RNI Regd No: APENG/2011/47294 ISSN No: 2320-3706(PRINT)
International Journal & Magazine of Engineering, Technology, Management and Research
YUVAENGINEERS
Transforming Young Engineers for Better Tomorrow

Online Social Networks Privacy and Protection Using Asymmetric Matching Protocols

Pavuluri Subbarao
MCA Student,
CMR College of Engineering & Technology, (Kandlakoya).

Ch.Dayakar Reddy
MCA, M.Tech, M.Phil, (Ph.D),
Professor & MCA HOD,
CMR College of Engineering & Technology, (Kandlakoya).

Gouda Rajesh
MCA Student,
CMR College of Engineering & Technology, (Kandlakoya).

Abstract:
Online social networks (OSNs) have experienced tremendous growth in recent years and become a de facto portal for hundreds of millions of Internet users. These OSNs offer attractive means for digital social interactions and information sharing, but also raise a number of security and privacy issues. While OSNs allow users to restrict access to shared data, they currently do not provide any mechanism to enforce privacy concerns over data associated with multiple users. Online Social Networks (OSNs), which attract thousands of million people to use everyday, also greatly extend OSN users' social circles by friend recommendations. OSN users' existing social relationship can be characterized as 1-hop trust relationship, and further establish a multi-hop trust chain during the recommendation process. As the same as what people usually experience in the daily life, the social relationship in cyberspaces are potentially formed by OSN users' shared attributes, e.g., colleagues, family members, or classmates, which indicates the attribute-based recommendation process would lead to more fine grained social relationships between strangers.Unfortunately, privacy concerns raised in the recommendation process impede the expansion of OSN users' friend circle. Some OSN users refuse to disclose their identities and their friends' information to the public domain.This project is motivated by the recognition of the need for a finer grain and more personalized privacy in data publication of social networks. It proposes a privacy protection scheme that not only prevents the disclosure of identity of users but also the disclosure of selected features in users' profiles. An individual user can select features of his/her profiles that should not be disclosed to others.Social networking is modelled as graphs in which users are nodes and features are labels. Labels are denoted either as sensitive or as non-sensitive. It treats node labels both as background knowledge an adversary may possess, and as sensitive information that has to be protected. It also presents privacy protection algorithms that allow for graph data to be published in a form such that an adversary who possesses information about a node's neighbourhood cannot safely infer its identity and its sensitive labels. It shows that our solution is effective, efficient and scalable while offering stronger privacy guarantees than those in previous research.

General Terms:
Networking, Security, Node detection Algorithms.

Keywords:
Online social networks, data privacy, social networking, privacy protection algorithms.

I.INTRODUCTION :
Can users have reasonable expectations of privacy in online social networks (OSNs)? Media reports, regulators, and researchers have replied to this question affirmatively. Even in the ―transparent‖ world created by Facebook, LinkedIn, and Twitter, users have legitimate privacy expectations that could be violated.Researchers from different computer science disciplines have tackled some of the problems that arise in OSNs and propose a diverse range of privacy solutions, including software tools and design principles. Each of these solutions is developed with a specific type of user, use, and privacy problem in mind. This has had some positive effects: we now have a broad spectrum of approaches to tackle OSNs' complex privacy problems. At the same time, it has led to a fragmented landscape of solutions that address seemingly

unrelated problems.Consequently, the field's vastness and diversity remain mostly inaccessible to outsiders and, at times, even to computer science researchers who specialize in a specific privacy problem. One of our objectives is to put these research approaches to OSN privacy into perspective.

II.LITERATURE SURVEY:

Privacy in OSNs shows that our solution is effective, efficient and scalable while offering stronger privacy guarantees than those in previous research. To know in detail working of Privacy in OSNs there should be in detail literature survey of Online Social Networks (OSNs).

II.1 Hummingbird: Privacy at the time of Twitter:

This paper assesses privacy in today's Twitter-like OSNs and describes architecture and a trial implementation of a privacy-preserving service called Hummingbird. It is essentially a variant of Twitter that protects tweet contents, hashtags and follower interests from the (potentially) prying eyes of the centralized server. It argues that, although inherently limited by Twitter's mission of scalable information sharing, this degree of privacy is valuable.It demonstrates, via a working prototype, that Hummingbird's additional costs are tolerably low. It also sketches out some viable enhancements that might offer better privacy in the long term.

II.2. A Trust-based Privacy-Preserving Friend Recommendation Scheme for Online Social Networks:

This paper proposes a trust-based privacy-preserving friend recommendation scheme for OSNs, where OSN users apply their attributes to find matched friends, and establish social relationships with strangers via a multi-hop trust chain.

