International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

Preserve data-while-sharing: An Efficient Techniquefor Privacy Preserving in OSNs

Nithish Ranjan Gowda (Research Scholar)
Department of Computer Science and Engineering
University Visvesvaraya College of Engineering, Bangalore University
Bangalore, India
nrg021182@gmail.com

Venkatesh (Associate Professor)
Department of Computer Science and Engineering
University Visvesvaraya College of Engineering, Bangalore University
Bangalore, India
Venkateshm.uvce@bub.ernet.in

Satish B Basapur (Associate Professor)
Department of Information Science and Engineering
Dr. Ambedkar Institute of Technology,
Bangalore, India
satish.basapur@gmail.com

Abstract— Online Social Networks (OSNs) have become one of the major platforms for social interactions, such as building up relationships, sharing personal experiences, and providing other services. Rapid growth in Social Network has attracted various groups like the scientific community and business enterprise to use these huge social network data to serve their various purposes. The process of disseminating extensive datasets from online social networks for the purpose of conducting diverse trend analyses gives rise to apprehensions regarding privacy,owing to the disclosure of personal information disclosed on theseplatforms. Privacy control features have been implemented in widely used online social networks (OSNs) to empower users in regulating access to their personal information. Even if Online Social Network owners allow their users to set customizable privacy, attackers can still find out users' private information by finding the relationships between public and private information with some background knowledge and this is termed as inferenceattack. In order to defend against these inference attacks this research work could completely anonymize the user identity.

This research work designs an optimization algorithm thataims to strike a balance between self-disclosure utility and their privacy. This research work proposes two privacy preservingalgorithms to defend against an inference attack. The research work design an Privacy-Preserving Algorithm (PPA) algorithm which helps to achieve high utility by allowing users to share theirdata with utmost privacy. Another algorithm-Multi-dimensional Knapsack based Relation Disclosure Algorithm (mdKP-RDA) thatdeals with social relation disclosure problems with low computational complexity. The proposed work is evaluated to testthe effectiveness on datasets taken from actual social networks. According on the experimental results, the proposed methodsoutperform the current methods.

Keywords- Online Social Networks (OSNs), Privacy Preservation, Data Utility, Inference attacks, Social Relations, Published Attributes.

I. INTRODUCTION

The usage of social networks on the Internet has increased significantly in recent years. Social networking sites like Facebook, Twitter, and LinkedIn are all examples of social networks sites that people frequently use. People can no longer imagine their lives without the constant presence of social networking sites. Social media accounts are where people keep data like birth dates and current locations. People keep everything, from bookmarks and photographs to email addresses and phone numbers, in the cloud. Through blog comments, tweets, and tags, people communicate with a wide audience. There are several online social networks in use today, and they all have their own features. Online social networks such as like Facebook, Friendster, and MySpace etc., seek to build a comprehensive digital profile of a user by collecting and analysing a wide range of data about that person. Further, they facilitate communication between users. By collecting and evaluating a user's information from a variety of sources, online status networks such as Twitter aim to create a detailed digital profile of the individual. In addition, they make iteasier for people to talk to one another. Online social networkssuch as ReseachGate, LinkedIn aims to bring together people with similar interests. For instance, LinkedIn is a business- oriented social networking platform that connects recruiters with qualified candidates. Online social neighbouring networksaims to locate nearby people for the purposes of information sharing, media file sharing, and social interaction. Searching for neighbours relies heavily on location data because these exchanges can lead to in-person meetings. There are three distinct contexts where privacy in online social network must be preserved

- User data must be protected at the node level.
- User attributes such as age, sex, interests, location,

andso on should be kept private.

- Users' friendship and association data should be kept private

An invasion of data privacy through behavioural advertising. These behavioural commercial advertising are based on individual user interest. Behavioural advertising access the user's location, relationship status etc., For financial gain online social network service provider makes regular use of a data provided on social media profiles, which results in identity theft [1]. In recent years, several privacy breach case such child abuse, stalking and catfishing are reported on online social network [2][3]. The bullying of children prompted strict age restrictions and other safety measures on OSN.

This research paper presents a new paradigm for sharing social network data that prioritizes user self-disclosure data utility while ensuring privacy protection, with the aim of mitigating inference attacks. The privacy models under consideration aim to maintain the integrity of both the data and context of information shared inside a network or uploaded to servers and third-party applications. The frameworks is designed in this research work provide user privacy-preservation solutions that preserve both other users (Node) and link information connected to the user. It identifies various attacks such as identity-based, location-based, eavesdropping manipulation based and device based attacks and propose a technique to thwart these attacks. *Motivation:* Ensuring users get maximum benefits from the services provided on Online Social Network while also preserving their privacy is of paramount importance. Protecting the sensitive information of individuals on online social networks (OSNs) is of utmost importance, particularly when such information is at risk of being exploited or leaked through the analysis of publicly available datasets and the attackers' background knowledge. Balance trade-off between excessive concealment of sensitive information and the self-disclosure utility of OSN by user. The disclosure of data obtained via social networks would directly undermine the privacy of individuals. It is an indispensable task for network data publishers to preserve data privacy. *Contribution:* In this research work, we have designed an optimization algorithm that achieves a balance between self-disclosure utility and their privacy.

- In this work, Social-attribute network model is designed to describe original social network data and attacker's knowledge.
- A self-disclosure rate is defined to measure the privacy loss of user secrets in a published network regardless of background knowledge of the attacker.
- This research presents a unique model for sharing social network data while ensuring privacy preservation. The proposed strategy aims to optimize the utility of user self-disclosure while providing privacy assurances in order to defend against the inference attack.
- Proposed model enable a versatile assessment of self-disclosure, catering to diverse user requirements and contexts while considering various user concerns.
- Privacy-Preserving Algorithm (PPA) algorithm is proposed that helps to achieve high utility by allowing users to share their data with utmost privacy.
- A Social relation based Multidimensional Knapsack Problem disclosure algorithm (mdKP-RDA) is designed that deals with social relation disclosure problems with low computational complexity.

