International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

COPY RIGHT

IJIEMR Transactions, online available on 16th July 2017. Link :
http://www.ijiemr.org/downloads.php?vol=Volume-6&issue=ISSUE-5

Title: Survey on Asymmetric Social Proximity Based Private Matching Protocols For Online Social Networks.

Volume 06, Issue 05, Page No: 1848 – 1853.

Paper Authors

*** MISS PRIYANKA PATIRAM SHAHARE, MISS.GUNJAN AGRE.**

* Dept of CSE, Nagpur Institute of Technology,Nagpur.

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

ASYMMETRIC SOCIAL PROXIMITY BASED PRIVATE MATCHING PROTOCOLS FOR ONLINE SOCIAL NETWORKS

***MISS PRIYANKA PATIRAM SHAHARE,**MISS.GUNJAN AGRE**

* PG Scholar, Dept of CSE, Nagpur Institute of Technology, Nagpur.
**Asst.Professor, Dept of CSE, Nagpur Institute of Technology, Nagpur.

ABSTRACT

—Online Social Networks (OSNs) have had rapid growth over the past few years. Some works are based on similar profile attributes. However, profile matching involves a very high privacy risk of exposing private profile information to strangers in the cyberspace. In the existing asymmetric Social proximity calculation, three protocols are used to provide privacy. The proposed method provides an improved asymmetric social proximity measure between two users. Community structures are used to redefine the OSN model. The proposed method protect user's privacy better than the previous works. Finally, validation of proposed method is compared with mutual friends and proximity measure. The results show the efficacy of our proposed proximity measure.

Keywords: Online Social Networks, Profile matching, Asymmetric social proximity.

I. INTRODUCTION

The concept of social networks was first introduced by J.A. Barnes [1954], who describes them as connected graphs where nodes represent entities and edges their interdependencies. Entities could be individuals, groups, organizations, or government agencies. The edges could be interactions, invitations, trades, values, etc.

Social network sites are defined as web-based services that allow individuals to:

- Construct a public or semi-public profile within a bounded system.
- Articulate a list of other users with whom they share a connection.
- View and traverse their list of connections and those made by others within the system.

Social media gives users an efficient way to communicate and network with one another on an unprecedented scale and at rates unseen in traditional media. The popularity of social media has grown exponentially resulting in evolution of social networking sites, blogs, micro-blogs, location-based social networks, wikis, social bookmarking applications, social news, media (photo, audio and video) sharing, product and business review sites, etc.

Networking through social networking sites is becoming a popular means for users to express feelings, communicate information, share thoughts, and collaborate. Social networking sites have reshaped business models, provided platform for communities to grow, stimulated viral marketing, provided trend analysis and sales prediction, and can be a grass-roots information source.

All social networking sites provide profile users a range of privacy settings to protect their personal information. These settings are often confusing and many times not well communicated to all users. Users can face a

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

breach of privacy, unless these settings are properly used. In some cases, user's profiles are completely public, making information available and providing a communication mechanism to anyone who wants it. It is not a secret that when a social networking profile is public, malicious individuals including stalkers, spammers, and hackers, can use sensitive
information for their personal gain. Sometimes malevolent users can even cause physical or emotional distress to other users.

There are several privacy preserving methods in online social networks. But each method as many limitations. The proposed method check email verification before sending request to a user. It provides better privacy than other previous works. Several privacy preserving protocols in online social networks are discussed in this paper. This is presented in section II. Section III deals with the proposed method. In section IV, proposed method is compared with a previously reported method. Finally the conclusion is presented in section V.

II. LITERATURE SURVEY

There are various privacy preserving protocols in online social networks. Some of them are mentioned below.

A. Efficient Private Matching and Set Intersection

Private Set Intersection (PSI) [1] is a cryptographic protocol that involves two players, say Alice and Bob, each with a private set. Their goal is to compute the intersection of their respective sets, such that minimal information is revealed in the process. In other words, Alice and Bob should learn the elements in the intersection (if any) and nothing else. Ideally, this should be a mutual process thereby neither party has any advantage over the other.