II.3 Asymmetric Social Proximity Based Matching Protocols for Online Social Networks:

This paper leverages community structures to redefine the OSN model and propose a realistic asymmetric social proximity measure between two users. Then, based on the proposed asymmetric social proximity, it designs three private matching protocols, which provide different privacy levels and can protect users' privacy better than the previous works.It also analyzes the computation and communication cost of these protocols. Finally, it validates proposed asymmetric proximity measure using real social network data and conduct extensive simulations to evaluate the performance of the proposed protocols in terms of computation cost, communication cost, total running time, and energy consumption. The results show the efficacy of our proposed proximity measure and better performance of our protocols over the state-of-the-art protocols.

II.4 Fairness-Aware and Privacy-Preserving Friend Matching Protocol in Mobile Social Networks:

This paper models the secure friend discovery process as a generalized privacy-preserving interest and profile matching problem. It identifies a new security threat arising from existing secure friend discovery protocols, coined as runaway attack, which can introduce a serious unfairness issue.To thwart this new threat, it introduces a novel blind vector transformation technique, which hides the correlation between the original vector and transformed results. Based on this, it proposes privacy-preserving and fairness-aware interest and profile matching protocol, which allows one party to match its interest with the profile of another, without revealing its real interest and profile and vice versa.

II.5 Privacy-Enabling Social Networking over Untrusted Networks:

This paper proposes architecture for social networking that protects users' social information from both the operator and other network users. This architecture builds a social network out of smart clients and an Untrusted central server in a way that removes the need for faith in network operators and gives users control of their privacy.

II.6 Scramble! Your social network data:

This paper proposes Scramble, the implementation of a SNS-independent Firefox extension that allows users to enforce access control over their data. Scramble lets users define access control lists (ACL) of authorized users for each piece of data, based on their preferences. The definition of ACL is facilitated through the possibility of dynamically defining contact groups. In turn, the confidentiality and integrity of one data item is enforced using cryptographic techniques. When accessing a SNS that contains data encrypted using Scramble, the plug-in transparently decrypts and checks integrity of the encrypted content.

II.7 Multiparty Access Control for Online Social Networks:

This paper proposes an approach to enable the protection of shared data associated with multiple users in OSNs. It formulates an access control model to capture the essence of multiparty authorization requirements, along with a multiparty policy specification scheme and a policy enforcement mechanism.

II.8 Safebook: A Privacy-Preserving Online Social Network Leveraging on Real-Life Trust:

Online social network applications severely suffer from various security and privacy exposures. This article suggests a new approach to tackle these security and privacy problems with a special emphasis on the privacy of users with respect to the application provider in addition to defense against intruders or malicious users. In order to ensure users' privacy in the face of potential privacy violations by the provider, the suggested approach adopts a decentralized architecture relying on cooperation among a number of independent parties that are also the users of the online social network application.

The second strong point of the suggested approach is to capitalize on the trust relationships that are part of social networks in real life in order to cope with the problem of building trusted and privacy-preserving mechanisms as part of the online application.The combination of these design principles is Safebook, a decentralized and privacy-preserving online social network application.Based on the two design principles, decentralization and exploiting real-life trust, various mechanisms for privacy and security are integrated into Safebook in order to provide data storage and data management functions that preserve users' privacy, data integrity, and availability. Preliminary evaluations of Safebook show that a realistic compromise between privacy and performance is feasible.

II.9 Must Social Networking Conflict with Privacy:

This paper proposes some built-in assumptions that can find different tradeoffs that give users more control over their privacy and require less trust in OSN operators.The goal of this paper is to guard user data from friends or governments but to reduce OSN providers' ability to disclose user data beyond users' wishes—without compromising functionality.

III.PROBLEM DEFINITION:

We distinguish the three types of privacy problems that computer science researchers typically tackle.The surveillance problem arises when governments and service providers leverage OSN users' personal information and social interactions.Social privacy problems emerge through the necessary renegotiation of boundaries as social interactions are mediated byOSN services.The third problem, institutional privacy, relates to users losing control and oversight of OSNs' collection and processing of their information. Each approach to these problems abstracts away some of the complexity of privacy in OSNs to focus on more solvable questions.However, researcher's working from different perspectives differs not only in what they abstract but also in their fundamental assumptions about what the privacy problem is. Thus, the surveillance, social privacy, and institutional privacy problems end up being treated as if they were independent phenomena. We argue that these different privacy problems are entangled and that OSN users would benefit from a better integration of the three approaches. For example, consider surveillance and social privacy issues. OSN providers have access to all the user-generated content and the power to decide who has access to which information. This might lead to social privacy problems—for example, OSN providers might increase content visibility in unexpected ways by overriding existing privacy settings. Thus, some of the privacy problems users experience with their ―friends‖ might not be due to their own actions but instead result from the OSN provider's strategic design changes.If we focus only on the privacy problems that arise from users' misguided decisions, we might end up deemphasizing the fact that there's a central entity with the power to determine the accessibility and use of information. Similarly, surveillance problems aren't independent of social privacy problems. OSN social practices might have consequences for the effectiveness of intrusive surveillance measures. For instance, the social tagging of people in pictures, coupled with the use of facial recognition by OSN providers, increases OSN users' visual legibility. This can be used for surveillance purposes, for instance, to identify unknown protesters in pictures taken at demonstrations. Furthermore, it decreases the protective function of simple obscurity measures such as untagging oneself—somethingOSN consumers often utilize as a privacy protection strategy toward their peers. However, untagging doesn't diminish the surveillance capabilities of OSN providers, who might keep a record of the tag as well as run facial recognitionalgorithms. This shows that the way social privacy problems are managed can directly impact the power relationships between OSN providers and users.