II. RELATED WORK

Authors in [4] have proposed a local recording-driven mechanism to preserve privacy in social networks. The proposed methodology adopts differential privacy to construct the framework. The proposed framework protects user privacy. However, the proposed framework does not guarantee reliable user privacy The various identity anonymization techniques are used to preserve the user's data privacy. However, the identity of a user is revealed using available public information [5]. Author in [5] designed an anonymized dataset that satisfies l-diversity anonymity. To achieve l-diversity the author designed MaxSub, MinSub graph manipulation algorithms, MaxSub algorithm deletes only edges which disclose more privacy while MinSub performs insertion of edges or vertices to achieve l-diversity anonymity. The anonymisation models used for protecting the private information of users in social networks will result in loss of information. So in [6] the author has used centrality measures to identify the importance of nodes in the social network and then anonymization by preserving important nodes. In [6] two different models of anonymization methods namely the k-degree anonymity achieved throughthe Fast K-Degree Anonymization algorithm (i.e., graph-modification anonymization approach) and the k-anonymity for social networks model achieved through the Sangreea algorithm (i.e., clustering-based anonymization approach) are proposed. The location privacy of users is disclosed in many mobile social networks. In [7] the author proposes a radius-constrained dummy trajectory algorithm for privacy preservation scheme in MSN (Mobile Social Networks). The proposed scheme generates a dummy location set for the user's real location by constraining the radius where a user can send the LBS (Location based service) request. Though there are various algorithms for privacy preservation which cannot be directly applied to a social network as there are structural properties along with labels for nodes. In [8] a method named GASNA (Greedy Algorithm for Social Network Anonymization) with three phases namely the clustering phase, adjustment phase, and anonymization phase is proposed. The clustering phase involves the process of gathering the nodes with a similar structure to form clusters. The adjustment phase involves the process of moving the nodes from a cluster that has less than k-nodes into a cluster with similar properties. Anonymisation phase involves either addition of edges by adding fake nodes, fake edges or deleting edges of user's behavior and the relationship between the users. Many popular OSNs use centralized architecture where a single service provider develops and deploys the OSN system. Though it eases the job of updating, an extension of the network, and manipulating architecture. However it enables attackers to build social network graphs. In [9] the author proposes three classes of servers namely the first class server, second class server and third class server. First class server includes Diaspora and OneSocialWebwhich uses federated architecture for independent servers, second class aims to protect data from storage providers using end to end encryption and third class uses Distributed Hash Table for server architecture. Even though we anonymize the user's identity it's still possible for an attacker to find theuser from the published anonymized records of a user ona social network. In [10] a k-couplet anonymity method is introduced to protect privacy under attribute couplet attacks. In this method if the dataset contains at least k-1 couplets having the same attributes then the dataset is said to satisfy k-couplet anonymity. In order to promote k-couplet anonymity the author has proposed 3 algorithms namely, Attribute Generalization (AG), Attribute Cluster Anonymisation (ACA), and Approximate Multiple-Attribute Generalization (AMAG). The three potential privacy leakage problems such as Edge weight disclosure, Link Disclosure and Identity disclosure are solved in [11]. A greedy algorithm by name MinSwap which uses weight unlinkability knowledge is designed in order to protect edge weight disclosure problems. Further, delta-MinsawapX is an improvised version of MinSwap which solves all three issues: identity disclosure, link disclosure and edge weight disclosure problem. In order to use various data running and ML techniques used to process the huge data generated by the OSN, the social network graph should be converted into a low-dimensional vector which is prone to privacy leakages. In [12] a model named LPPG (Link-Privacy Preserving Graph) is proposed in order to preserve privacy along with achieving privacy utility tradeoff between utility and privacy. There are various techniques based on graph generation and differential privacy to protect users' identity in online social networks. However these techniques do not provide optimal data utility. In [13] the author proposes an approach based on differential privacy and field theory which involves 2 steps. The approach encompasses a two-step process for the dissemination of a social network. In the initial stage, the degrees of the nodes are disrupted using differential privacy techniques by introducing noise that adheres to a Laplacian distribution. In the second step, the edges of the social network are synthesized using field theory. The present study introduces a field theory model to analyze social networks, drawing inspiration from the principles of gravity in physics. By establishing a connection between the gravitational field in physics and the proposed field theory model, a simulation-based approach is employed to investigate the dynamics of social networks. In the process of edge formation, the selection of the starting node is biased towards nodes with high degrees, indicating a preference for nodes with a large number of connections. Subsequently, the selection of the ending node is biased towards nodes with a strong interaction force with the starting node. The proposed strategy demonstrates a higher capacity to maintain genuine social connections in contrast to earlier methodologies. Additionally, it does not result in the loss of structural attributes within the datasets, such as degree distribution and clustering coefficients. However this method will preserve only the structure information of social networks. But in the case of real social networks that contain a substantial amount of attribute information, this model fails to maintain the topological characteristics and the correlations between attributes and edges. Due to the large volume of data and high sensitivity it is challenging for privacy protection schemes to allocate a reasonable amount of noise, while preserving the desirable data and executing data utility services efficiently. In [14], the privacy protection strategy known as PBCN (Privacy Preserving strategy Based on Clustering and Noise) is founded on the principles of clustering. The proposal consists of five algorithms, namely random disturbance based on clustering, network reconstruction following disturbance of degree sequence, and production of noise nodes, among others. In addition, a privacy measure method is proposed that utilizes the concept of adjacency degree. This algorithm aims to provide an objective evaluation of the effectiveness of different strategies in preserving privacy against attacks targeting graph structure and degree. Simulation studies are carried out in order to undertake performance comparisons among the following techniques: PBCN, Spctr Add/Del, Spctr Switch, DER, and HPDP. The experimental findings demonstrate that the implementation of PBCN leads to improveddata availability and execution efficiency. Ultimately, the studyof parameters utility reveals that PBCN has the capabilityto strike a balance between the availability of data and the level of privacy protection. However PBCN is more complex if we try to reduce complexity then there is a chance of losing data availability. The traditional Deep Packet Inspection(DPI) Mechanisms like NIDS and NIPS, due to granularity limitation and poor performance cannot efficiently adapt to privacy preservation and privacy detection in OSN (Online Social Network). In [15] a privacy-preserving framework that is based on domain gateway called Shutter Roller is used. Existence of the social features such as user generated contentsand user behaviors, that causes privacy leakage is examinedby Shutter Roller by the detection of OSN traffic through the gateway. In case of weighted neighborhood attack, the attacker is considered to have information on the target's 1- neighborhood graph as well as degrees and edge weights.Using this data, an attacker can find the identity of a target given that any node's 1-neighborhood is isomorphic with (k-1) other nodes. In [16] the author introduces a heuristic indistinguishable group anonymization (HIGA) scheme to build an anonymized social network which includes four steps namely Node grouping, Approximate Matching Test, Group Anonymization and randomization. In cyber physical social networks (CPSN), an enormous amount of data is frequently shared between users. In order to provide privacy in CPSN a privacy protection scheme based on differential privacy is used which introduces noises into the social network. However this creates an unexpected relationship between noises and social actors that eases the process of identifying secrets. The two major attacks on customisable privacy protection are background attacks and collusion attacks. In [17] the author aims to offer customisable protection to every user and ensuresusers are attack resistant using a model called customizable reliable differential privacy model (CRDP). In order to providequality services for users Various Data mining applicationsuse huge crowd sourced data of mobile devices available on social networks. Though users avail quality service, exposing these data to the public leads to privacy leakage of mobile users. In [18] the author introduces a scheme that generates groups from regions with minima statistics based on similarity of data change and further in order to reduce perturbationerror, laplace noise is added to group instead of region. This scheme is called REal-time Spatiotemporal Crowd-soUrcEd Data Publishing with Differential Privacy.

III. Problem Statement

The major problem in online social networks is how to preserve user’s privacy. Generally, online social networks provide a platform to publish the data in such a way that users’ privacy is protected and allow the maximum utilization of the data (i.e, the published data is capable of predicting new important decisions from the ML model). A design greedy based method that preserves privacy of a data and allows data analyser or data analytics to utilize data at maximum level to perform knowledge discovery. For example, the data utility feature of instagram provides recommendations of ads, reels etc to the user. At the same time, the user’s privacy should also be protected.

IV. Preliminaries, Terminologoes And Methodology

A. Social Attribute based Network

A social attribute network is a representation of a social network that incorporates both social actors (individuals or entities within the network) and their attributes (characteristics or information associated with them). In this model, we have the following components:

V_N (Social Actor Set): This set represents the social actors within the network. These could be individuals, organizations, or any entities that interact in the social network.

V_A (Attribute Node Set): This set represents the attributes associated with the social actors. Attributes could include information like age, gender, location, interests, etc. These attributes help in characterizing the social actors.

E_N (Social Relation Set): This set represents the relationships or connections between the social actors. For example, ina social network, relationships could be friendships, following,co-authorship, etc.

E_A (Attribute Link Set): This set represents the links or connections between attributes and social actors. It indicates which attributes are associated with which social actors.

The categorical attribute and numerical attributes with the social actors and their relationships, the social-attribute network model provides a comprehensive representation of the network.

B. Privacy-Inference attack

In a social attribute network, a privacy deduction attack involves an attacker using both publicly available information from available social networks and prior knowledge to infer sensitive attributes and relationships of users. This attack can be seen as a special case of link prediction, where the goalis to predict connections or attributes that are not explicitly provided in the dataset. To model this attack, a knowledge graph is employed. This graph, referred to as the attack graph (GA), encapsulates the background knowledge of the attacker. It includes the statistical Information and Node and Edge Information, the statistical Information is derived from known statistics or from the available dataset. It represents probabilities or likelihoods of certain attributes or relationships given other attributes. Node and Edge Information used to infer relationships between users based on their shared interestsor activities, even if these relationships are not explicitly mentioned in the published data.