This protocol enables two parties that each hold a set of inputs − drawn from a large domain − to jointly calculate the intersection of their inputs, without leaking any additional information. Applications include online recommendation services, online dating services, medical databases etc..

Protocol works as follows:

- A private matching (PM) scheme is a two-party protocol between a client (chooser) C and a server (sender) S.
- C's input is a set of inputs of size k_C, drawn from some domain of size N.
- S's input is a set of size k_S drawn from the same domain.
- C learns which specific inputs are shared by both C and S. That is, if C inputs X = {x1, . . . , xk_C } and S inputs Y = {y1, . . . , yk_S }, C learns X ∩ Y.

B. Semi-honest case: PSI

Protocols secure in the presence of semi−honest adversaries (or honest-but-curious)[2] assume that parties faithfully follow all protocol specifications and do not misrepresent any information related to their inputs, e.g., set size and content.

In this model, both Alice and Bob are assumed to act according to their prescribed actions in the protocol. The security definition is straightforward, particularly as in this case where only one party
(C) learns an output.

The protocol follows the following basic structure. C defines a polynomial P whose roots are her inputs:

$$p(y) = (x_1 - y)(x_2 - y).....(x_{k_c} - y) = \sum_{u=0}^{k_c} \alpha_u y^u$$

She sends to S homomorphic encryptions of the coefficients of this polynomial. S uses the homomorphic properties of the encryption system to evaluate the polynomial at each of his inputs.

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

He then multiplies each result by a fresh random number r to get an intermediate result, and he adds to it an encryption of the value of his input, i.e., S computes the result. Therefore, for each of the elements in the intersection of the two parties' inputs, the result of this computation is the value of the corresponding element, whereas for all other values the result is random.

C. Private Intersection of Certified Sets

In authorized PSI(APSI)[3] each element in the client set must be authorized (signed) by some recognized and mutually trusted authority. The goal of certifying the private sets of participants is to restrict their inputs to "sensible" or "appropriate" inputs. This reduces the strength of a malicious participant.

A certification authority (CA) is a trusted party who certifies that each participant's set is valid. Once the sets are certified, the CA need not be online. For example, suppose companies want to perform set operations on their financial data. Each company uses a different, but trusted, accounting firm who certifies the data. The companies can then perform as many operations with as many other companies with their certified data.

Certified sets will only reveal information about customers when law enforcement has a warrant for such information (signed by a judge). Participants can use different certifying authorities, provided both parties trust the authorities.

Certification will be done by the CA, who issues a CL signature to the set holder A for the set $S_A=(a_1,....a_k)$. Given this signature (or certificate) A must be able to prove the following:

- That encrypted coefficients correspond to the polynomial representation of a certified set.
- That the set used in a computation is certified.
- The size of the set.

APSI is a tuple of three algorithms: { Setup; Authorize; Interaction}.

- Setup: a process wherein all global/public parameters are selected.
- Authorize : a protocol between client and CA resulting in client committing to its input set and CA issuing authorizations (signatures), one for each element of the set.
- Interaction: a protocol between client and server that results in the client obtaining the intersection of two sets.

D. Perfectly Secure Multiparty Computation

The goal of secure multi−party computation [4] is to enable a set of n players to compute an arbitrary agreed function of their private inputs. The computation must guarantee the correctness of the outputs while preserving the secrecy of the player's inputs, even if some of the players are corrupted by an active adversary and misbehave maliciously. A passive adversary can read the internal state of the corrupted players, trying to obtain some information he is not entitled to. An active adversary can additionally make the corrupted players deviate from the protocol, trying to falsify the outcome of the computation.

The communication overhead of resilient multi−party protocols over private protocols is due mainly to the sophisticated techniques for achieving resilience against faults. Such protocols are very communication-intensive. The necessity of the broadcast channel is independent of whether or not actual faults occur: often broadcast is used to complain about an inconsistency, but when no inconsistency is detected, the players must nevertheless broadcast a confirmation message.

SMC protocol will work as follows

- In an SMC, a given number of

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

participants, p1, p2, ...,pN, each have private data, respectively d_1, d_2, ..., d_N.