III.1 Existing System:

The current trend in the Social Network it not giving the privacy about user profile views. The method of data sharing or (Posting) has taking more time and not under the certain condition of displaying sensitive and non-sensitive data.

III.2 Problems on existing system:

1.There is no way to publish the Non sensitive data to all in social Network.
2.It's not providing privacy about user profiles.
3.Some mechanisms that prevent both inadvertent private information leakage and attacks by malicious adversaries.
For exa
mple, consider surveillance and social privacy issues. OSN providers have access to all the user generated content and the power to decide who may have access to which information.

This may lead to social privacy problems, e.g., OSN providers may increase content visibility in unexpected ways by overriding existing privacy settings. Thus, a number of the privacy problems users experience with their ―friends‖ may not be due to their own actions, but instead result from the strategic design changes implemented by the OSN provider.Another major problem is that users encounter great difficulties to effectively configure their privacy settings.

III.3 Proposed System:

Here, we extend the existing definitions of modules and we introduced the sensitive or non-sensitive label concept in our project. We overcome the existing system disadvantages in our project.

Advantages:

1.We can publish the Non sensitive data to every-one in social Network.
2.It's providing privacy for the user profiles so that unwanted persons not able to view your profiles.

IV.ALORITHM USED:

Graph Based Noisy Node detection:

The algorithm starts out with group formation, during which all nodes that have not yet been grouped are taken into consideration, in clustering-like fashion. In the first run, two nodes with the maximum similarity of their neighbourhood labels are grouped together. Their neighbour labels are modified to be the same immediately so that nodes in one group always have the same neighbour labels. For two nodes, v1 with neighbourhood label set (LSv1), and v2 with neighbourhood label set (LSv2), we calculate neighbourhood label similarity (NLS) as follows:

$$NLS(v_1, v_2) = \frac{|LS_{v_1} \cap LS_{v_2}|}{|LS_{v_1} \cup LS_{v_2}|}$$

Larger value indicates larger similarity of the two neighbourhoods. Then nodes having the maximum similarity with any node in the group are clustered into the group till the group has nodes with different sensitive labels. Thereafter, the algorithm proceeds to create the next group. If fewer than nodes are left after the last group's formation, these remainder nodes are clustered into existing groups according to the similarities between nodes and groups. After having formed these groups, we need to ensure that each group's members are indistinguishable in terms of neighbourhood information.Thus, neighbourhood labels are modified after every grouping operation, so that labels of nodes can be accordingly updated immediately for the next grouping operation. This modification process ensures that all nodes in a group have the same neighbourhood information.The objective is achieved by a series of modification operations.

To modify graph with as low information loss as possible, we devise three modification operations: label union, edge insertion and noise node addition.Label union and edge insertion among nearby nodes are preferred to node addition, as they incur less alteration to the overall graph structure. Edge insertion is to complement for both a missing label and insufficient degree value.A node is linked to an existing nearby (two-hop away) node with that label. Label union adds the missing label values by creating super-values shared among labels of nodes.The labels of two or more nodes coalesce their values to a single super-label value, being the union of their values. This approach maintains data integrity, in the sense that the true label of node is included among the values of its label super-value.After such edge insertion and label union operations, if there are nodes in a group still having different neighbourhood information, noise nodes with non-sensitive labels are added into the graph so as to render the nodes in group indistinguishable in terms of their neighbours' labels.We consider the unification of two nodes' neighbourhood labels as an example.One node may need a noisy node to be added as its immediate neighbour since it does not have a neighbour with certain label that the other node has; such a label on the other node may not be modifiable, as it is already connected to another sensitive node, which prevents the re-modification on existing modified groups.