Example: Given original Social Network with user A,B,C, D and information about user is as follows: User A: A1=Senior, A2=Urban, S1=Yes User B: A1=Young, A2=Suburban, S1=No User C: A1=Middle-aged, A2=Rural, S1=Yes User D: A1=Senior, A2=Urban, S1=Yes

Next, attribute Inference Attack from attacker, using the information gathered from external sources, can infer that older individuals are more likely to have the medical condition.The attacker then examines the social network and identifies User B, who is young and doesn’t have the condition. They can then infer that User B is less likely to be older based onthe absence of the medical condition.

C. Adversarial Ability

An external entity that is interested in accessing the hidden information of users within a social network. The user engages with a service provider or provider and discloses publicly available information that is maintained within the social network platform. The service provider utilizes the publicly available information to create a structured input for its assault model. The goal of this attack model is to predict whether the user has a specific secret attribute.

Example: given Public Information on User A: Age (25-34), Location (Urban), Interests (Technology, Travel), User B: Age (35-44), Location (Suburban), Interests (Food, Music), User C: Age (18-24), Location (Rural), Interests (Art, Sports). With these information, adversary predicts whether a user is likely to be a Programmer.

D. Utility and Privacy

Utility refers to the usefulness or benefit that users gain from sharing their information. Privacy concerns the protection of personal information. Users want to ensure that sensitive or private details are not exposed to unauthorized parties.The platform needs to find a balance between providing useful and personalized experiences for users (utility) while also safeguarding their sensitive information (privacy). Users should also have control over the level of information they share, allowing them to customize their privacy settings based on their comfort level and preferences.

The utility of a social attribute is influenced by its semantic properties and the needs of third parties. To assess attribute utility in a more general manner, we examine the attribute's neighbors within the social network. This approach generally reveals how prevalent or common the attribute is throughout the entire social network.

Uniqueness score of an attribute (a) within a network context is calculated based on information theory principles, it is observed that attributes with fewer social actor neighbors convey more unique information. The uniqueness score of an attribute (a) is calculated using equation 1.

$$Pr_U(a) = \frac{1}{log(|N_a|) + 1} \qquad (1)$$

Log (N_a) represents the number of social actor neighbors associated with attribute a. It's the degree centrality of the attribute, which measures how many other nodes are directly connected to it. As N_a increases, the denominator log (N_a)+1 also increases. This means that as an attribute has more social actor neighbors, its uniqueness score $Pr_{U(a)}$ decreases. An attribute with many neighbors is considered less unique because it's shared by more individuals. Conversely, if an attribute has fewer neighbors, the uniqueness score increases. This indicates that the information carried by that attribute is more distinctive, making the user associated with it more unique in the network.

Commonness of the attribute a and social actor U is given by the number of social actors who are friends of actor U and has the attribute a divided by the number of friends of U.

$$Pr_U(a, U) = \frac{|N_U| \cap |N_a|}{|N_U|} \qquad (2)$$

This research work use either *uniqueness* or *commonness* score to find the utility of the attribute.

The value of an edge between two social actors in a network based on node resemblance between two social network's actors. Jaccard Coefficient, score of Adamic/Adar Score indicate the node resemblance between two social actors.

The *Jaccard Coefficient* is a measure of similarity between the sets ofneighbors of two nodes. Higher Jaccard coefficient is equation3 indicates more common friends.

$$PrJa(e_{u,v}) = \frac{|N_u \cap N_v|}{|N_u \cup N_v|} \qquad (3)$$

The Adamic/Adar Score indicate ”rarity” of common features between two nodes/actors in social network, it implies astronger connection between them.

$$PrAd(e_{u,v}) = \textstyle\sum_{k\epsilon\{f_u \cup f_v\}} \frac{1}{log|N_k|} \qquad (4)$$

V. MATHEMATICAL MODEL

The framework for quantifying privacy disclosure in a social network context. This research work introduces concepts like *disclosure risk*, *self privacy disclosure*, and *privacy guarantees* using mathematical expressions.

Disclosure Risk: This is the likelihood of the most possible sensitive attribute assignment considering background knowledge in privacy-preserving data sharing.

$$Pr\{\, t\_\{u\}(s) \;=\; 1|GA, GP\} \;=\; Pr\{t_A u(s) = 1\;|g(A^p{}_u)\,\}\,(5)$$

Here, $t_A u(s)$ = 1, means that sensitive attribute s of social actor u is disclosed.

A. Self-Privacy Disclosure

Self data Privacy Disclosure: The data privacy disclosure rate/indicator of a social actor's confidential/secret (s) in the social graph G considering both attributes and social relations. The self data privacy revelation/disclosure from the viewpoint of attributes Φ_A and social relations Φ_N, is given in equation 6 and 7.

$$\Phi_A(u, s, GP\,) = Pr\{tu(s) = 1|A_v \cap A_u\,\} \qquad (6)$$

Equation 6 measures disclosure considering attributes.

$$\Phi_N(u, s, GP\,) = Pr\{tu(s) = 1|N_v \cap N_u\,\} \qquad (7)$$

Equation 7 measures disclosure considering social relations.

Privacy Guarantee: This research work defines the outset or threshold for self data privacy revelation/disclosure. An operation is considered privacy preserving if it satisfies constraint (i.e. the distinguish between the adversary's prior and adversary's later knowledge about the sensitive and private information is meager enough).

The Pr t_u (s) = 1 indicate adversary's prior knowledge on sensitive information 's', ϵ is the non-negative parameter called 'privacy budget', regulating the proximity between the rate of self-privacy disclosure and the prior probability. The another parameter 'δ' controls the tolerance of privacy disclosure. The privacy guarantee is defined as:

$$\Phi(u, s, GP\,) = \le\; exp(\epsilon)Pr\{t_u(s) = 1\} + \delta \qquad (8)$$

User's Privacy Concern: In this research work, User' Privacy Concern is represented as tuples consisting of secret attributes 's', privacy budget 'ϵ', and tolerance 'δ' andC= (s,ϵ,δ) represents the aggregation of all privacy settings.

Privacy-Preserving Graph: The disclosed graph (GP) is considered privacy-preserving If it meets the requirements of the privacy guarantees for all users.

Example: Consider a social network with three users: A, and C. They have secret attributes denoted as S_1, S_2, S_3 respectively. Their privacy concerns are as follows:

A(S_1, ϵ_1, δ_1) with ϵ_1 = 0.1, δ_1=0.05,
B(S_2, ϵ_2, δ_2) with ϵ_2 = 0.2, δ_2 = 0.1,
C(S_3, ϵ_3, δ_3) with ϵ_3 = 0.15, δ_3 = 0.08,

Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*

Let's say the prior probabilities of their secrets being disclosedare: Pr{$t_u(s_1)$ =1} =0.3 , Pr{$t_u(s_2)$ = 1} = 0.2, Pr{$t_u(s_3)$ =1} = 0.25.

If the disclosed graph GP satisfies the privacy guarantees for all users according to the defined thresholds (as defined in Equation 9), then it can be considered privacy-preserving. This means that the disclosed information about each user's secret attributes adheres to their specified privacy concerns.

$$\Phi(u, s, GP) \leq \Theta_u, \forall_u \epsilon V_N \qquad (9)$$

Here, Θ_u is privacy threshold vector $\theta_{u,i}$ and it defines as:

$$\theta_{u,i} = exp(\epsilon)Pr\{t_u(S_{u,i}) = 1\} + \delta_{u,i} \qquad (10)$$

B. General Self Disclosure Problem

The goal of this research work is to allow users to share as much personal information as possible while ensuring privacy. This is achieved by masking certain edges in the social- attribute network.

