AN APPROACH TOWARDS EXPLOITATION OF SOCIAL COMMUNICATIONS IN MOBILE SYSTEMS

MADDALI DHANESH
M.Tech Student, Dept of IT
Sathyabama University
Chennai, T.N, India

PRAKASH JORDAN JENCY.J
Assistant Professor, Dept of IT
Sathyabama University
Chennai, T.N, India

ABSTRACT: **Social network is the networking of communications which bond the people cooperatively and comprise the flow of information connecting people, business connections. Mobile social networks as promising social communication platforms have achieved enormous attention in recent times. Privacy preservation is an important issue of research in social networking. The protection of user's privacy is connected to their profiles and their results of profile matching. The protocols of profile matching allow the users to get hold of the results of profile matching which enclose partial information of profile and can be categorized on the basis of profiles format and the types of matching functions into three classes such as non anonymity, conditional anonymity and full anonymity. A family of novel protocols such as profile matching approaches of explicit comparison-based with conditional anonymity which allows two users to measure up to their values of attribute on a specific attribute devoid of revealing the values to each other; implicit comparison-based the responder organizes numerous categories of messages where two messages are created for each group; and implicit predicate-based with full anonymity permits the comparisons of numerous attributes intended for profile matching were introduced.**

Keywords: **Mobile social networks, Profile matching protocols, User privacy, Anonymity.**

I. INTRODUCTION

Social network is a set of connections, where the entities are consisted by nodes, and the edges consist of the interactions between these entities. In social networking the data is mainly located on a single server makes the access control system weaker by the prevention of the data security. The social websites includes greatly extended range of possible communications, permits us to distribute messages, pictures, and files. In the mobile social networks, users are capable to correspond with peers in close vicinity by means of restricted wireless communications. Mobile social networks hold up numerous promising applications and the current research efforts have been put on to advance the effectiveness of the communications among the users of mobile social networks [4]. Several protocols were developed on specialized data routing in addition to forwarding related with the social features revealed from the user's behaviour. Mobile social networks as promising social communication platforms have achieved enormous attention in recent times and profile matching acts as a significant initial step to assist users, in particular strangers, initialize discussion with each other in a distributed mode [10]. Privacy preservation is an important issue of research in social networking shown in fig1. In view of the fact that more personalized data is shared with the public, violating the confidentiality of a target user turns out to be much easier. There are quite a lot of existing schemes of homomorphic encryption that support several operations such as addition as well as multiplication on ciphertexts [8]. To triumph over the privacy violation of privacy in mobile social networks, numerous techniques of privacy enhancing have been adopted into the applications of mobile social networks. The protection of user's privacy is connected to their profiles and their results of profile matching. The protocols of profile matching allow the users to get hold of the results of profile matching which enclose partial information of profile [1] [6]. The results of profile matching may possibly cause behaviour linkage in assured conditions such that the exposed profile information will be related to break anonymity of the user. The profile matching can be categorized on the basis of profiles format and the types of matching functions into three classes such as non anonymity, conditional anonymity and full anonymity [11]. A protocol of profile matching providing non-anonymity if after attackers carrying out numerous runs of the protocol with a user, the probability of accurately estimating the user profile equals to 1. A profile matching protocol attains conditional anonymity if after attackers carrying out numerous runs of the protocol with a user, the probability of exactly estimating the user profile is larger than $1/v$. A protocol of profile matching attains full anonymity if after attackers carrying out numerous runs of the protocol with a user, the probability of accurately estimating the profile of the user is regularly $1/v$ [3] [13]. In the homogenous mobile social networks consisting of N mobile users having equivalent range of wireless communication which is bi-directional was considered. The technique of multi-pseudonym was accepted to preserve user identity and privacy of location. A Trusted Central Authority is made used for bootstrapping however not concerned in user communication.