Algorithm 1: Global-Similarity-based Indirect Noisy Node Algorithm

Input: graph $G(V, E, L, L^s)$, parameter l;
Result: Modified Graph G'

```
while V_left > 0 do
    if |V_left| ≥ l then
        compute pairwise node similarities;
        group G ← v_1, v_2 with Max_similarity;
        Modify neighbors of G;
        while |G| < l do
            dissimilarity(V_left, G);
            group G ← v with Max_similarity;
            Modify neighbors of G without actually adding noisy nodes ;
    else if |V_left| < l then
        for each v ∈ V_left do
            similarity(v, Gs);
            G_Max_similarity ← v;
        Modify neighbors of G_Max_similarity without actually adding noisy
        nodes;
Add expected noisy nodes;
Return G'(V', E', L');
```

In this algorithm, noise node addition operation that is expected to make the nodes inside each group satisfy sensitive-label-diversity are recorded, but not performed right away. Only after all the preliminary grouping operations are performed, the algorithm proceeds to process the expected node addition operation at the final step. Then, if two nodes are expected to have the same labels of neighbours and are within two hops (having common neighbours), only one node is added. In other words, we merge some noisy nodes with the same label, thus resulting in fewer noisy nodes.

V.METHODOLOGY

Main Modules:

1.Authentication Module:

In this module, Users are having authentication and security to access the detail which is presented in the system. Before accessing or searching the details user should have the account in that otherwise they should register first.

2.Social Network:

The user will demonstrate social network features wherein he will perform following operations:

•Edit Profile
•View and Add Friends
•Search Users
•View User Profile

3.Sensitive Label Privacy Protection:

This module facilitates the system to compare features of both user profiles the one who is accessing the profile and the one whose profile is being accessed. Based on the attributes compared the system generates a weighted graph of associated attributes using which selected attributes are identified. This is very useful to identify sensitive data to be hidden and data that should be made visible to users from the unknown users.

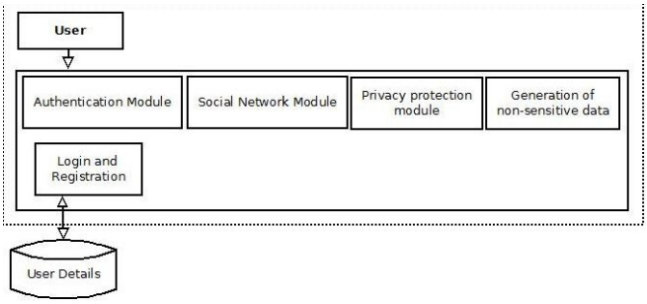

Fig 1. System architecture diagram

VI.CONCLUSION:

In this article, we argue that these different privacy problems are entangled, and that OSN users may benefit from a better integration of the three modules.
1.Authentication Module
2.Social Network
3.Sensitive Label Privacy Protection

Also, we can publish the Non sensitive data to everyone in social Network.It's providing privacy for the user profiles so that unwanted persons not able to view your profiles.

REFERENCES:

[1]E. de Cristofaro et al., ―Hummingbird: Privacy at the Time of Twitter,‖ IEEE Symp. Security and Privacy, IEEE CS, 2012, pp. 285–299.

[2]J. Anderson and F. Stajano, ―Must Social Networking Conflict with Privacy?‖ IEEE Security & Privacy, vol. 11, no. 3, 2013, pp. 51–60.

[3]A. Cutillo, R. Molva, and T. Strufe, ―Safebook: A PrivacyPreserving Online Social Network Leveraging on RealLife Trust,‖ Communications Magazine, vol. 47, no. 12, 2009, pp. 94–101.

[4]F. Beato, M. Kohlweiss, and K. Wouters, ―Scramble! Your Social Network Data,‖ Privacy Enhancing Technologies, LNCS 6794, Springer, 2011, pp. 211–225.

[5]J. Anderson et al., ―Privacy-Enabling Social Networking over Untrusted Networks,‖ ACM Workshop Online Social Networks (WOSN 09), ACM, 2009, pp. 1–6.

[6]A Trust-based Privacy-Preserving Friend Recommendation Scheme for Online Social Networks‖ Guo, L.; Zhang, C.; Fang, Y; Publication Year: 2014.

[7]Asymmetric Social Proximity Based Private Matching Protocols for Online Social Networks‖ Thapa, A.; Li, M.; Salinas, S.; Li, P. Publication Year: 2014.

[8]Fairness-Aware and Privacy-Preserving Friend Matching Protocol in Mobile Social Networks‖ Haojin Zhu ;SuguoDu ;Muyuan Li ; ZhaoyuGao. Publication Year: 2013, Page(s): 192 – 200.

[9]Multiparty Access Control for Online Social Networks: Model and Mechanisms‖ Hu, Hongxin ;Ahn, Gail-Joon ; Jorgensen, Jan. Publication Year: 2013 , Page(s): 1614 – 1627.