The masking process start with the network consists ofnodes (both users and attributes) with no edges. Edges are added to the network. The traditional social network with data sharing problem is expressed as follows. Given a social network graph (G) with nodes (V_N), attributes (V_A), edges(E_N, E_A). Users have privacy concerns represented by C = S, ϵ, Δ . There's a data utility function p(T) that measures the value of disclosing a set of edges (T). The objective is to find a disclosed social network (GP) with a disclosed edge set (T = E_N, E_A) such that privacy requirements are satisfied with maximum utility. The goal is to find the maximum utility (y) by selecting a set of edges (T) from the union of user-user and user-attribute edges, subject to privacy constraints. The maximum utility is expressed as follows:

$$y = max_{T \subset E_N \cup E_A}\{p(T) : \Phi(u, S_u, T) \leq \Phi_u, \forall_u \epsilon V_N\} \quad (11)$$

Φ_u is computed using Equation 10 with values of *S*, ϵ, Δ

The self privacy disclosure function does not follow *submodular and monotonic Functions*. Example for *Non-submodularity*: Example Network (G): Users a, b, c, d, e, f, Attributes S, A_1, A_2 Edges (EA): (a, S), (a, A_1), ... Consider T_1 and T_2 defined as in the equation 11. Add an edge e=(a, A2). It understood that adding e to T_1 is not as beneficial as adding it to T_2, which demonstrates non-submodularity. Example for *Non-monotonicity*: Using the same network and edges as in the previous example. Consider e1=(a, A_1) and e2=(a, A_2) along with set T defined as in the equation 11. It understood that adding e_1, then adding e_2, does not adhere to the definition of monotonicity.

Due to non-submodular and non-monotonic nature of the self privacy disclosure function, addressing the general problem of data sharing in social networks is challenging.

To make self privacy disclosure function to follows *sub-modular and monotonic functions*, this research work consider separate attribute and relation disclosure problems based on different assumptions about adversarial abilities.

C. Attribute Disclosure Problem

Each user has an independent profile. Changing one user's profile doesn't affect the disclosure strategies of other users. Therefore, attribute disclosure problem is considered for each individual user independently. attribute disclosure problem is formulated optimization problem with Maximize the sum of the utility values (p_i) associated with disclosing the public attributes (x_i) for a user *u*.

$$\sum_{i=1}^{|p_u|} p_i x_i \qquad (12)$$

The optimization should satisfy the following constraints:

- Ensure that the self data privacy revelation/disclosure (Φ_A) of user u's secret s_j, based on the vector of attribute disclosures **x**, is less than or equal to a privacy protection threshold ϑ_j for each secret s_j.

$$\Phi_A(u, s_j, X) \leq \theta_j, \forall j = 1, 2..|S_u| \qquad (13)$$

- x_i takes binary values (0 or 1) represent whether to revelation/disclose the corresponding public attribute a_i.

$$x_i \epsilon \{0, 1\}, \forall i = 1, 2, ..|P_u| \qquad (14)$$

D. Social relation disclosure problem

Social relation disclosure problem in social networks involves relation between two or more social actors. While disclosing social relation of an actor, it is necessary to consider influence of social relation on other actors specifically in directed and undirected networks.

Attribute disclosure problem in directed social network refers to revealing information about a single social actor (likea user) without involving other actors.

Example: disclosing the interests of a user without affecting others. The social connection/relation revelation/disclosure problem in directed social network refers to revealing the successors (whom a user follows) rather than the followers (who follow the user). The removal of a directed social relationdoes not affect its reverse relation. Example: On Twitter, disclosing who a user follows without revealing who follows them.

The social relation disclosure problem can be formulated as follows:

Objective is to maximize a function involving edge weights (x)

$$\sum_{i=1}^{|E_N|} p_i x_i \qquad (15)$$

Subject to protection constraints.

$$\Phi_N(u, s_j, x/GP) \leq \Theta_{k,j} \qquad (16)$$

where $\Theta_{k,j}$ = exp(ϵ)Pr $t_{u_k}\{(s_{k,j}) = 1\}$ $\delta_{k,j}$, all social network actors and their confidential/secrets information protection constraints are considered while preserving privacy.

Term $\Theta_{k,j}$ indicate weighted combination of probability and protection factor. The term pr $t_{u_k}(s_{k,j})$ represent probability of some event happening. $\delta_{k,j}$ indicate protection factor. The term s_{u_k} is set of successors of social actor u.

Example: Let's consider an undirected social network with 4 users: *A*, *B*, *C*, and *D*. The edges represent friendships. *A is friends with B. B is friends with C. C is friends with D*. The goal is to disclose some relationships while respecting privacy constraints. Objective is to maximize the sum of weights of the disclosed edges with constraints to ensure that disclosing any edge doesn't violate privacy constraints for any user. For instance, if disclosing the edge (A, B) has a higher weight compared to (B, C), the optimization problem would aim to prioritize revealing the friendship between A and B. The problem arises because removing an edge (e.g., (B, C)) affects both B and C.

VI. Algorithms

A. Privacy Preserving Algorithms (PPA)

In this section, description of Privacy Preserving Algorithms (PPA) is given, this research work co-relate the social network privacy preserving problem to the Knapsack problem, PPA solving social network privacy preserving problem.

Every edge of the Social network graph as an item in a knapsack. The cumulative impact of the chosen elements on the confidentiality/secret of social actor n, as measured by the rate of self-disclosure in terms of self/personal privacy is considered as the weight of the edge/item. The utility of the selected items/nodes is considered as profit gained. The aim is to find the maximum utility possible with the minimum self privacy disclosure rate. The total contribution(i.e., self privacy disclosure rate) measures the significance of specific elements to a social actor's secret.

$$w_s(T_{sel}) = \Phi(u, s, T_{sel}) \qquad (17)$$

Equation 17 indicates that if a social actor '*u*' with a secret '*s*'. If T_{sel} is the set of selected items, then the self privacy disclosure rate $w_s(T_{sel})$ quantifies how much information about 's' is revealed by the selected items.

Contribution of a single item is computed using equation 18.

$$w_{s,t}(T_{sel}) = \Phi(u, s, T_{sel} \cup \{t\}) - \Phi(u, s, T_{sel}) \qquad (18)$$

It's the incremental contribution of a single item '*t*' to a social actor's secret '*s*', given the set of selected items 'T_{sel}'. Example: If '*t*' is added to the set of selected items, the contribution '$w_{s,t}$ (T_{sel})' is computed as the difference in total contribution with and without '*t*'. The aforementioned procedure is iteratively executed until all edges have been visited, enabling a comprehensive comparison of all edges, which may represent attribute linkages or social relations. Through this comparison, the most appropriate edge is determined at each iteration. The efficiency of an edge is determined by Equation 19.

$$\rho = \frac{P_i}{\sum_{j=1}^{m} b_j, w_{i,j}} \qquad (19)$$

For each edge (attribute link or social relation), an efficiency $\rho$is calculated. This efficiency is based on the value-to-weight ratio, considering multiple constraints with different thresholds. Example: An edge with a higher efficiency provides more utility while leaking less information about the secrets.

The pseudo code of privacy preservation algorithm (PPA) is given in Algorithm 1. PPA algorithm is based on greedy approach to solve knapsack edge masking problem. Algorithm1 select the edges of the nodes which have high utility and with minimal leakage of information about private attributes while satisfying all the privacy requirements. Initially the utility of all the edges is pre-computed. in every iteration, weights of all secrets is computed and for every edge we will find ρ, whichis the ratio of edge utility to the total sum of ratios of weights of secrets to its threshold value. The edge with maximum ρ and satisfying all privacy constraints is selected.

Algorithm 1 iteratively select items based on their efficiencies and how well they meet the privacy constraints specified by the thresholds. The final output will give us the optimal selection of items that maximizes the value while minimizing the disclosure of sensitive information.