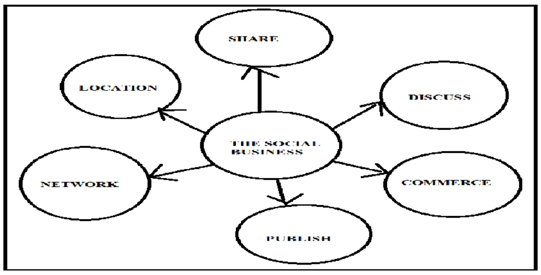

Fig 1: An overview of social networking

II. METHODOLOGY

There are quite a lot of existing schemes of homomorphic encryption that support several operations such as addition as well as multiplication on ciphertexts. A user is competent to process the encrypted plaintext devoid of making out the secret keys and due to this property; the schemes of homomorphic encryption are extensively used in aggregation of data and computation explicitly for privacy-sensitive content [14]. The model of Autoregressive is a classic tool intended for understanding and forecasting a series of time data and is often combined with the model of Moving-Average to obtain complex model of Autoregressive Moving Average which is intended for generally improved accurateness. A family of novel protocols such as profile matching approaches of explicit comparison-based with conditional anonymity, implicit comparison-based and implicit predicate-based both with full anonymity were introduced which rely on the homomorphic encryption to defend the content of user profiles from revelation and present increasing levels of anonymity [9]. The protocol of explicit comparison-based profile matching allows two users to measure up to their values of attribute on a specific attribute devoid of revealing the values to each other. However, the protocol reveals the assessment consequence to the initiator, and as a result presents conditional anonymity. The protocol has an essential phase of bootstrapping, where the trusted central authority makes all the parameters of the system, user pseudonyms in addition to keying materials and moreover generates a pair of private key: which is a secret key used to issue certificates intended for user pseudonyms as well as keying materials; and public key: which is open to all users [5] [7]. The trusted central authority makes disjoint sets of homomorphic public keys and moreover disjoint sets of pseudonyms for users. In the approach of implicit comparison-based, the responder organizes numerous categories of messages where two messages are created for each group. The initiator can get hold of only one message associated to one category intended for each run. Throughout the protocol, the responder is not capable to make out the type of the initiator's attention. Receiving of message in the category is reliant on the result of comparison on a specified feature. The responder does not make out the message which was received by the initiator, although the initiator cannot obtain the result of comparison from the received message [2] [15]. The approach of implicit comparison-based profile matching was extended to attain implicit predicate-based profile matching which has the identical anonymity property as the implicit comparison-based profile matching. The implicit Comparison-based Profile Matching and implicit Predicate-based Profile Matching facilitates users to anonymously appeal for messages and act in response to the requests in accordance with the result of profile matching, devoid of disclosing any profile information [12]. The implicit predicate-based profile matching permits the comparisons of numerous attributes intended for profile matching. The responder describes a predicate, which is a logical expression made of numerous comparisons among its own values of attribute and the initiator's values of attribute. The initiator accepts one message from the responder in relation to the specific category. Receiving of message in the category relies on the attribute values of initiator satisfying the predicate or not.

III. RESULTS

Two protocols with full anonymity such as implicit Comparison-based Profile Matching and implicit Predicate-based Profile Matching were devised. The implicit Comparison-based Profile Matching and implicit Predicate-based Profile Matching make available full anonymity. The implicit Comparison-based Profile Matching handles profile matching based on a single assessment of an attribute whereas the implicit Predicate-based Profile Matching is put into practice by means of a logical expression made of numerous comparisons spanning multiple attributes. The implicit Comparison-based Profile Matching and implicit Predicate-based Profile Matching facilitates users to anonymously appeal for messages and act in response to the requests in accordance with the result of profile matching, devoid of disclosing any profile information.

IV. CONCLUSION

Social networks are mostly helpful, and maintain social relationships mutually online and offline, while the users are using them their information may be available to the people who want to make a mess of it. To triumph over the privacy violation of privacy in mobile social networks, numerous techniques of privacy enhancing have been adopted into the applications of mobile social networks. A family of novel protocols such as profile matching approaches of explicit comparison-based with conditional anonymity, implicit comparison-based and implicit predicate-based both with full anonymity were introduced. These protocols rely on the homomorphic encryption to defend the content of user profiles from revelation and present increasing levels of anonymity.

REFERENCES

[1] 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.

[2] R. Lu, X. Lin, H. Luan, X. Liang, and X. Shen, "Pseudonym changing at social spots: An effective strategy for location privacy in vanets," *IEEE Trans. Veh. Technol.*, vol. 61, no. 1, pp. 86 – 96, 2011.

[3] R. Lu, X. Lin, X. Liang, and X. Shen, "A secure handshake scheme with symptoms-matching for mhealthcare social network," *ACM Mobile Networks and Applications (MONET)*, vol. 16, no. 6, pp. 683–694, 2011

[4] G. Chen and F. Rahman, "Analyzing privacy designs of mobile social networking applications," *IEEE/IFIP International Conference on Embedded and Ubiquitous Computing*, vol. 2, pp. 83–88, 2008.

[5] 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.

[6] 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.

[7] E.Bulut and B.Szymanski, "Exploiting friendship relations for efficient routing in delay tolerant mobile social networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 23, no. 12, pp. 2254–2265, 2012.

[8] D. Balfanz, G. Durfee, N. Shankar, D. K. Smetters, J. Staddon, and H.-C. Wong, "Secret handshakes from pairing-based key agreements," in *IEEE Symposium on Security and Privacy*, 2003, pp. 180–196.

[9] C. Hazay and Y. Lindell, "Efficient protocols for set intersection and pattern matching with security against malicious and covert adversaries," *J. Cryptology*, vol. 23, no. 3, pp. 422–456, 2010.

[10] 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.

[11] R. Lu, X. Liang, X. Li, X. Lin, and X. Shen, "Eppa: An efficient and privacy-preserving aggregation scheme for secure smart grid communications," *IEEE Trans. Parallel Distrib. Syst.*, vol. 23, no. 9, pp. 1621– 1631, 2012.

[12] 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.

[13] D. Niyato, P.Wang, W. Saad, and A. Hjørungnes, "Controlled coalitional games for cooperative mobile social networks," *IEEE Trans. Veh. Technol.*, vol. 60, no. 4, pp. 1812–1824, 2011.

[14] 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.

[15] X. Liang, X. Li, T. H. Luan, R. Lu, X. Lin, and X. Shen, "Moralitydriven data forwarding with privacy preservation in mobile social networks," *IEEE Trans. Veh. Technol.*, vol. 7, no. 61, pp. 3209–3222, 2012.