Survey on Privacy-Preserving Friend Suggestion system for Online Social Networks

[1]Mr. Sandeep Konjere, [2]Prof. V. N. Dhawas
*[1]Dept. of Computer Engineering, SIT, Lonavala, Savitribai Phule
Pune University, Pune, India.*
*[2]Dept. of Computer Engineering, SIT, Lonavala, Savitribai Phule
Pune University, Pune, India*
[1] konjeresandeep@gmail.com , [2]vnd.sit@sinhgad.edu

Abstract: In day to day world use of Online Social Network (OSN)like Orkut, YouTube, and Flickr .is growing tremendously. in the day to day life, the social relationship in are possibly formed by OSN users shared attributes, e.g., colleagues, family members, or classmates, which shows the attribute-based recommendation process would lead to more fine-grained social relationships between strangers. So for this reason securing the privacy and personal information of a individual is of prime Importance. And so trust-based routing has received much attention as an effective way to improve security of wireless ad hoc networks (WANETs). Although various trust metrics have been designed and included into the routing metrics, the survey is done and got the conclusion that none of the existing works have used mathematical tools such as routing algebra to analyze the compatibility of trust related routing metrics and routing protocols in WANETs.

Keywords – OSN, WANETS, ONLINE SOCIAL NETWORKS.

I. INTRODUCTION

Online social networks (OSNs) for example, Facebook, MySpace, and Twitter empower individuals to stay in contact with their contacts, reconnect with old colleagues, and set up new connections with other individuals in view of shared components, for example, groups, leisure activities, intrigues, and covers in fellowship circles. Late years have seen phenomenal development in the use of OSNs, with around 300 OSN frameworks gathering data on more than a large portion of a billion enlisted client . Accordingly, OSNs store an enormous measure of perhaps delicate furthermore, private data on clients and their associations. This data is generally private and expected for the eyes of a particular gathering of people just. On the other hand, the notoriety of OSNs pulls in unwavering clients as well as gatherings with rather antagonistic intrigues too . The broadening and complexity of purposes and utilization examples of OSNs unavoidably present security encroachment dangers to all OSN clients as a consequence of data trade and sharing on the Internet. It is along these lines not astounding that stories about security breaks by Facebook and MySpace show up over and again in standard media.

Despite the reason for an OSN, one of the primary inspirations for clients to join an OSN, make a profile, and utilize distinctive applications offered by the OSN is the likelihood to effortlessly impart data to chose contacts or people in general, also, encourage social co-operations between the clients of OSNs. Uncovering individual data in OSNs is a twofold edged sword. On one hand, data introduction is typically a additionally, even an unquestionable requirement, if individuals need to take an interest in social groups.

Perceivability of clients' profiles and open presentation of associations (companion records) are fundamental for executing center functionalities of OSNs, for example, social enquiry. On the other hand, leakage of personal information, especially one's identity, may invite malicious attacks from the real world and cyberspace, such as stalking, reputation slander, personalized spamming, and phishing [7]. Despite the risks, many of the privacy and access control mechanisms of today's OSNs are purposefully weak to make joining the OSN and sharing information easy. We believe that more effective and flexible security mechanisms are therefore required for the safety of OSN users as well as the continued thriving of OSNs.

II. RELATED WORK

In [1] author explained Online social networking like Orkut , YouTube, and Flickr are among the most mainstream locales on the Internet. Clients of these locales shape an informal community, which gives a capable method for sharing, arranging, and discovering substance what's more, contacts. The prominence of these locales gives a chance to think about the qualities of online social system charts everywhere scale. Understanding these charts is essential, both to enhance current frameworks and to outline new uses of online informal communities.

This paper presents a large-scale measurement study and analysis of the structure of multiple online social networks. We examine data gathered from four popular online social networks: Flickr, YouTube, Live Journal, and Orkut. We crawled the publicly accessible user links on each site, obtaining a large portion of each social network's graph. Our data set contains over 11.3 million users and 328 million links. We believe that this is the first study to examine multiple online social networks at scale.

