A SURVEY ON SECURE AND PRIVACY IN SOCIAL NETWORK WITH GROUP MATCHING TECHNIQUES

Sneha k.Wahane[1], Prof. Jayant Rohankar [2]

Department of CSE, TGPCET, RTM Nagpur University, Nagpur, India

Email: rani.wahane10@gmail.com

Assistant Professor, Department of CSE, TGPCET, RTM Nagpur University, Nagpur, India

Email: jayant_rohankar@gmail.com

Abstract— Groups are commonly used in social networks. In order to choose a suitable group to join, a stranger who is still outside of a group may have the need to figure out matching information about the attributes of all the group members based on its own attributes. However, privacy is one of the most important issues, how can we allow the stranger to find out matching information between itself and a group without gaining private attributes is a challenging task. In this paper, we propose secure and privacy-preserving group matching scheme, where the privacy of both a stranger and group members in social networks are preserved. By leveraging attribute based group signatures, stranger is able to collect exact matching information while the private information of this stranger and group members are not revealed. Batch verification is proposed to significantly improve efficiency of the matching process.

Index Terms— Group Signature, Batch Verification, Attribute Based Group Signature.

1 INTRODUCTION

Groups are commonly used in online social network such as Face book and Twitter. Groups are collection of users with their attributes and resources. The need of groups, people are able to easily access to comments and description that they are more interested in based on their attributes. In order to share those comments and description of a group, a stranger, who is outside a group, would like to find an interested group to join.

Unfortunately, the description of a group may sometimes only contain a few keywords, which is difficult for a stranger to make better decision. This situation is more serious when several groups have similar description. Imaging you join ten similar groups, and always receive and check same news notified by ten different emails. To overcome this issue and make a better evaluation of a group, the stranger can collect matching information from all the members of a group based on his own attributes, which is referred to as group matching [1]. Unfortunately, since users concern about the privacy of their attributes and prefer to store these attributes privately [2], directly revealing personal attributes and enabling the collection of matching information will introduce several private issues [1, 2, 8].

First of all, since the stranger is still not familiar with a group, it is reluctant to disclose its sensitive attributes to any group member in the process of group matching. Likewise, because the stranger is an outsider of a group, group members do not fully trust this stranger and do not want to reveal personal private attributes to the stranger during group matching. Moreover, in order to convince the stranger the correctness of matching information, each group member also needs to compute verification metadata (i.e., signatures) on it. However, due to the enforceability of signatures, where only the entity with the knowledge of the private Key is able to generate valid signatures; the stranger is even able to learn the exact matching information between itself and each particular group member after verifying the correctness of matching information [3]. Since this stranger is still an outsider of the group and not fully trusted by any group member, this leakage of exact matching information clearly discloses more private information to the stranger during group matching. Recent work [1] provided a solution to support private-preserving group matching without revealing private information mentioned above. However, this previous scheme is not suitable and efficient for groups with a large number of users. The main reason is that the design of this scheme is based on ring signatures [9]. In this paper, we propose an efficient group matching scheme in social networks based on attribute based group signatures [14].

We proposed scheme, the privacy of both the stranger and group members can be protected. Efficiently a stranger is able to access matching information from each group member without revealing its own attributes to group members. In addition, the properties of attribute based group signatures [14], a stranger is convinced that those matching information is gain from group members, but it is not able to learn exact matching information between stranger and group member. With the method of batch verification on group signatures, the stranger is able to securely verify valid verification multisets from multiple group users.

2. Literature Survey:-

Various methods to deal with secure privacy preserving group matching in social network have been proposed.

2.1 Ring Signature:-

R. L. Rivest, A. Shamir, and Y. Tauman [9] Formalize the notion of a ring signature which makes it possible to specify a set of possible signers without revealing which member actually produced the signature. Verification must satisfy the usual soundness and completeness conditions but in addition we want the signature to be signer ambiguous in the sense that the sense that the verifier should be unable to determine the identity of the actual signer in a ring signer should able to assemble an arbitarig ring without any coordination with the other ring members.

2.2 Privacy Preserving Techniques:-

Michael J. Freedman, Kobbi Nissim and Benny Pinkas formalize the problem to maintain security of private input sets of users. No party learns more information about other parties' private input sets. Design efficient, secure and compassable method of the union, intersection and element reduction operations [7,8]. It provides efficient solution for private multiparty intersection set secure against malicious stranger. It prevents private input multisets without gaining any other information. Private set intersection protocol proposed against with malicious adversary model and Honest-but-curious adversary model.

Michael J. Freedman, Kobbi Nissim and Benny Pinkas [8] consider the problem of private intersection of private input multisets. Multiparty learn the intersection of all private input multisets without gaining any other information. For this problem it suggests (HBC) Honest- But-Curious adversaries.

2.3 Group Signature:-

In group-oriented signature, nobody besides the designated group can verify the signature. Group signature with limited verification range is necessary in some instances.