- Participants want to compute the value of a public function on that private data: $F(d_1, d_2, ..., d_N)$ while keeping their own inputs secret.
- Most basic properties that a multi−party computation protocol aims to ensure are:

– Input privacy: No information about the private data held by the parties can be inferred from the messages sent during the execution of the protocol. The only information that can be inferred about the private data is whatever could be inferred from seeing the output of the function alone.

– Correctness: Any proper subset of adversarial colluding parties willing to share information or deviate from the instructions during the protocol execution should not be able to force honest parties to output an incorrect result. This correctness goal comes in two flavours: either the honest parties are guaranteed to compute the correct output (a ”robust” protocol), or they abort if they find an error (an SMC protocol ”with abort”).

III. PROPOSED METHOD

The proposed method is an improvement of asymmetric proximity measure. In particular, each OSN user is affiliated with some communities (or groups), which the user weighs differently. Communities can actually tell a lot about their members. There can be a wide variety of communities in an OSN like a university community, a department community, a fan community of an artist, movies, or sports, and a community of certain professions. Besides that in real life people also value their friendships differently. Thus, proposes an asymmetric social proximity between two users, which is the cumulative weight of the common communities to one user considering both his/her and his/her friend's perceptions. Also different private matching protocols are designed based on the asymmetric social proximity.

Asymmetric social proximity measure between two users in an OSN, which considers both each user's and his/her friend's perceptions on the common communities between the two users.

Three different private matching protocols are L1P, L2P/EL2P, and L3P, which provide users with different privacy levels. In particular, the protocol L3P with the highest privacy level ensures that two users will not know any of their common communities before they become friends.

Before delve into details, first present some definitions below:

- An Initiator is an OSN user who initiates a protocol for calculating social proximity. In other words, an Initiator is an OSN user who asks another user (a Responder) for friendship.
- A Responder, upon the the request from an Initiator, replies by following the protocol.

Besides, when an Initiator asks a Responder for friendship, it should be the Responder who determines whether or not to accept the request by executing the protocol to find the social proximity.

A. Protocol for Level 1 Privacy (L1P)

The protocol ensuring level 1 privacy is suitable for users who decide to make friends with each other simply based on the common communities of their overall community sets. First Responder learn the mutual communities and the size of the Initiator's input set, while let the Initiator learn nothing but the size of the Responder's input set. Then, the Responder securely sends the common communities to the Initiator, if she confirms the request from the Initiator.

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

The Initiator uses semantically secure homomorphic encryption to encrypt the coefficients of the polynomial P, whose roots are the elements of his input set C_i . The Responder cannot decrypt or distinguish the coefficients, and hence cannot know C_i . Following the protocol, the Responder then sends encrypted message back to the initiator with R_i . R_i is a random ID generated by the Responder for the community corresponding. The Initiator chooses a public key K as the key for a predefined symmetric encryption function and decrypts the message and send to responder. The Responder will be able to figure out mutual communities and let the Initiator know as well if she decides to confirm the request.

B. Protocol for Level 2 Privacy (L2P)

In the protocol for level 1 privacy (L1P), the Responder determines whether or not to accept the Initiator's request for a social friendship only based on their common overall communities, which may not characterize the social proximity well.

This protocol is suitable for the case when the Initiator is willing to establish a friendship relation with the Responder but the Responder accepts the relationship only if her requirement on the friendship is fulfilled. In particular, in L2P, the Responder accepts the friendship request from the Initiator if the social proximity measured by her is greater than a threshold predefined by herself.

C. Protocol for Level 3 Privacy (L3P)

In the L2P protocol, the Responder determines whether or not to be friends with the Initiator based on the community based social proximity, while the Initiator still can only make his final decision based on their common communities. A protocol for level 3 privacy, called L3P, to address the above problems. This protocol is suitable for users with very high privacy requirements. Both the Initiator and the Responder make sure their requirements on friendship are fulfilled before revealing any matching information to each other. If either of the requirements is not satisfied, neither of them knows the matching profile information, i.e., the common communities. In this method there is having different login for individual user profile and community and also it involves more time while doing the encryption process. Single user is not able to create a community. Also while joining a community verification is not done.

