Privacy Measurements in Online Social Networks

P.NARAYANA, K.Srivani, P.Sravya, T.Spoorthi
Assistant Professor, IV B.TECH IT
Malla Reddy Engineering College for Women

Abstract- Rapid changes are occurring in Social Networks since once decade. Using Online Social Networks people can interact with their friends i.e, existing or new friends. However it is people can interact in a attractive way means they can get friend requests depends on their similar attributes. Everyone can maintain their profiles here profile matching involves an inherent privacy risk of exposing private profile information to strangers in the cyberspace. The existing systems problem attempt to protect users' privacy by privately computing the intersection or intersection cardinality of the profile attribute sets of two users. These approaches are having some limitations and can still reveal users' privacy. So there's no privacy preservation in the existing systems. In this paper, we leverage community structures to redefine the OSN model and propose a realistic asymmetric social proximity measure between two users. Using Profile parameters they can become friends.

Keywords- Attributes, Privacy,Friend,Community.

I. INTRODUCTION

(OSN) Online Social Networks uage is rapidly increasing overt the past few years. Facebook, Google+,Orkut,Linkedin are most visited sites on the Internet. Using these web sites users are spending lot of time on thes Social Networks.

Today every thing is available in our palm means smart phones are extendedt the platforms used for accessing online social networks and provided a plenty of opportunities for mobile socual networking.

Usually people are showing interest to add any new friend so that's why here OSN model was redefined the way of interacting with existing friends and also to add new friends. OSNs have redefined the way people interact with existing friends, and more importantly, make new friends. In particular, people can now explore potential friendships via OSNs, by looking for common interests, friends, and symptoms, close geographic proximity, etc., between each other.

II. LITERATURE SURVEY

In OSNs and Mobile Social Networks (MSNs), many distributed solutions to privately finding the social proximity between two users have been proposed. The most common way of determining friendship between two people is through profile matching, i.e. finding out if they have common profile attributes, like interests [4], [5], symptoms [6]–[8], or some other social coordinates [9], [10]. In some cases, the number of common friends also serves as the proximity measure between two users .Such previous works employ various cryptographic tools to protect the privacy of the profile information of the users in the private matching process. After two strangers, say with profile attribute sets X and Y , execute a private matching protocol, the one who initiates the protocol will know either $X \cap Y$ or some function of $X \cap Y$ while the other one who responds does not know anything. Thus, a malicious user can execute the protocol with any user and leave without letting him/her do the same.

Moreover, most previous schemes for profile matching in online/mobile social networking are based on the premise that two people are likely to establish a social relationship only if they share similar profile attributes like interests, symptoms, or some other social coordinates. While it is true that people with similar profile attributes are likely to be friends, this is not the only way of determining friendship. For example, a doctor's best friend may not necessarily always be a doctor, but We notice that whether two people can become friends not only depends on whether they have anything in common, but also is affected by whether their friends have anything in common. The intuition behind this is simple: a friend's friend can also be a friend. In this paper, we leverage community structures to redefine the OSN model, and propose an asymmetric social proximity between two users. In particular, we consider that each OSN user is affiliated with some communities (or groups), which the user weighs differently. We notice that the 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, we notice that in real life people also value their friendships differently. Thus, we propose 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 friends' perceptions. We also design three different private matching protocols based on the proposed asymmetric social proximity. The main contributions of this paper can be briefly summarized as follows. We define an asymmetric social proximity measure.

III. SYSTEM MODELS

EXISTING SYSTEM:

In Existing System numbers of solutions are provided to privately finding the social proximity between two users. The general way of finding friendship between two people is via profile matching.

That means finding if they have common profile parameters like interests, symptoms, and other social coordinates. Most of the cases number of common friends also serves as the proximity measure between two users. That earlier works employ various cryptographic tools to protect the privacy of the profile information of the users in the private matching process.

DISADVANTAGES OF EXISTING SYSTEM:

Here the people who are at server side like admin can know users data. i.e. a server knows all the user's personal information and there is a chance of single point of failure. In this proposed method all users' privacy is at risk.

PROPOSED SYSTEM**:**

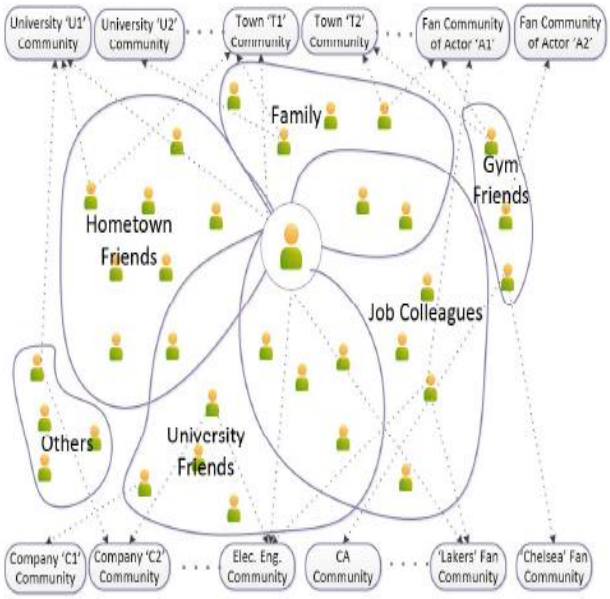
In the proposed system we discuss community structures to remodel the OSN model and propose an asymmetric social proximity between two users. Especially each Online Social Network user is attached with some communities which the user weights differently. Here the communities can say about their members.

There are wide variety of communities in an OSN like a department community, fan community of an artist, professional community, university community, and other communities. Besides, we notice that in real life people also value their friendships differently. Thus, we propose 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 friends' perceptions. We also design three different private matching protocols based on the proposed asymmetric social proximity.