Chunbo Ma and Jun Ao overcome the problem in ring signature. Group signatures are useful when the members want to cooperate and setup procedure for group matching. Group manager maintains identity of the real singers of a valid signature. Group signature method is providing large size key for large group.

2.4 User Profile Matching Techniques:-

Elie Raad, Richard Chbeir and Albert Dipanda formalize the problem of matching user profiles by providing a suitable matching framework able to consider all the profile's attribute [9]. Investigating the same person between two social networks whether two profiles refer to the same person or not. The selection of suitable profiles scores on higher than threshold matching value. The decision of Profile matching is computed by using decision making algorithm.

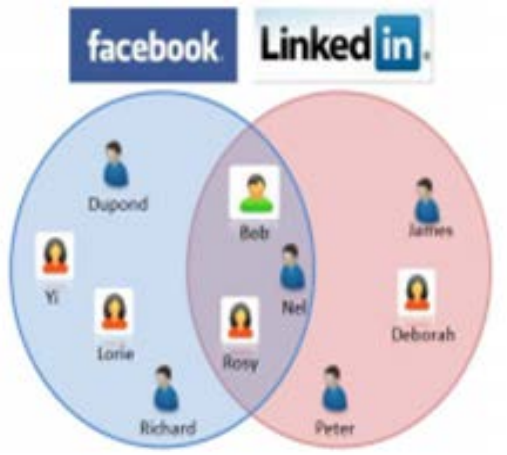

Fig.2.4.1 Social Network of Bob within Face book and LinkedIn

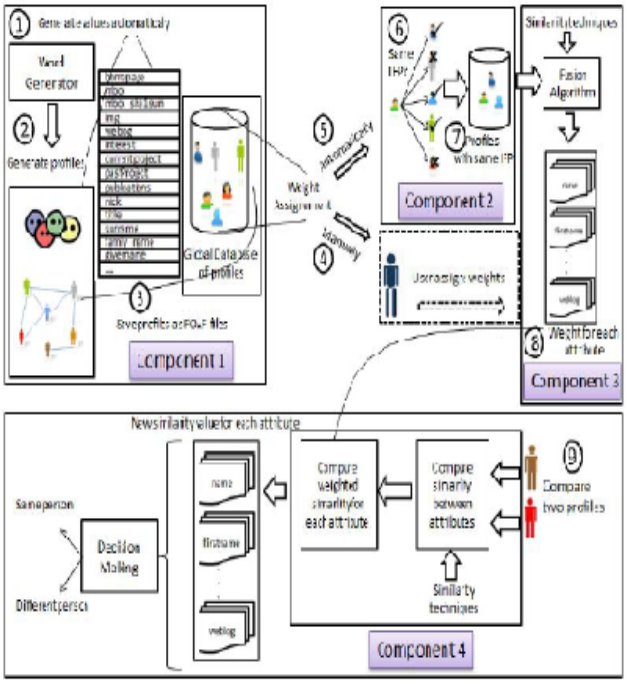

Fig.2.4.2 Prototype Architecture

Prototype architecture based on Profile generator which is used to generate random social network profiles with different or similar attributes. Profile retriever: is used to extract profiles having the initial set of profiles. Weight assignment: is used to assign manually each attribute in the user profile to their weight. Profile matcher: returns the decision whether the two compared profiles are the same or not which is based on decision making algorithm [10].

2.5 Batch Verification:

Gregory M. Zaverucha and Douglas R. Stinson formalize a batch verification algorithm for attribute based group signature scheme verifies a list of n (message, predicate) pairs as a group. It outputs 1 if all n signatures are valid, and it outputs 0 if one or more are invalid [13]. Batch verification algorithms may provide large gains in efficiency, as verification of the n signatures is significantly faster than individual verifications .Batch verification algorithm is finding the invalid signatures which caused the batch to fail.

2.6 Privacy Preserving Personal Profile Matching Technique:-

Ming Li, Ning Cao, Shucheng Yu and Wenjing Lou proposed stranger can find from a group of users the one whose profile best matches with participants to limit the risk of privacy exposure , only necessary and minimal information about the private attributes of the participating users is exchanged[2].

In mobile social network, user finds best matching privately and directly and connect each other without revealing private infor-

mation. Secure and privacy preserving in a profile matching formalize intersection protocol which includes the intersection set of profile attributes and Honest-but-Curious (HBC) model can prevent several key malicious attacks.