Algorithm 1 Privacy Preservation Algorithm (PPA)

```
Require: $\vec{S} = \{S_1, S_2, \ldots S_n\}$, list of secret of actor
         $\vec{N} = \{N_1, N_2, \ldots N_n\}$, list of actor's neighbors
         $\vec{\Theta} = \{\Theta_1, \Theta_2, \ldots \Theta_n\}$, list of secret threshold
Ensure: result set Sel
Calculate Privacy using Jaccard Coefficient
$\vec{P} = \{P_1, P_2, \ldots P_n\}$, $Pr_{Ja}(e_{u,v}) = \frac{|N_u \cap N_v|}{|N_u \cup N_v|}$
For every social relation existing between social actor u and social actor v:
$P(u,v) = \frac{Total\ commonneighbor\ of\ u\ and\ v}{Total\ neighbor\ of\ u\ and\ v}$
$C = V_n$ (Set of vertex set of social actors)
$Sel = \phi$, $V_{max} = 0$, $\vec{l} = \{1,2,\ldots n\}$
while { until $\vec{l} = \phi$} do
    Initialize $\rho_{max} = -1$, $s = -1$, $w_{sel} = \phi$
    for {every i in $\vec{l}$ } do
        for {J=1,2,…n} do
            Calculate $w_j$ : $w_j = \frac{|C \cap N_i \cap S_j|}{|C \cap N_i|}$
        end for
        Calculate $\rho$ : $\rho = \frac{p_i}{\sum_{k=1}^{m} w_j/\Theta}$
        if { $\rho > \rho_{max}$ } then
            $\rho_{max} = \rho$, $s = i$, $w_{sel} = w_j$
        end if
    end for
    if { $w_j \leq \Theta_j$ and every $j \in \{1, 2, \ldots n\}$} then
        $Sel = Sel \cup \{s\}$, $C = C \cap N_s$, $\rho_{max} = \rho_{max} + \rho_s$
    end if
    Remove s from $\vec{l}$
end while
return $\rho_{max}$, Sel
```

For each node actor, the time complexity is O (n2 m. |VN|), where, n represents the quantity of attributes, while m is the quantity of secrets. |VN| represents the size of the set of all items. The algorithm1's time complexity for the entire network is O(|S|.|VN|.| EN |2), where, |S| is the The aggregate quantity of all constraints or secrets, |VN| is the size of the set of all items, and |EN| is the size of the set of all edges in the network.

B. Social relation based dynamic knapsack problem (mdKP-RDA)

The PPA algorithm exhibits a high temporal complexity dueto its consideration of all attributes and social actors' relationships when assessing self-privacy disclosure. One potential consequence of ignoring correlations and assuming conditional independence among public information is the potential a decrease of privacy protection. This is due to the possibility that the combination of two or more public attributes or social actors' relations provide a greater amount of information than what can be inferred from each attribute or relation alone. However, this will also streamline the issue by ascertaining the significance of each attribute or social relationship.

The Social relation based dynamic knapsack problem (mdKP-RDA) simplified version of the optimization problem is proposed in this section, the objective of mdKP-RDA algorithm is to maximize the total value while ensuring that the total information gained about the secrets is below a threshold

First, transform the original relation disclosure problem into a multi-dimensional knapsack problem, with a focus on how to assign fixed weights to each social relations based on constraints (equation 13 and equation 14). It also introduces the concept of mutual information to quantify the relationship between social relations and secrets.

Given node *u*, with secret information *s* and social relation *x*, calculate condition probability Pr(t_u(s) = 1). Example, probability that A's income is high given that A is connected to both B and C. This would involve calculating the conditional probabilities (shown in equation 20) based on the network structure.

$$\Phi_N(u, s, x) = Pr\{t_u(s) = 1\}, \forall N\{v_1, v_2, ...v_n\} of u \quad (20)$$

By substituting the expression for Φ_N (u,s,x) into the original constraints(equation 13 and 14) weight of each social connection/relation is found. If *'e'* is linking edge connecting node *'u'* and *'v'* then weight of edge indicate mutual information measures the dependence between two social actors *U* and v. The social actor *'u'* is linked to another social actor *'v'*of edge *'e'*, and *'uk'* possesses the secret information of '$s_{k,j}$'. Equation 21 quantify the relationship between a social connection/relation *'e'* and node u_k's confidential/secret $s_{k,j}$

$$I(e: s_{(k,j)} = \frac{Pr\{v, t_{uk}(s_{k,j})=1\}}{\{Pr\{v\}\ Pr\{\ t\_\{uk\}(s\_\{k,j\}) = 1\ \}\}} \quad (21)$$

For example: Suppose we have a social network with threeindividuals: A, B, and C, and the following information: Attributes (public information): Person A: Age: 30, Gender: Male Person B: Age: 25, Gender: Female Person C: Age: 35, Gender: Male. Secrets (private information): Person A: Income: High Person B: Income: Low Person C: Income: High Social Relations (Edges): (A, B) (A, C) (B, C). Let's say we're interested in find the probability that A's income is high given that A is connected to both B and C using equation (21).

The *mdKP-RDA* algorithm aims to select edges that provide the highest information gain while ensuring that the total information gain from all selected edges does not exceed the specified threshold. The use of a greedy approach ensures that the algorithm iteratively selects edges with the highest individual information gain. In line 3, *mdKP-RDA* algorithm calculates the information gain for a given edge *'e'* and relevant secrets $s_{k,j}$. It iterates through the relevant secrets ($s_{k,j}$) and checks if the edge *'e'* connects to that secret. If it does, it calculates the mutual information using the formula specified in the equation 21. It calculate and store the information gains for all edges in the E_N list. In line 5, the edges are then sorted in non-increasing order of information gains. Line 6 iterate through the sorted edges, adding them to SelectedEdges if they don't exceed the threshold. If adding the current edge would exceed the threshold, we break out of the loop. Finally, we return the list of selected edges *SelectedEdges*.

The *mdKP-RDA* algorithm is a faster way to find solutions for privacy protection, especially when a quick response is crucial. It achieves this by using simplified calculations and fixed weights for items.

Algorithm 2 Multi-dimensional Knapsack based Relation Disclosure Algorithm(mdKP-RDA)

```
Require: $\overrightarrow{E_N}$ = {E_1, E_2,….E_n}, list of edges in the network
         $\delta_{k,j}$: represent additional parameter, Pr: probabilities
         $\theta_{k,j}$ = In(exp(ϵ)) + $\frac{\delta_{k,j}}{Pr\{t_{uk}(S_{k,j})=1\}}$ new thresholds
calculated based on $\delta_{k,j}$ and $Pr\{t_{uk}(S_{k,j}) = 1\}$
Ensure: SelectedEdges: List of selected edges.
1:  Initialize SelectedEdges as an empty list
2:  for {Each edge e in $E_N$ and all relevant secrets $S_{k,j}$} do
3:      Find gain I(e:$S_{k,j}$) = $\frac{Pr\{v,\ t_{uk}(S_{k,j})=1\}}{Pr\{v\}.Pr\{t_{uk}(S_{k,j})=1\}}$ and store in a
        list Gains
4:  end for
5:  Sort $E_N$ in non-increasing order of information gain
6:  for {Each edge e in $E_N$} do
7:      if {Gain(e) ≤ $\theta$ } then
8:          add 'e' to SelectedEdges
9:      else
10:         break
11:     end if
12: end for
13: return SelectedEdges
```

Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*

VII. Experiment Results

To see how well our proposed privacy preservation algorithm for sharing content on social networks work, we conducted comprehensive experiments using actual social network data of Facebook and Google+. We conducted several experiments by different data utility settings to make sure it works in various situations, and we also used different existing inference algorithms to compare the performance of proposed algorithm.

A. Datasset

The Facebook dataset contains information from Facebook, specifically about people's connections, which are called *'circles'* or *'friends lists'*. The data was gathered through a Facebook app used by people who took part in a survey.

The dataset includes details about individual profiles, these circles of friends, and the networks of connections around each person. To protect people's privacy, the original IDs used by Facebook were changed to new ones. This dataset contains 4039 node and 88234 edges. Each user's profile has information in 11 different categories. These include things like *gender*, *birthday*, *where they live*, *where they're originally from*, *where they work*, *school education*, *graduate degree details* etc. In some of these categories, there are even more specific details. For example, in the *'work'* category, there's information about *where they work* and *when they started working there*.