In [2] author perform a large-scale study to calculate just how severe the privacy leakage problem is in Facebook. As a case study, we focus on estimating birth year, which is a fundamental human attribute and, for many people, a private one. Specifically, we attempt to estimate the birth year of over 1 million Facebook users in New York City. We examine the accuracy of estimation procedures for several classes of users: (i) highly private users, who do not make their friend lists public; (ii) users who hide their birth years but make their friend lists public.

In [3] author demonstrated that it is not surely knew how protection concern and trust impact social collaborations inside of person to person communication destinations. An online overview of two well known person to person communication destinations, Facebook and MySpace, looked at impression of trust and protection concern, alongside ability to share data and grow new connections. Individuals from both locales reported comparative levels of security concern. Facebook individuals communicated altogether more prominent trust in both Facebook and its individuals, and were more willing to share recognizing data. Indeed, even thus, MySpace individuals reported altogether more experience utilizing the site to meet new individuals. These outcomes recommend that in online communication, trust is not as important in the building of new connections as it is in eye to eye experiences. They likewise demonstrate that in an online webpage, the presence of trust and the readiness to share data don't consequently interpret into new social communication. This study shows online connections can create in locales where seen trust and security protections are feeble.

In [4] author explained trust-based steering has gotten much consideration as a compelling approach to enhance security of remote commercial hoc systems (WANETs). Albeit different trust measurements have been outlined and joined into the steering measurements, as far as we probably am aware, none of the current works have utilized scientific instruments, for example, steering variable based math to examine the similarity of trust related steering measurements and directing conventions in WANETs. In this paper, they first distinguish extraordinary components of trust measurements contrasted and QoS-based steering measurements. At that point, they give a orderly investigation of the relationship between trust measurements and

trust-based identifying so as to steer conventions the essential logarithmic properties that a trust metric must have keeping in mind the end goal to work effectively and ideally with distinctive summed up separation vector then again connection state directing conventions in WANETs.

In [5] author explained mobile social software has become an active area of research and development. A multitude of systems have been proposed over the past years that try to follow the success of their Internet bound equivalents. Many mobile solutions try to augment the functionality of existing platforms with location awareness. The price for mobility, however, is typically either the lack of the popular friendship exploration features or the costs involved to access a central server required for this functionality. In this paper, we try to address this issue by introducing a decentralized method that is able to explore the social neighborhood of a user by finding friends of friends. Rather than only exploiting information about the users of the system, the method relies on real friends, and adequately addresses the arising privacy issues. Moreover, we present VENETA, a mobile social networking platform which, among other features, implements our novel friend of friend detection algorithm.

In [6] author explained that recent years have seen uncommon development in the notoriety of interpersonal organization frameworks, with Facebook being a model case. The entrance control worldview behind the security conservation system of Facebook is particularly not the same as such existing access control ideal models as Discretionary Access Control, Role-Based Access Control, Capability Systems, and Trust Management Systems. This work steps in extending the comprehension of this entrance control worldview, by proposing an access control demonstrate that formalizes and sums up the protection safeguarding component of Facebook. The model can be instantiated into a group of Facebook-style informal organization frameworks, each with an unmistakably distinctive access control instrument, so that Facebook is yet one instantiation of the model.

In [7] author explained how Confidentiality and data handling are important issues for social network users. Ideally, access control enforcement should not depend on the social networking provider but should be under the control of the user. In this paper, we propose a practical, SNS platform-independent solution, for social network users to control their data. We develop concepts that are general enough to describe access control restrictions for different SNS platforms. Our architecture uses encryption to enforce access control for users' private information based on their privacy preferences. We have implemented our model as a Firefox extension

In [8] author explained Online social networks such as Facebook, Myspace, and Twitter have experienced tremendous growth in recent years. These OSNs offer striking means of online social interactions and communications, but also raise privacy and security concerns. In this article we explained the design issues for the security and privacy of OSNs. We find there are inherent design conflicts between these and the traditional design goals of OSNs such as usability and sociability. We present the distinctive security and privacy design problems brought by the core functionalities of OSNs and highlight some opportunities of utilizing social network theory to mitigate these design conflicts.