ADVANTAGES OF PROPOSED SYSTEM:

In our proposed system we are going to provide privacy measurement of both each user and their friends perceptions on the communities. Generally communities are built for sharing information of like minded people. Here we proposed Level3 Protocol with the highest privacy level ensures that two users will not know any of their common communities before they become friends.

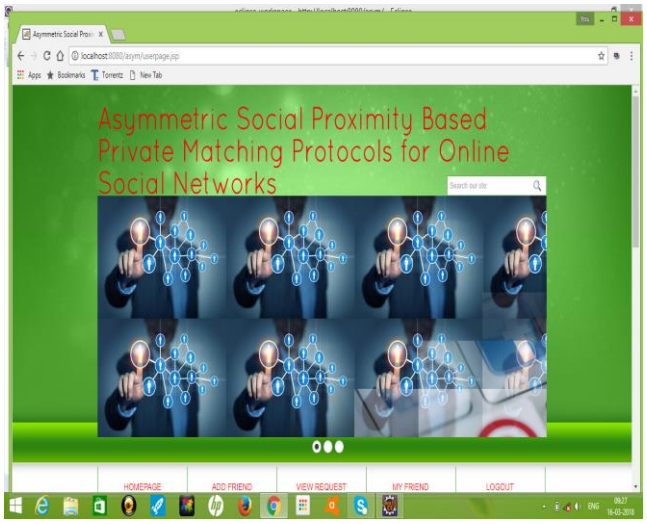
Our protocols protect users' privacy better than the previous works based on symptoms, interests, and the number of common friends, with lower computation and communication cost.

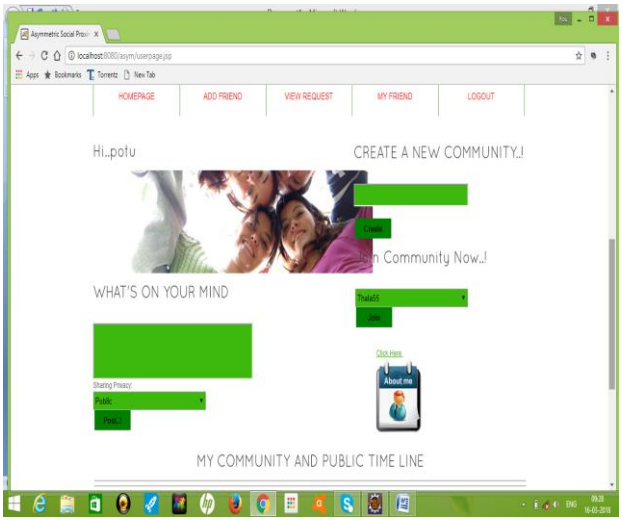


IV. MODULES

Here we have different kinds of modules to make a way of communication between multiple people. Similar to Facebook and all here also any two users can exchange their views with different perspectives. But here matter is they can coordinate with different cardinalities'. If he/she is a registered user they can easily logged in otherwise he/she has to register and create a new account in online social network. After completion of this they can send a friend request to any individual members or to the communities. Here nobody are able to see others personal information. That is the very important flavour added here. They too can share their views or discus in chat box.

V. DESIGN AND VIEW





VI. CONCLUSION

Here Online Social Networks usage is different and providing the security to personal information of the users. Privacy preserving is enabled here. To get new friends in OSNs by preserving their privacy is an important and face off problem. In this paper we have explained the community structure of an OSN to characterize a realistic asymmetric social proximity measure and have gone through different levels of protocols for preserving privacy between any two users.

VII. FUTURE ENHANCEMENT

Here technology is a continuous evolution process. So none of the application is constant. User requirements keep changing as the system is being used. By using newly adaptable technologies we can develop and preserve privacy in a more efficient way. In future may be used Level4 privacy measurement protocol for preserving the privacy to achieve accurate communication between users.

VIII. REFERENCES

[1]. (2013, October). [Online]. Available: http://www.alexa.com/ topsites

[2]. CNN, "Report: Eastern european gang hacked apple, facebook, twitter," http://www.cnn.com/2013/02/20/tech/web/hackedapple-facebook-twitter/index.html, February, 2013.

[3]. IGN, "Microsoft hacked by same method as apple and facebook," http://www.ign.com/articles/2013/02/23/microsofthacked-by-same-method-as-apple-and-facebook, February, 2013.

[4]. H. Lin, S. S. M. Chow, D. Xing, Y. Fang, and Z. Cao, "Privacy-Preserving Friend Search over Online Social Networks," Cryptology ePrint Archive, Report 2011/445, 2011. [Online]. Available: http://eprint.iacr.org/

[5]. R. Zhang, Y. Zhang, J. S. Sun, and G. Yan, "Fine-grained Private Matching for Proximity-based Mobile Social Networking," in IEEE International Conference on Computer Communications (INFOCOM'12), Orlando, Florida, USA, March 2012.

[6]. M. Li, N. Cao, S. Yu, and W. Lou, "FindU: Privacy-preserving Personal Profile Matching in Mobile Social Networks," in IEEE International Conference on Computer Communications (INFOCOM'11), Shanghai, China, April 2011.

[7]. R. Lu, X. Lin, X. Liang, and X. Shen, "A Secure Handshake Scheme with Symptoms-Matching for mHealthcare Social Network," Mobile Networks and Applications, vol. 16, pp. 683–694, 2011.

[8]. X. Liang, M. Barua, R. Lu, X. Lin, and X. Shen, "HealthShare: Achieving Secure and Privacy-preserving Health Information Sharing through Health Social Networks," Computer Communications, vol. 35, no. 15, pp. 1910–1920, 2012.