The proposed method solves the above problems. In the proposed method there is having a single login for individual user profile and community. More secure than existing method, since no more time consuming methods are used. It is very efficient and effective also it provides Email verification before sending friend request. Proximity is calculated on both sides and they are asymmetric. Single user can create a community and also verification and deletion is done by that user.

An asymmetric proximity measure between two users is the the cumulative weight of the common communities to one user considering both his/her and his/her friend's perceptions.

- Each user 'i' is affiliated with a set of communities, denoted by C
- $C_i = \{ C_i^1, C_i^2, C_i^3, C_i^4 ..... C_i^{c_i} \}$

To measure the social proximity (denoted by Ψ) between two users in an OSN without revealing their privacy, the user's overall community sets instead of their private profiles. Suppose A and B are to persons. Proximity measured by A is :

$$\Psi_{A \leftarrow B} = \frac{\sum C_A \cap C_B}{\sum C_A}$$

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

Proximity measured by B is :

$$\Psi_{B \leftarrow A} = \frac{\sum C_A \cap C_B}{\sum C_B}$$

IV. EXPERIMENTAL RESULTS

The proposed method is implemented using Python. The performance of proposed method is compared with mutual friends and proximity measure. The output of proposed method is shown in Fig. 1. Even though when there is no mutual friends there is having proximity measure. That is they have more relationship with the user through mutual communities. As the mutual communities get increased proximity measure will also increase. Hence, proposed method is more effective than the existing methods.

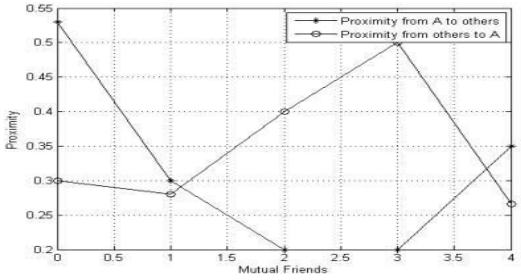

Fig. 1. Proximity Calculation

V. CONCLUSION

The ever increasing use of OSNs has introduced a new paradigm in interacting with existing friends and making new friends in the online world as well as in real life. Privacy is the major concern. There are several methods for providing privacy in online social networks. Proposed method avoids the demerits of existing method. It provides better privacy and better proximity calculation.

REFERENCES

[1] M. J. Freedman, K. Nissim, and B. Pinkas, ”Efficient private matching and set intersection”, in Proc. 17th Int. Conf.
Theory Appl. Cryptographic Techn , Interlaken, Switzerland, May 2004, pp. 119.

[2] C. Hazay and K. Nissim, ”Efficient set operations in the presence of malicious adversaries”, J. Cryptology, vol. 25, no. 3, pp. 383−433, 2012.

[3] J. Camenisch and G. M. Zaverucha, ”Private intersection of certified sets”, in Financial Cryptography and Data
Security, New York, NY, USA: Springer, Feb. 2009.

[4] I. Damgard, Y. Ishai, and M. Kroigaard, ”Perfectly secure multiparty computation and the computational overhead of cryptography”, in Proc. 29th Annu. Int. Conf. Theory Appl. Cryptographic Techn., French Riviera, France,May 2010, pp. 445465.

[5] Michael Fire, Roy Goldschmidt, and Yuval Elovici, ”Online Social Networks: Threats and Solutions”, IEEE
Communication surveys tutorials , Vol. 16, No. 4, Fourth Quarter 2014.

[6] Michael Fire, Roy Goldschmidt, and Yuval Elovici, ”Online Social Networks: Threats and Solutions”, IEEE
Communication surveys tutorials , Vol. 16, No. 4, Fourth Quarter 2014.

[7] Arun Thapa, Ming Li, Sergio Salinas and Pan Li, ”Asymmetric Social Proximity Based Private Matching Protocols for Online Social Networks”, IEEE Transactions on parallel and distributed systems , Vol. 26, No. 6, June 2015.

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org