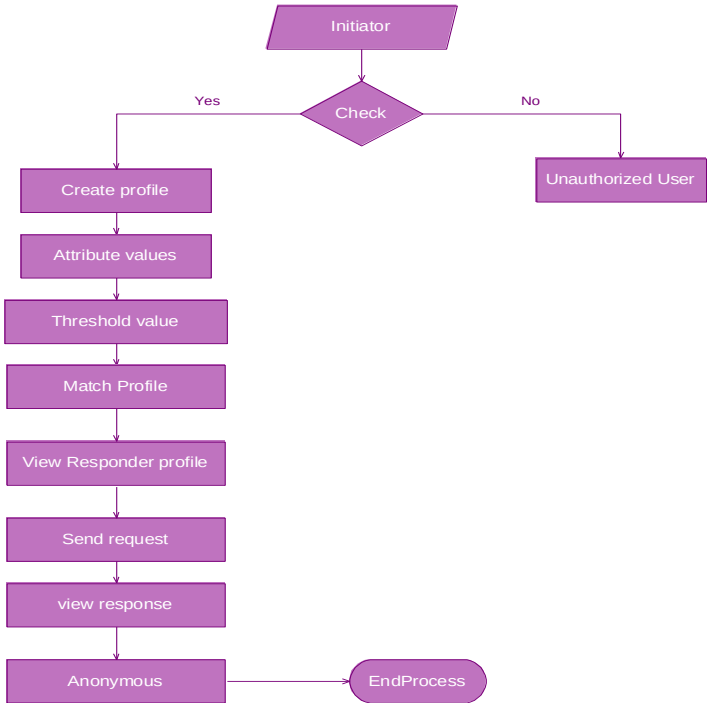
This study is carried out to check the technical feasibility, that is, the technical requirements of the system. Any system developed must not have a high demand on the available technical resources. This will lead to high demands on the available technical resources. This will lead to high demands being placed on the client. The developed system must have a modest requirement, as only minimal or null changes are required for implementing this system.

6.1.3. Operational feasibility study

The aspect of study is to check the level of acceptance of the system by the user. This includes the process of training the user to use the system efficiently. The user must not feel threatened by the system, instead must accept it as a necessity. The level of acceptance by the users solely depends on the methods that are employed to educate the user about the system and to make him familiar with it. His level of confidence must be raised so that he is also able to make some constructive criticism, which is welcomed, as he is the final user of the system.

VII. Data Flow Diagram (DFD's)

The DFD is also called as bubble chart. It is a simple graphical formalism that can be used to represent a system in terms of the input data to the system, various processing carried out on these data, and the output data is generated by the system.



Fig(a): In it I at ofr

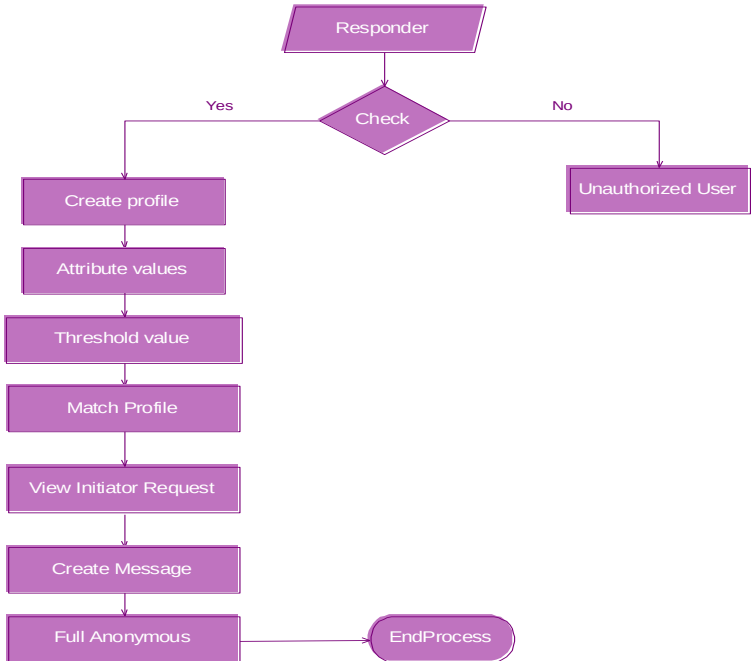


Fig (b): Responder

VIII. CONCLUSION

We have investigated a unique comparison-based profile matching problem in Mobile Social Networks (MSNs), and proposed novel protocols to solve it. The explicit Comparison based Profile Matching (eCPM) protocol provides conditional anonymity. It reveals the comparison result to the initiator. Consider the *k*-anonymity as a user requirement; we analyze the anonymity risk level in relation to the pseudonym change for consecutive eCPM runs. We have also devised two protocols with full anonymity, i.e., implicit Comparison-based Profile Matching (iCPM) and implicit Predicate-based Profile Matching (iPPM). 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. The iCPM and the iPPM both enable users to anonymously request for messages and respond to the requests according to the profile matching result, without disclosing any profile information. 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 "$\geq$" and "$\leq$". Another future work is 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 be of significance for advancing comparison-based family of profile matching protocols and warrants deep

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.

Sites Referred:

http://java.sun.com, http://www.roseindia.com/l, http://www.java2s.com/

