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. 5, May 2014, pg.506 – 514

SURVEY ARTICLE

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

RESHMA ZUNKE GUIDE:-AMIT PIMPALKAR

M.TECH IV SEM

G.H. RAISONI ACADEMY OF INSTITUTE AND ENGINEERING

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

ABSTRACT

Groups are becoming one of the most compelling features in both online social networks and Twitter-like microblogging services. A stranger outside of an existing group may have the need to find out more information about attributes of current members in the group, in order to make a decision to join. However, in many cases, attributes of both group members and the stranger need to be kept private and should not be revealed to others, as they may contain sensitive and personal information. How can we find out matching information exists between the stranger and members of the group, based on their attributes that are not to be disclosed? In this paper, we present a new group matching mechanism, by taking advantage private set intersection and ring signatures. With our scheme, a stranger is able to collect correct group matching information while sensitive information of the stranger and group members are not disclosed. Finally, we propose to use batch verification to significantly improve the performance of the matching process.

1. INTRODUCTION

As online social networks and Twitter-like micro-blogging services redefine our lifestyle, groups are becoming one Of the most frequently used features. Groups are, in general, formed with common attributes, such as geographic locations and hobbies. However, the features of a group are generally described by only a few keywords or a short description, which sometimes is not enough for users to make decisions when choosing an appropriate Especially, when several groups have similar (or even the same) keywords and descriptions, it is very inconvenient for users to choose the most suitable one among these groups. In order to make a better decision when choosing a group to join, a stranger with a profile of his own attributes — who is still an outsider of the group — needs to collect detail matching information from all the group members' profiles. Such a problem is referred as to group matching. In most situations, attributes of users are sensitive, such as personal health records and religious preferences. It is typical for a user to store these attributes privately so that only his friends or members in the same group are able to reveal these attributes, but strangers or any third party cannot learn these sensitive information. Unfortunately, collecting group matching information using these sensitive attributes may introduce a number of privacy problems. On one hand, since the stranger is not familiar with the group, the stranger does not want to reveal his sensitive attributes to any group member during the matching process. On the other hand, because the stranger is an outside and untrusted user to the group, each group member is reluctant to reveal his own attributes and the exact matching results between two entities to the stranger. To make matters more challenging, each group member needs to generate a signature on his matching response, which contains matching information between the stranger and himself, and sends the signature and the matching response.

2. PROBLEM STATEMENT

System Model Our system is a social network, which includes a stranger S and all d group members P1, ..., Pd in the group P (as shown in Fig. 1). The stranger S, who is not a member of the group P,has k attributes in his profile and the j-th attribute is denoted as as,j . The stranger's profile is denoted as As = {as,1, ..., as,k}. Group member Pi has m attributes and the profile of this group member is denoted as Ai = {ai,1, ..., ai,m}. In our model, we assume all group members have the same size of profile. Attributes in every user's profile are private and sensitive, which are stored and maintained locally by each user. Note that we also assume there does not exist of a third party that first collects all the group members' profiles, and then simply completes group matching between itself and the stranger. Even if there exists a group manager who maintains basic activities of the group, such as the changes of membership, it is still not able to access sensitive attributes of group members. The stranger completes group matching in

B. Privacy Threats:-

In this paper, we assume the stranger is honest-but - curious. It means the stranger will honestly follow the protocol to collect group matching information, but may attempt to learn more information than allowed.

C. Design Objectives

During the group matching, our scheme should be able to provide the following desirable privacy properties. (1)

1)Stranger’s Attributes Privacy: The stranger does not reveal any attribute in his profile to any group member.

(2) Group Members’ Attributes Privacy: The stranger only obtains matched attributes that both in his profile and some group member’s profile, while the unmatched attributes in group members’ profiles are not disclosed to the stranger.

(3) Exact Matching Information Privacy: The stranger is able to compute group matching information, while any exact matching information between himself and each group member is not revealed.

3. PRELIMINARIES

In this section, we briefly introduce cryptographic primitives that we implement in Gmatch.

A. Bilinear Maps

Let G1, G2 and GT be three multiplicative cyclic groups of prime order p, g1 be a generator of G1, and g2 be a generator of G2. A bilinear map e is a map G1 × G2 ! GT with the following properties:

(1) Computability: there exists an efficient algorithm for computing map .

(2) Bilinearity: for all u 2 G1, v 2 G2 and a, b 2 Zp, e(ua, vb) = e(u, v)ab.

(3)Non-degeneracy: e(g1, g2) 6= 1.

B. Ring Signatures:-

The concept of ring signatures was first proposed by Rivest . A ring signature scheme has the property that, a verifier is convinced that a ring signature was produced using one of group members' private keys, but this verifier is not able to determine which one.