Google+ dataset contains information from Google+, a social media platform. The data was collected from users who chose to share their circles using a *'share circle'* feature on Google+., which are groups of people with common interests or connections. The dataset includes details about individual profiles, these circles of connections, and the networks of people around each user. In total, there are 107,614 user profiles and 13,673,453 edges/connections between them in this dataset. Each user's profile has information in 5 different categories. These include *gender*, *company name*, *job designation*, *work location*, and *degree from university*).

B. State of art Methods for Comparison on Self - Privacy disclosure

To test effectiveness of our new methods, work, the experiment results of this research work is compared with following commonly used and well-known methods.

Random Mask (RND): This method randomly hides or removes certain information until all privacy requirements are met. *Naive Bayes Mask (NB)*: The *Naive Bayes classifier* calculates the likelihood of certain information being linked to a person and removes the information with the highest likelihood of revealing someone's identity.

The proposed *mdKP-RDA* algorithm aims to select edges (i.e. attribute or social relation) that provide the highest informationgain while ensuring that the total information gain from all selected edges does not exceed the specified threshold.

C. Inference Attacks via Attribute or Social relation

Set of experiments are conducted to protect sensitive information of user by controlling or avoiding inference attack. This research used several edge predictor/classifier programs (such as *Triadic*, *Jaccard*, *Resource Allocation*, *Adamic Adar* and *Preferential Attachment*) and proposed algorithm to guess someone's private information using either the information that's already public or by looking at social relation of actor(s) in the social network. The inference attack is launched with following experiment setting.

- Inference attack by local classifier *via* published attributes: The adversary gets to see all the information about everyone in the dataset, and adversary use this dataset to train their model. Then, adversary try to guess sensitive and private information about a different group of social actors based on what they learned.
- Inference attack by rational classifier *via* social relation: the adversary have only half of the dataset and published information and the social relation to train the model. After training the model, adversary try to inference the sensitive and private information of actors from other halfof dataset.

D. Privacy Protection Performance: Attribute Disclosure

The effectiveness of the privacy preservation algo- rithm(PPA) relies on a self-privacy disclosure constraint (δ). This δ parameter is crucial in determining whether the pub- lished social network can be considered privacy-preserving. It ensures that the disclosed information about an individual is kept within acceptable limits.

The performance of algorithm is depends on self-disclosure rate δ because δ is a crucial factor as it influences how much information is disclosed. When δ is smaller, the algorithm is more conservative in what it reveals. Set of experiment is conducted on small *Facebook* ego network with 414 users. The targeted secret is the *education attribute School* which 224 users have. Before applying the PPA algorithm, the adversary is able to successfully infer information about 193 out of the 224 users. This results in a Precision of 85.80%, Recall of 79.24%, and F-Score of 82.51% (as shown in figure 1).

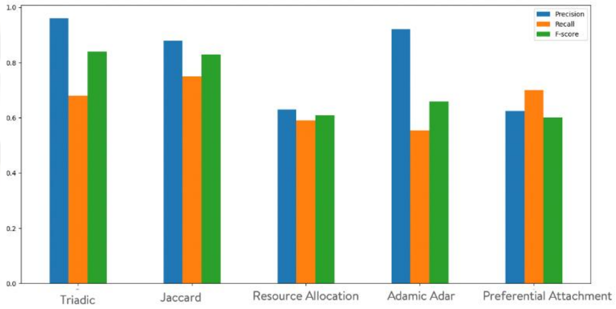


Fig. 1. Performance of adversary inference attacks on FB dataset before applying PPA.

After applying the PPA algorithm with a δ valueof 0.3, the adversary's performance in the inference attack is significantly hindered. Now, the adversary can only correctly identify 23 users out of the original 224. This leads to a much

***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

lower Precision of 16.43%, Recall of 18.30%, and F-Score of 17.36% (as shown in figure 2).

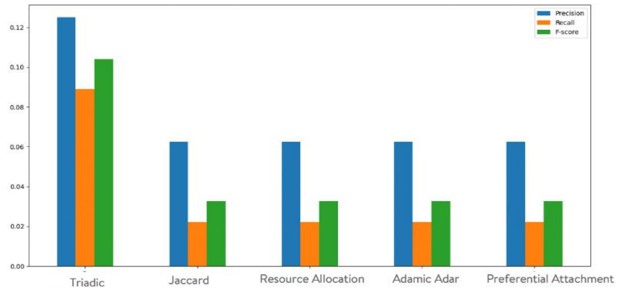


Fig. 2: Performance of adversary inference attacks on FBdataset After applying PPA.

E. *Attribute disclosure via Utility and masked attribute*

To assess how well different methods protect sensitive information, this research work use *utility scores* and the *percentage of hidden/masked attributes*. The utility score is calculated using equation 22.

$$u = \frac{\sum_{u\epsilon V_N^*} \sum_{i=1}^{|p_u|} p_i x_i}{\sum_{u\epsilon V_N^*} \sum_{i=1}^{|p_u|} p_i} \qquad (22)$$

Where *u* is the utility score we're calculating, V_N^* represents the set of social actors who are affected and have privacy concerns. p_u indicates the number of attributes for a specific social actor. p_i represents a specific attribute's score, like uniqueness or commonness. The equation 22 essentially sums up the scores for all the attributes and divides it by the total number of attributes for the actors we're concerned about.

The utility score helps us understand how much useful non-sensitive information is shared. To calculate this, we usea formula (equation 22) that considers the *uniqueness* and *commonness scores* of the shared attributes.

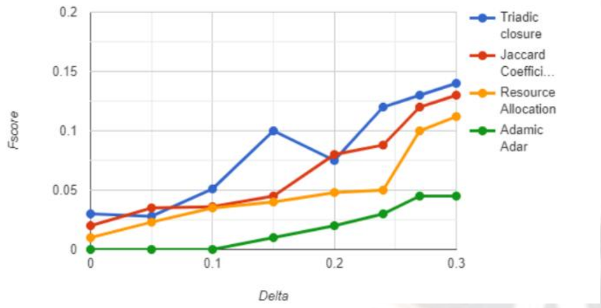
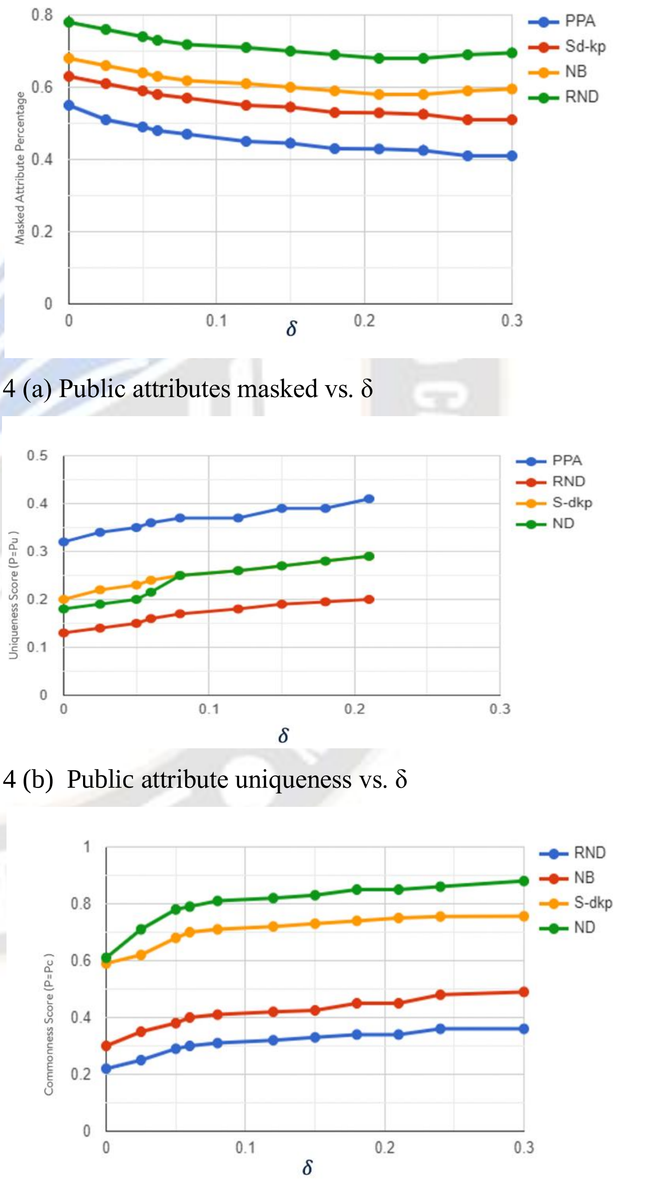


Fig. 3: Performance of local classifier (i.e F_1 Score under different values δ) after applying PPA.