III. ARCHITECTURAL VIEW

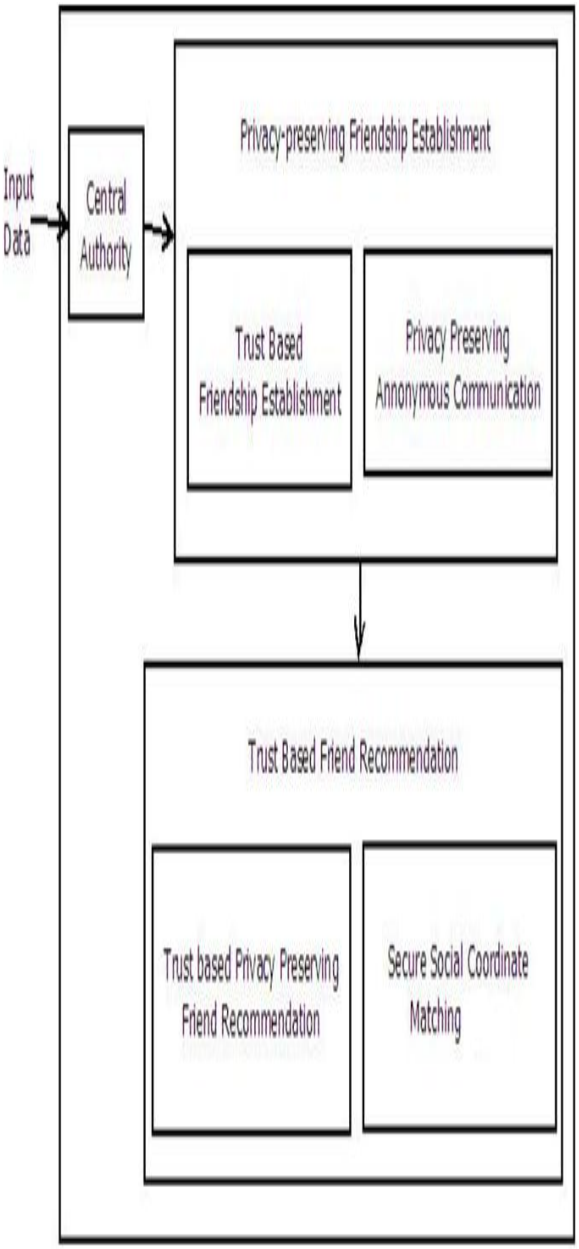
Input Data
Central Authority
Privacy-preserving Friendship Establishment
Trust Based Friendship Establishment
Privacy Preserving Annonymous Communication
Trust Based Friend Recommendation
Trust based Privacy Preserving Friend Recommendation
Secure Social Coordinate Matching

Fig.1: System Architecture

Sr no.	Paper	Technique	advantages	disadvantages	Result
1	Measurement and Analysis of Online Social Networks	This paper presents a large-scale measurement study and analysis of the structure of multiple online social networks.	the power-law, small-world, and scale free properties of online social networks	the structure and dynamics of the content graph is an open problem	Social networks have a much higher fraction of symmetric links and also exhibit much higher levels of local clustering . We have outlined how these properties may affect algorithms and applications designed for social networks.
2	Estimating Age Privacy Leakage in Online Social Networks	To estimate Facebook users' ages, we exploit the underlying social network structure to design an iterative algorithm, which derives age estimates based on friends' ages, friends of friends' ages, and so on.	greatly reduce privacy leakages in its service.		We found that for most users, including private users who hide their friend lists, it is possible to estimate ages within a few years
3	Trust and privacy concern within social networking sites:	In this paper Comparsion is done between facebook and Myspace to show that trust and privacy concern in social networking sites	It show that in an online site, the existence of trust and the willingness to		in online interaction, trust is not as necessary in the building of new