C. Private Set Intersection:-

Private set intersection [2], [6], [7] enables two parties to calculate the intersection of their private sets without leaking any additional information. Private set intersection can be construct using additive homomorphic encryption, such as Paillier cryptosystem [8]. The additive homomorphic encryption algorithm Enc(·) is able to complete following operations, without knowing the corresponding plaintexts.

- Given Enc(m1) and Enc(m2), output Enc(m1+m2) = Enc(m1) · Enc(m2).

- Given Enc(m1) and a constant c, output Enc(c ·m1) = Enc(m1)c.

4. GMATCH: SECURE AND PRIVACY-PRESERVING GROUP MATCHING

A. Overview

In this section, we introduce Gmatch, a secure and privacy preserving group matching scheme. By utilizing private set intersection, the stranger can learn the matching information from the group without revealing any unmatched attributes in group members' profiles. With ring a signature, the stranger is convinced that a matching response is correct and generated by a group member, yet cannot distinguish this matching response belongs to which particular group member. Exploiting the properties of bilinear maps, Gmatch can support batch verification, which is able to greatly improve the efficiency of verification of ring signatures. In addition, with minor modifications in the construction of Gmatch, we can achieve even higher privacy levels.

Gmatch includes four steps:

Setup, ***Compute***, ***Evaluate***, ***Match***. In ***Setup***, stranger S and each group member generate their own public/private key pairs. In ***Compute***, stranger S first generates a polynomial, where each attribute in his profile is a root of this polynomial and all the roots are in his profile Then, stranger S encrypts all the coefficients of this polynomial by performing additive homomorphic encryption, and sends all the encrypted coefficients to all the group members .In Evaluate, each group member evaluates a matching value for each attribute in his own profile using all the encrypted coefficients, signs a matching response that contains all the matching values generated by himself, and sends this matching response and the corresponding signature to the stranger. In Match, stranger S first checks the correctness of a matching response by verifying its signature, then computes whether each matching value in this matching response indicates a matched attribute. After collecting all the matching responses from all group members, the stranger S calculates matching degrees for all the attributes in his profile. Details of each

Step are listed as follows.

Setup. Stranger S generates his public/private key pair (pks, sks) for additive homomorphic encryption. Here, we utilize Paillier cryptosystem [8]. The encryption algorithm is denoted as Enc, and the corresponding decryption algorithm is denoted as Dec. Each group member generate his public/private key pair (pk i, ski) for computing ring signatures. The ring signature scheme we used is which is based on bilinear maps. The total number of group members is d. The number of attributes in the stranger's profile is k, and the number of attributes in each group member's profile in m.

Compute. Stranger S first constructs a k-degree polynomial P(x), whose k roots are all attributes in his profile. This polynomial is described as:

P(x) = (x − as,1)(x − as,2) . . . (x − as,k) = Xk

i=0i xi. Clearly, if an attribute ai,j from group member Pi is a matched attribute that equals some attribute in stranger S's profile, then ai,j is also a root of this k-degree polynomial P(x), and we

have P(ai,j) = 0. After generating polynomial P(x), stranger S encrypts all the k+1 coefficients of this polynomial P(x) using Enc with his public key pks. He then sends all the k + 1 encrypted coefficients {Enc(0), ..., Enc(k)} to each group member.

Evaluate. Group member Pi has m attributes and evaluates a matching value wi,j for each attribute ai,j in his profile. More specifically, group member Pi first computes an encrypted polynomial value Enc (P (ai,j)) for each attribute ai,j . Due to properties of additive homomorphic encryption we introduced in Section III, this encrypted polynomial value Enc(P(ai,j)) can be easily computed by Pi's attribute ai,j and all the encrypted coefficients Enc(i), for i 2 [0, k], as follows:

Enc(P(ai,j))= Enc(0 + 1ai,j + · · · + kaki,j)

= Enc(0) × Enc(1)ai,j × · · · × Enc(k)a

Match:- Upon receiving a matching response wi and its ring signature i, stranger S first verifies the correctness of this matching response matching response passes the verification, stranger S decrypts each wi,j 2 wi with decryption algorithm Dec. If the result of decryption matches one of his attributes, then ai,j is a matched attribute. Otherwise, it is an unmatched attribute. This is because

Dec(wi,j) = Dec(Enc(i,j · P(ai,j) + ai,j))

= i,j · P(ai,j) + ai,j where P(ai,j) = 0 and Dec(wi,j) = ai,j , if ai,j 2 Ai,j C.

Batch Verification:-

Generally, the stranger in Gmatch has to verify d matching responses from all the d group members separately, which introduces prohibitive huge computation cost to himself. Utilizing properties of bilinear maps, the stranger can reduce the cost of verification by checking the integrity of all the matching responses in a batch manner, instead of verifying them one by one. still pass verification, we can leverage binary search during batch verification. More specifically, when batch verification fails, the stranger further divides the set of all the matching responses into two halves, and rechecks each half using batch verification. If one half passes, all the matching responses in this half are valid. Otherwise, two sub halves of this half will be further rechecked.