In figure 3, the results of an experiment focused on deriving/inferring out the secret information related to a *'education attribute School'* in the Facebook dataset. In the original data, four different edge predictor algorithm were used to try and guess this secret information. They had varying success rates: Decision Tree had an 85.17% success rate, Random Forest had84.24%, Naive Bayes had 66.83%, and Logistic Regression had 69.05%. These numbers are much better than random guessing, which would only be around 15.62%. However,when we apply the *PPA* algorithm (a privacy protection method), the success rates of these four programs drop significantly. Even with a relaxed privacy setting (δ = 0.3), thesuccess rates are no higher than 15%. This means that withcritical information hidden, the published user data confuses the programs, leading to inaccurate predictions. In fact, withvery strict privacy constraints (δ = 0), nearly every personwith the secret related to *'education attribute School'* is wellprotected, with success rates as low as 1%. This demonstratesthat the *PPA* algorithm effectively defends against attemptsto figure out this secret using various types of computer programs. To put it simply, the *PPA* algorithm makes it very difficult for these programs to accurately guess the secretinformation, even when they have access to the published data.This means that actor's private information is well protected.



4 (a) Public attributes masked vs. δ

4 (b) Public attribute uniqueness vs. δ

4 (c) Public attribute commonness vs. δ

Fig. 4: Attribute disclosure via utility scores and the percentage of masked attributes

In fig 4, the utility score of different algorithms is at sharing valuable non-sensitive attributes while protecting privacy.

Figure 4a shows the results of research experiments on Face- book datasets regarding the protection of sensitive information.For all four algorithm we tested, as we make the privacyconstraints stringent (i.e., δ), the percentage of hidden at-tributes decreases. On Facebook dataset, the PPA algorithm consistently performed the best. At the less regid privacy constraint (i.e., δ = 0.3), it only needed to mask 40.74% of the published attributes. On the other hand, the other three algorithms (i.e., *mdKP-RDA*, *NB*, and *RND*) needed to hide 49.66%, 59.79%, and 71.27% respectively. Even under very strict privacy settings (i.e., δ = 0), the PPA algorithm only hid 55% of the public attributes. The mdKP-RDA algorithm also outperformed the Naive Bayes Masking method with fewer attributes being hidden. In general, combining these protection performance results, the PPA algorithm seems to provide effective protection by hiding as few critical attributes as possible. This means more information can be shared while still maintaining privacy.

The PPA algorithm stood out as the best performer among the four methods. It showed a significant improvement of around 40-50% over the Naive Bayes Masking method. This means it was particularly effective at minimizing the amount of revealing information in the shared profiles.

Figure 4c show performance of different algorithm in terms of commonness scores. The commonness indicate attributes that are shared by a lot of people. Both the *PPA* and mdKPRDA algorithms have significantly higher scores compared to the Naive Bayes Masking method. PPA and mdKP-RDA algorithms do a better job at handling attributes that many people have in common. The Naive Bayes Masking algorithm is only slightly better than Random Masking. This is because the Naive Bayes Masking method doesn't focus on maximizing the utility score as its main goal. In summary, when it comes to protecting attributes, the *PPA* algorithm is the most preferable option. It achieves a higher utility score, meaning it shares more useful information, while also hiding fewer attributes.

F. Experiment results of Social Relation Disclosure

Directed relations in a social network that have a specific direction. For example, on Twitter, if user A follows user B, it's a directed relation because it goes one way (A follows B). Undirected relationship doesn't have a specific direction. For example, on Facebook, if user A is friends with user B, it's an undirected relation because the connection goes both ways (A is friends with B and B is friends with A). Percentage of masked relations measures how many social connections are hidden or disguised to protect privacy. Jaccard coefficient is a measure of similarity between two individuals. Adamic/Adar Score is used in social network analysis to estimate the importance or similarity between nodes. It takes into account the shared connections between two nodes. Normalized Utility Score (*p*) is a measure of how well the protection method balances between privacy and utility. The utility score *u* is calculated using equation 23.

$$u = \frac{\sum_{i=1}^{|E_N^*|} p_i x_i}{\sum_{i=1}^{|E_N^*|} p_i} \qquad (23)$$

Where |E∗N| set of edges connected to social actors having privacy concern.

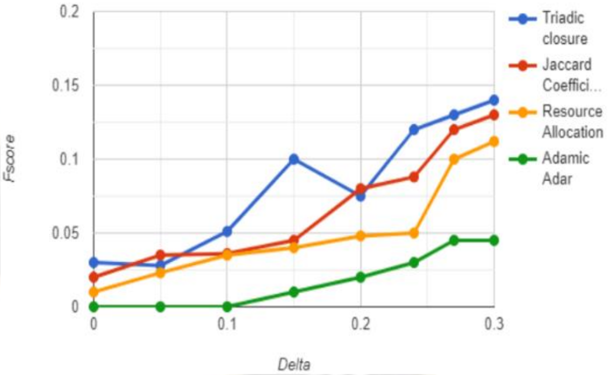
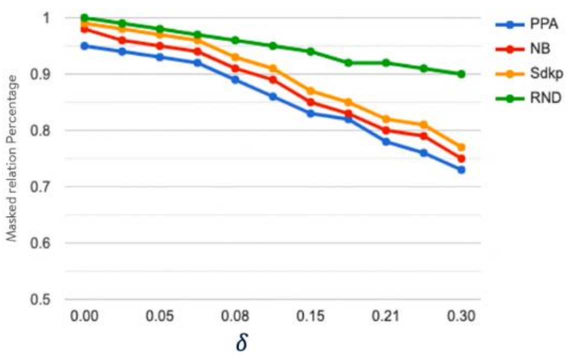


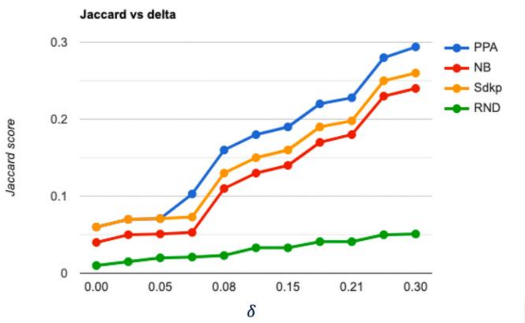
Fig. 5: F-score Vs local classifiers after applying mdKP-RDA

Figure 5 show performance of classifiers with change in δ. The classifier considered are: Weighted-Vote Relational Neighbour Classifier (WVRN), Class-Distribution Relational Neighbour Classifier (CDRN), Network-Only Bayes Relational Classifier (NOLB). The F-Score is a metric that combines precision (accuracy of positive predictions) and recall (sensitivity to find all positive cases). It's used to evaluate the performance of classification algorithms.

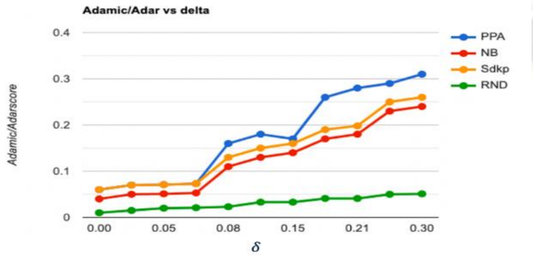
As δ increases, the performance of NOLB significantly decreases. It becomes less effective at making accurate predictions about user attributes. the performance of WVRN and CDRN does not drop dramatically even at a relatively relaxed privacy setting of δ = 0.3. In fact, they still perform better than NOLB on the original dataset. When δ is very strict (say ≤ 0.06), the F-Scores of WVRN and CDRN are smaller than 0.5. The results suggest that a loose privacy constraint for social relation disclosure can still potentially expose users' private information to the threat of inference attacks, especially when using relational classifiers. Given these results, it is recommended to set a small value for the privacy threshold (both δ and ϵ) to provide a stronger defense against inference attacks based on social relations.