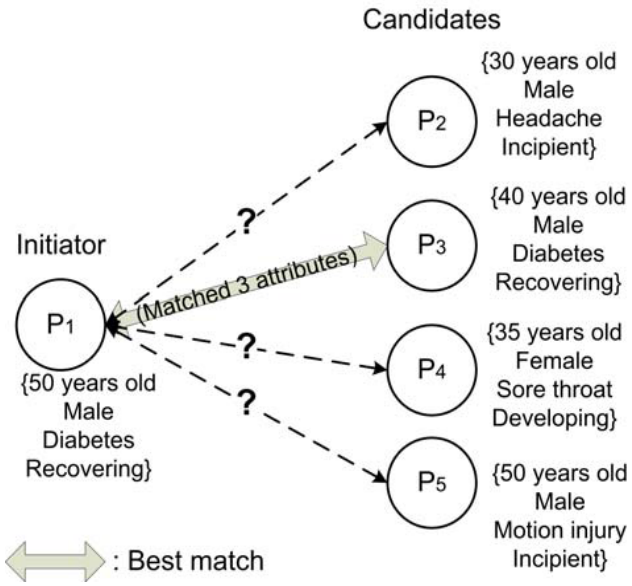

Fig 2.5 private profile matching in MSN

2.7 Attribute Based Group Signature:

Attribute Based Group Signature (ABGS) is a new cryptography generation of group signatures. The verifier request from the signer that they own certain attributes. Strangers start building l an attribute tree on the basis of threshold matching value. An attribute tree is a tree in which each interior node is a threshold gate and the leaves are linked with attributes. A threshold gate represents that the number m of n children branching from the current node need to be satisfied for the parent to be considered satisfied. Satisfaction of a leaf is achieved by owning an attribute [14]. Dalia Khader formalizes first ABGS and proves it to be secure against SSA and UTA attacks. Its step would be to have signatures and keys within our scheme, independent on the attributes.

3. Challenges for Group Matching Technique:-

We have used attribute based group signature and batch verification for preventing private information of users in group matching. We design an attribute tree whose checks threshold matching value. The threshold matching value based on a percentage of matching attributes. We improve efficiency of group matching by batch verification.

In social network group is most common features. Stranger checks to get suitable group and join with best group without gaining private information. Group matching formalize on the basis of percentage of matching attributes of users. Secure and privacy preserving group matching proposed attribute based group signature.

4. Conclusion:-

This paper proposes group matching techniques which formalize private multisets, private input sets, private attributes and stranger's privacy without gaining private information. We overcome the problem in privacy concern and propose secure and efficient group matching in social network. More secure and privacy preserving group matching proposes attribute based group signature and batch verification in social networks.

References:-

[1] Boyang Wang, Baochun Li and Hui Li, "Gmatch: Secure and Privacy-Preserving Group Matching in Social Networks", *in Proc. IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING, 2013, pp. 1-6.*

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

[3] A. Sorniotti and R. Molva, "Secret Interest Groups (SIGs) in Social Networks with an Implementation on Facebook," *in Proc. ACM SAC, 2010, pp. 621–628.*

[4] D. Dachman-Soled, T. Malkin, M. Raykova, and M. Yung, "Efficient Robust Private Set Intersection," *in Proc. International Conference on Applied Cryptography and Network Security. Springer-Verlag, 2009, pp. 125–142.*

[5] R. Li and C. Wu, "An Unconditionally Secure Protocol for Multi-Party Set Intersection," *in Proc. ACNS. Springer-Verlag, 2007, pp. 226–236.*

[6] Y. Sang, H. Shen, Y. Tan, and N. Xiong, "Efficient Protocols for Privacy Preserving Matching Against Distributed Datasets," *in Proc. ICICS. Springer-Verlag, 2006, pp 210-227.*

[7] L. Kissner and D. Song, "Privacy-Preserving Set Operations," *in Proc.CRYPT. Springer Verlag, 2005, pp. 241–257.*

[8] M. J. Freedman, K. Nissim, and B. Pinkas, "Efficient Private Matching and Set Intersection," *in Proc. EUROCRYPT. Spring-Verlag, 2004, pp.1–19.*

[9] R. L. Rivest, A. Shamir, and Y. Tauman, "How to Leak a Secret," *in Proc. ASIACRYPT. Springer-Verlag, 2001, pp. 552–565.*

[10] Elie Raad, Richard Chbeir and Albert Dipanda, "User Profile Matching in Social Networks," *International conference on network based information systems(NBiS),2010,pp.1-8.*

[11] R. Agrawal, A. Evfimievski, and R. Srikant, "Information Sharing

Across Private Databases," *in Proc. ACM SIGMOD, 2003, pp. 86–97.*

[12] D. Boneh, C. Gentry, B. Lynn, and H. Shacham, "Aggregate and Verifiably Encrypted Signatures from Bilinear Maps," *in Proc.EUROCRYPT. Springer-Verlag, 2003, pp.416- 432.*

[13] Gregory M. Zaverucha and Douglas R. Stinson, "group testing and batch verification,"*2009,pp1-18.*

[14] Dalia Khader, "Attribute Base Group Signature,"inProc.iacr, 2007, pp1-18.

IJSER