IJRRECS/June 2015/Volume-3/Issue-6/4091-4095 **ISSN 2321-5461**

INTERNATIONAL JOURNAL OF REVIEWS ON RECENT ELECTRONICS AND COMPUTER SCIENCE

AN EXPOSURE TOWARDS PRESERVING OF PRIVACY IN MOBILE SOCIAL NETWORKS

R.Ajay Kumar[1], M.Swathi[2]

[1]M.Tech Student, Dept of CSE, TRR College of Engineering, Hyderabad, T.S, India

[2]Assistant Professor, Dept of CSE, TRR College of Engineering, Hyderabad, T.S, India

ABSTRACT:

In recent times, mobile social networks as a rising platform for social communication have attracted attention. In the applications of mobile social networking, profile matching acts as a significant initial step to assist users in a distributed method. Privacy preservation is regarded as the chief issue in literature in the area of research. In mobile social networking we consider a generalized function to manage information exchange by means of usage of profile matching as a metric. In our work we put forward an explicit Profile Matching procedure based on comparison by conditional anonymity, an implicit Profile Matching protocol based on comparison by full anonymity and an implicit Profile Matching protocol based on Predicate by full anonymity to solve the considered problems of profile matching. Explicit Profile Matching protocol provides simply conditional anonymity and reveals comparison result to initiator. Implicit Profile Matching and Implicit Profile Matching protocol based on Predicate does not disclose the result at all and offer full anonymity.

Keywords: Mobile social networking, Profile Matching, Anonymity, Privacy preservation.

1. INTRODUCTION:

Because of the geographical nature, the practice of mobile social networking manages numerous effective and innovative applications. Several research efforts which are made in literature have been put on advancing the efficacy of communications among users of mobile social networking by

means of realizing the prospective benefits that are brought by mobile social networking [1]. There are several protocols concerning preserving of profile matching procedures privacy in literature and moreover they aspire to determine overall resemblance of two profiles rather than their relation in particular attributes. These protocols do not consider well-built, equivalent, or less important relations of attribute values as matching metrics. They usually make sure whether proximity measure of two profiles is well-built, equivalent, or less important than the value of pre-defined threshold. The protocols of profile matching permit the users to get hold of the profile matching results which enclose partial profile information. The results of profile matching might cause behaviour linkage in assured conditions so that profile information which is revealed will be related to break user anonymity. In our work, we design the protocols for profile matching with conditional anonymity as well as full anonymity. We propose an explicit Profile Matching protocol based on comparison by conditional anonymity, an implicit Profile Matching protocol based on comparison by full anonymity and an implicit Profile Matching protocol based on Predicate by full anonymity [2][3]. Explicit Profile Matching protocol based on comparison runs among two parties, an initiator and a responder and enables the initiator to attain comparison-based matching result with reference to a particular attribute in their profiles, while avoiding their attribute values from disclosing. It provides simply conditional anonymity and reveals comparison result to initiator. Implicit Profile Matching protocol based on comparison allows initiator to directly get hold of some messages rather than comparison result from the responder. It does not disclose the result at all and offer full anonymity. Implicit Profile Matching protocol based on Predicate permits difficult comparison criterion spanning multiple attributes. These entire protocols accomplish the confidentiality concerning user profiles. It does not disclose the result at all and offer full anonymity.

2. OVERVIEW OF MOBILE SOCIAL NETWORKING:

Social networking is considered as an integral unit of our daily lives that mainly allows us to contact friends and families. The mobile applications concerning mobile social network have been developed and put

into practice pervasively. In mobile social networking we consider a generalized function to manage information exchange by means of usage of profile matching as a metric. In mobile applications of social networking, profile matching is initial step to assist users in a distributed method. In mobile social networking users are capable to communicate with peers in secure vicinity by means of restricted wireless communications and they developed specialized data routing as well as forwarding protocol that are connected with social features exhibited from behaviour of users. The conventional solutions can be later extended to resolve the problems of mobile social networking by means of considering exceptional social features [4]. When the platforms of social networking are extended into mobile environment, users necessitate additional extensive privacy-preservation since they are unknown with the neighbours in close vicinity. To prevail over violation of privacy in mobile social networking numerous methods of privacy enhancing were adopted into the applications of mobile social networking. Numerous research efforts on privacy preserving profile matching were carried out and the intention of these works is to facilitate the handshake among two encountered users when both users assures each other's prerequisite while eliminating unnecessary information revelation if they are not [5].