Higher Privacy Levels:-

There are two ways to modify the construction of Gmatch, so that it can achieve even higher privacy levels. First, similar to the previous work [2], each matching value is computed as wi,j = Enc(i,jP(ai,j)) instead of wi,j = Enc(i,jP(ai,j))+ ai,j . Then, when the decryption result is 0, it means that there is a matched attribute in the group. However, the stranger cannot determine which particular attribute in his profile is matched to this attribute.

SECURITY ANALYSIS:-

In this section, we show that Gmatch is able to achieve the privacy properties we defined in Section II.

Theorem 1: Assuming that the additive homomorphic encryption is semantically secure, Gmatch achieves stranger attributes privacy.

Proof: In Gmatch, group member Pi obtains k + 1 encrypted coefficients of polynomial P(x) computed by additive homomorphic encryption algorithm Enc. If the additive homomorphic encryption Enc is semantically secure [8], it is computational infeasible for the group member to derive any plaintext when given only its corresponding ciphertext and public encryption key pks. Because Paillier cryptosystem, which we use in Gmatch, is semantically secure. Then, given encrypted coefficients {Enc(0), . . . , Enc(k)} and public encryption key pks, group member Pi cannot learn{0, . . . , k} without the stranger's private key sks. Further, group member Pi is not able to reconstruct the polynomial P(x) and compute all the k roots of P(x). Therefore, all the k attributes in stranger' profile are not revealed member, stranger's attributes privacy is achieve.

PERFORMANCE:-

1) Efficiency of Gmatch: As we can see from and the efficiency of group matching can be significantly improved by utilizing batch verification. More specifically, when the size of users' profiles are fixed the rum time of Gmatch without batch verification exponentially increases with the total number of group members, while the one with batch verification only increases linearly with the group size.
2) Efficiency of Batch Verification with Invalid Matching Responses: We now evaluate the performance of batch verification under different numbers of invalid matching responses Clearly, the increasing number of invalid responses.

RELATED WORK:-

A. Two-party private matching:-

In this paper proposed a private matching scheme, which allows a client and a server compute the set intersection with their own private sets. During private matching, the client only obtains the set intersection while the server does not know any m Agrawal et al. introduced a private matching scheme between two databases using commutative encryptions. Hazay and Lindell exploited pseudo random functions to evaluate set intersection. In Dachman -Soledet al. exploited polynomial evaluations to compute the set intersection between two parties, and also leveraged Shamir secret sharing and cut-and-choose protocol to improve efficiency .matching result Recent work in introduced an authorized private set intersection (APSI) based on blind AES signatures. In APSI, each element in the client's set must be authorized by some mutually trusted authority.

B. Multi-party private matching:-

In this paper proposed a multi-party private matching scheme to compute the union, intersection and element reduction operations for multiple sets. However, this scheme requires a group decryption among multiple entities, which is impractical between the stranger and group members in social networks. Ye et al extended previous scheme to a distributed scenario with multiple with their own private sets. During private matching efficiency of batch verification. In this experiment, we set the total number of matching responses. The dataset of the original server is shared by several sub-servers using shamir secret sharing. proposed a private multi-party set intersection scheme based on the two-dimensional verifiable secret sharing scheme.

C. Private matching in social networks:-

In this paper focuses on finding the best matched user from the group in mobile social networks. Yang et al. introduced E-SmallTalker, which allows users to privately match other people in mobile social networks using the iterative bloom filter (IBF) protocol.

5. CONCLUSION

In this paper, we proposed Gmatch, a secure and privacy preserving group matching in social networks. With Gmatch, the stranger can successfully collect group matching information while the private information of group members are preserved. Our experimental results show that Gmatch can efficiently compute correct group matching information with batch verification.

ACKNOWLEDGEMENT:-

We are grateful to the anonymous reviewers for their helpful comments. This work is supported by the National Science and Technology Major Project Fundamental Research Funds for Central Universities Doctoral Foundation of Ministry of Education of (No. 20100203110002) and Program for Changjiang Scholars and Innovative Research Team.

REFERENCES

1) 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.

2) M. J. Freedman, K. Nissim, and B. Pinkas, “Efficient Private Matching and Set Intersection,” in Proc. EUROCRYPT. Spring-Verlag, 2004, pp.1–19.

3) R. L. Rivest, A. Shamir, and Y. Tauman, “How to Leak a Secret,” in Proc. ASIACRYPT. Springer-Verlag, 2001, pp. 552–565.

4) 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.

5) 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.