6 (a) Social Relation masked vs. δ.



6 (b) Jaccard vs. δ



6 (c) Adamic Adar Score vs. δ

Fig. 6: Social Relation disclosure *via* utility scores: masked social relation Jaccard and Adamic Adar Score.

Figure 6a illustrate the percentage of masked social connections in the Facebook social online network dataset using different privacy protection algorithms. Compared to protecting attributes, safeguarding social relations (like friendships or followers) requires masking a much larger portion of the social relations. This is especially true for undirected social networks.

In the Facebook network dataset, if we want to ensure a higher level of privacy (i.e., δ = 0), Facebook social network need to remove almost 95% of the affected social relations. With the PPA algorithm, only about 18.54% of affected social relations can be retained. The mdKP-RDA method retains 13.67% and the Naive Bayes classifier retains 11.25%. The PPA algorithm can only keep around 30% of the social relations at privacy constraints δ = 3, but the effectiveness of the privacy protection doesn't decrease significantly. This means that to effectively protect privacy, it's crucial to mask a substantial number of social relations, which can limit the usefulness of privacy-preserving algorithms. Because of this, the performances of the three disclosure algorithms might appear similar. However, the PPA algorithm still performs slightly better than mdKP-RDA and Naive Bayes in this context.

The Jaccard coefficient and Adamic/Adar score are used to determine the importance of social relations based on how similar two connected social actors are. 6b shows results of structure similarity (i.e., common friends) using the Jaccard coefficient in both directed and undirected social networks. In the undirected Facebook network, the performances of the PPA and mdKP-RDA methods are very similar and slightly better than the Naive Bayes (NB) method when the privacy constraints is at δ ≤ 0.06. In the directed Google+ network, the PPA algorithm performs better in terms of utility scores compared to the other two algorithms.

6c shown results of *Adamic/Adar score*. It emphasizes the similarity between the profiles of the two social actors. The PPA algorithm consistently performs well because it's designed to preserve important social relations as much as it can. However, in experiments focusing on undirected social connections, the mdKP-RDA algorithm, which simplifies the original problem and reduces computational complexity, performs very similarly to the PPA algorithm under strict privacy constraints. mdKP-RDA algorithm balance privacy and data utility.

Based on the experiment results, it's clear that the PPA algorithm is highly effective in protecting against various types of inference attacks using both public attributes and social connections/relations. When compared to the best existing methods and under the same security standards, the PPA algorithm consistently achieves a higher utility score for both revealing attributes and disclosing social relations.

VIII. Conclusion

This research work delved into the sharing of data in online social networks, focusing on safeguarding against inference attacks. It laid out an optimization problem aiming to balance utility, privacy guarantees, and user concerns. The paper introduced two algorithms to tackle tradeoff between data utility, privacy guarantees.

The first method, called *PPA* find a workable and beneficial solution to the original problem. The second, *mdKP-RDA* algorithm, simplifies the disclosure problem involving undirected social relations into a more manageable form known as *mdKP-RDA.*

Extensive experiments on Facebook and Google+ datasets confirmed the efficiency and effectiveness of our proposed algorithms in thwarting inference attacks. Notably, the PPA algorithm outperforms existing masking techniques significantly. On the other hand, the *mdKP-RDA* approximation algorithm boasts lower computational complexity and is especially useful for addressing undirected social relation disclosure problems.

Acknowledgmt

The authors would like to thank K Thanujashree, Lakshmi Priya B, Nimitha J for their contribution towards implementing algorithm on Facebook and Google+ dataset.

References

[1] C. Cohn and C. Cohn, "Social Media Ethics and Etiquette," https://www.compukol.com/social-media-ethics-and-etiquette/, Apr 13 2011.

[2] J. Heidemann, M. Klier, and F. Probst, "Online social networks: A surveyof a global phenomenon," *Computer Networks*, vol. 56, no. 18, pp. 3866–3878, 12 2012.

[3] B. Bosker, "Serial Sex Offender Admits Using Facebook To Rape And Murder Teen," https://www.huffpost.com/entry/peter-chapman-admits-usin n 489674, dec 7 2017.

[4] W. Li and H. Li, "Lrdm: Local record-driving mechanism for big data privacy preservation in social networks," in *2016 IEEE First International Conference on Data Science in Cyberspace (DSC)*. IEEE,2016, pp. 556–560.

[5] N. Li, N. Zhang, and S. K. Das, "Relationship privacy preservation in publishing online social networks," in 2011 IEEE Third International Conference on Privacy, Security, Risk and Trust and 2011 IEEE Third International Conference on Social Computing. IEEE, 2011, pp. 443– 450.

[6] Y. Alufaisan and A. Campan, “Preservation of centrality measures in anonymized social networks,” in *2013 International Conference on Social Computing*. IEEE, 2013, pp. 486–493.

[7] J. Zhang, X. Wang, Y. Yuan, and L. Ni, “Rcdt: Privacy preservation based on r-constrained dummy trajectory in mobile social networks,” *IEEE Access*, vol. 7, pp. 90 476–90 486, 2019.

[8] M. S. Shishodia, S. Jain, and B. Tripathy, “Gasna: Greedy algorithm for social network anonymization,” in *Proceedings of the 2013 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining*, 2013, pp. 1161–1166.

[9] L. Schwittmann, M. Wander, C. Boelmann, and T. Weis, “Privacy preservation in decentralized online social networks,” *IEEE Internet Computing*, vol. 18, no. 2, pp. 16–23, 2013.

[10] D. Yin, Y. Shen, and C. Liu, “Attribute couplet attacks and privacy preservation in social networks,” *IEEE Access*, vol. 5, pp. 25 295–25 305, 2017.

[11] K. M. Chong and A. Malip, “Trace me if you can: An unlinkability approach for privacy-preserving in social networks,” *IEEE Access*, vol. 9, pp. 143 950–143 968, 2021.

[12] K. Zhang, Z. Tian, Z. Cai, and D. Seo, “Link-privacy preserving graph embedding data publication with adversarial learning,” *Tsinghua Science and Technology*, vol. 27, no. 2, pp. 244–256, 2021.

[13] H. Zhu, X. Zuo, and M. Xie, “Dp-ft: A differential privacy graph generation with field theory for social network data release,” *IEEEAccess*, vol. 7, pp. 164 304–164 319, 2019.

[14] H. Huang, D. Zhang, F. Xiao, K. Wang, J. Gu, and R. Wang, “Privacy-preserving approach pbcn in social network with differential privacy,” *IEEE Transactions on Network and Service Management*, vol. 17, no. 2, pp. 931–945, 2020.

[15] B. Yang, J. Li, L. Liu, Y. Cao, H. Wei, P. Sun, N. Wu, and B. Li, “Shut-terroller: Preserving social network privacy towards high-speed domain gateway,” in *2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing*. IEEE, 2015, pp. 1811–1818.

[16] Q. Liu, G. Wang, F. Li, S. Yang, and J. Wu, “Preserving privacy with probabilistic indistinguishability in weighted social networks,” *IEEE Transactions on Parallel and Distributed Systems*, vol. 28, no. 5, pp. 1417–1429, 2016.

[17] Y. Qu, S. Yu, W. Zhou, S. Chen, and J. Wu, “Customizable reliable privacy-preserving data sharing in cyber-physical social networks,” *IEEE Transactions on Network Science and Engineering*, vol. 8, no. 1, pp. 269–281, 2020.

[18] Q. Wang, Y. Zhang, X. Lu, Z. Wang, Z. Qin, and K. Ren, “Real-time and spatio-temporal crowd-sourced social network data publishing with differential privacy,” *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 4, pp. 591–606, 2016.