3. AN OVERVIEW OF PROFILE MATCHING PROTOCOLS:

Privacy preservation is considered as an important issue in literature in the area of research. While a lot of personalized information is shared with public, violation of privacy concerning target user have turned out to be much easier. Research efforts have been put on identity presentation as well as privacy concerns in the sites of social networking. In mobile social networking we consider a generalized function to manage information exchange by means of usage of profile matching as a metric. In our work we propose an explicit Profile Matching protocol based on comparison by conditional anonymity, an implicit Profile Matching protocol based on comparison by full anonymity and an implicit Profile Matching protocol based on Predicate by full anonymity to solve the considered problems of profile matching.

These procedures depend mainly on homomorphic encryption to defend content

of user profiles from revelation and mainly they provide rising levels of anonymity. For a particular attribute, the explicit profile matching protocol allows the initiator to attain comparison-based matching result with reference to a particular attribute in their profiles to be exact it has well-built, equivalent, or less important value than the responder on attribute. Due to the revelation of comparison result, user profile will be linked in a number of conditions. Explicit profile matching protocol based on comparison runs among two parties, an initiator and a responder and simply provides conditional anonymity and reveals comparison result to initiator. In the procedure of implicit profile matching protocol based on comparison, the responder prepares numerous categories of messages in which two messages are generated for every category. The procedure allows initiator to directly get hold of some messages rather than comparison result from the responder. It does not disclose the result at all and offer full anonymity. We extend procedure of implicit profile matching protocol based on comparison to obtain Implicit Profile Matching protocol based on Predicate. It permits difficult comparison criterion spanning multiple attributes. These entire protocols accomplish the confidentiality concerning user profiles. It does not disclose the result at all and offer full anonymity. The responder describes a predicate, which is a logical expression that is made of several comparisons among its own attribute values and the initiators attribute values. The initiator obtains one message from responder equivalent to specified category [6]. To receive which message in category is based on whether initiators attribute values convinces the predicate or not.

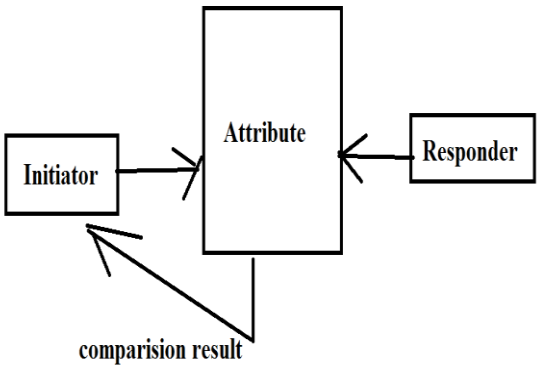

Fig1: A scenario in which attribute values are unknown to initiator and responder and finally initiator gets the comparison result.

4. CONCLUSION:

The applications concerning mobile social network have been developed and put into practice. To succeed over violation of confidentiality in mobile social networking numerous methods of privacy enhancing

were adopted into the applications of mobile social networking. Several efforts in earlier works have been put on identity presentation as well as privacy concerns in the sites of social networking. We recommend an explicit Profile Matching protocol based on comparison by conditional anonymity, an implicit Profile Matching protocol based on comparison by full anonymity and an implicit Profile Matching protocol based on Predicate by full anonymity to solve the considered problems of profile matching. The explicit protocol permits the initiator to attain comparison-based matching result with reference to a particular attribute in their profiles. In implicit procedure, the responder prepares numerous categories of messages in which two messages are generated for every category. We extend practice of implicit protocol based on comparison to obtain Implicit Profile Matching protocol based on Predicate. It permits difficult comparison criterion spanning multiple attributes. These entire protocols accomplish the confidentiality concerning user profiles.

REFERENCES

[1] 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.

[2] 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.

[3] 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.

[4] O. Goldreich, S. Micali, and A. Wigderson, "How to play any mental game or a completeness theorem for protocols with honest majority," in STOC, 1987, pp. 218–229.

[5] I. Ioannidis, A. Grama, and M. J. Atallah, "A secure protocol for computing dot-products in clustered and distributed environments," in ICPP, 2002, pp. 379–384.

[6] I. F. Blake and V. Kolesnikov, "Strong conditional oblivious transfer and computing on intervals," in ASIACRYPT, 2004, pp. 515–529.