	A comparison of Facebook and MySpace	is not yet understood to a sufficient degree to allow accurate modeling of behavior and activity	share information do not automatically translate into new social interaction		relationships as it is in face to face encounters.
4	A Formal Study of Trust-Based Routing in Wireless Ad Hoc Networks	They first identify unique features of trust metrics compared with QoS-based routing metrics. Then, they provided a systematic analysis of the relationship between trust metrics and trust-based routing protocols by identifying the basic algebraic properties that a trust metric must have in order to work correctly and optimally with different generalized distance-vector or link-state routing protocols inWANETs.		System is restricted up to unicast routing.	they develop a formal framework and theory to investigate the correctness, optimality, inter-operativity of trust-based routing protocols for WANETs.
5	VENETA:-Serverless Friend-of-Friend Detection in Mobile Social Networking	a technique that seamlessly incorporates the friendship exploration functionality of traditional social networking websites into purely decentralized environments.	The arising privacy issues have been addressed adequately.		The arising privacy issues have thereby adequately been addressed.
6	A Privacy Preservation Model for Facebook -Style Social Network	We have formalized the distinct access control paradigm behind the Facebook privacy preservation mechanism			

	Systems	into an access control model, which delineates the design space of protection mechanisms under this paradigm of access control.			
7	Enforcing Access Control in Social Network Sites	a practical, SNS platform-independent solution, for social network users to control their data. they develop concepts that are general enough to describe access control restrictions for different SNS platforms.	Confidentiality and data handling are handled.		They implemented a system that allows users to define and enforce selective access control policies for data published on social lnetwork sites. By using a PKI encryption scheme, such as Open PGP we were able to keep users' data confidential, even towards the SNS operator, by means of encryption
8	Privacy and Security for Online Social Networks: Challenges and Opportunities	We present the unique security and privacy design challenges brought by the core functionalities of OSNs and highlight some opportunities of utilizing	Here Security and privacy issues od social networking sites are maitained		Here they discussed security and privacy design issues on online social networks and

		social network theory to mitigate these design conflicts.			pointed out a few research directions for mitigating the design conflicts between the various design design goals of OSNs

V. CONCLUSION

In this paper, Survey is done on a privacy-preserving trust-based friend recommendation scheme for online social networks, which enable two strangers establish trust relationships based on the existing 1-hop friendships.

REFERENCES

1) A. Mislove, M. Marcon, K. P. Gummadi, P. Druschel, and B. Bhattacharjee, “Measurement and analysis of online social networks,” in Proc. 7th ACM SIGCOMM Conf. Internet Meas., 2007, pp. 29–42.

2) R. Dey, C. Tang, K. Ross, and N. Saxena, “Estimating age privacy leakage in online social networks,” in Proc. IEEE Conf. Comput. Commun., 2012, pp. 2836–2840.

3) C. Dwyer, S. R. Hiltz, and K. Passerini, “Trust and privacy concern within social networking sites: A comparison of facebook and myspace,” in Proc. 13th Amer. Conf. Inf. Syst., 2007, p. 339

4) C. Zhang, X. Zhu, Y. Song, and Y. Fang, “A formal study of trust based routing in wireless ad hoc networks,” in Proc. IEEE 29th Int. Conf. Comput. Commun ., Mar. 2010, pp. 1–9.

5) M. von Arb, M. Bader, M. Kuhn, and R. Wattenhofer, “Veneta: Serverless friend-of-friend detection in mobile social networking,” in Proc. IEEE Int. Conf. Wireless Mobile Comput. Netw. Commun., Oct. 2008, pp. 184–189.

6) P. W. L. Fong, M. Anwar, and Z. Zhao, “A privacy preservation model for facebook-style social network systems,” in Proc. 14t Eur. Conf. Res. Computer. Security, 2009, pp. 303–320.

7) B. Carminati, E. Ferrari, and A. Perego, “Enforcing access control in web-based social networks,” ACM Trans. Inf. Syst. Security, vol. 13, no. 1, pp. 6:1–6:38, Nov. 2009.

8) C. Zhang, J. Sun, X. Zhu, and Y. Fang, “Privacy and security for online social networks: Challenges and opportunities,” IEEE Netw., vol. 24, no. 4, pp. 13–18, Jul./Aug. 2010.

.