INTRODUCTION

Due to the extended use of online social networks on the web, wide range of humans subscribe to social networks or social media. This has generated large quantity of personal statistics that is gathered and maintained with the aid of the social community service providers. The data generated by using social community services is termed as the social network data and that is desired to be posted for other users in positive situations. One of the major situations is when precise analysis of the person data desires to be achieved and another scenario is when the provider of the statistics has to share the information with events like marketing companions which is section of insurance policies normally customary by way of subscribers. The statistics includes precious records about customers that help third party events in bettersocialized on their advertisements. Social network analysis is being used in modern-daysociology, geography, economics, and information sciences. Researchers in more than a fewfields use this information for special purposes like, government establishments require social community facts for data and security purposes. So, information desires to be shared or published in all above stated situations. Owner of data can post it for others to analyze but it may additionally create serious privacy threats. To fulfill the demands for thenetwork data, online social media operators have been sharing the data they collect and maintain with external third events such as advertisers, software developers, and tutorial researchers like Facebook has lots of third-party applications and there has been two exponential enlarge in this number[1]. Social community facts incorporate touchy and exclusive data about the users. Thus sharing of this information in its uncooked form mayadditionally breach privacy of individuals. Individual privacy is defined as the right of the person to determine what records about himself has to be communicated to others and under what circumstances. A privacy breach takes place when non-public and personal information about a person is disclosed to an adversary. So, keeping privacy of people whilst publishing his/her accrued information is an important research area. The privacy breaches in social networks can be categorized into three types:

1. **Identity disclosure** - Identity disclosure happens when a character behind a report is exposed. This type of breach leads to the revelation of records of a consumer and relationship he/she shares with other persons in the network.
2. **Sensitive link disclosure** - Sensitive hyperlink disclosure happens when the associations between two persons are revealed. Social activities generate this kind of information when social media offerings are utilized by way of customers.
3. **Sensitive attribute disclosure** - Sensitive attribute disclosure takes location when an attacker obtains the records of a sensitive and confidential consumer.

*Corresponding author: Reshmi T S*

Department of Information and Technology Bannari Amman Institute of Technology, Tamil Nadu

**ARTICLE INFO**

**Article History:**
Received 13th July, 2019
Received in revised form 11th August, 2019
Accepted 8th September, 2019
Published online 28th October, 2019

**Key Words:**
The user shares their current status and updates their information about personal lives.

**ABSTRACT**

Nowadays the world is connected to the Internet and the social networks have important role in our everyday life, so security and privacy is must. The online social networks have clear picture that shows the users social relationships. The user shares their current status and updates their information about personal lives. The privacy risks for such activities are more, such as disclosure of their personal information to public than planned. Also, they post information about others without their permission. The lack of experience and unconscious about social networks services continue the situation. So, propose an automated system that would protect the user’s identity and also helps to share the posts and images without losing users privacy to the public. And the proposed method allows send messages and photos privately as messages to their friends while posting their timeline, which provide more privacy than the existing approaches.

**Copyright © Reshmi T S and Priya J, 2019**, this is an open-access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution and reproduction in any medium, provided the original work is properly cited.
attribute. Sensitive attributes may also be linked with an entity and hyperlink relationship.

All these stated privacy breaches pose extreme threats like stalking, blackmailing and theft because users expect privacy of their data from the service provider. Besides that it damages the picture and popularity of an individual. There are many cases of unintentional disclosure of private data of users that makes companies to be conservative in releasing the network data. Ensuring privacy for social network facts is tough than the tabular micro-data because:

1. Modeling of background understanding of adversaries is tough in social community statistics than tabular micro-data. In tabular micro-data, users are recognized by way of linking quasi-identifiers, whereas in social network data from a range of sources such as labels of vertices and edges, sub graphs and neighborhood graphs should be used to identify individuals.

2. Information loss is the metric which measures the amount of distortion. In tabular micro-data records loss can be measured using the sum of records loss in character records. Since, a social community is a graphical shape with a set of vertices and edges hence it is hard to examine two social networks by evaluating the vertices and edges individually. Anonymous social network and original social network which have the identical quantity of vertices and edges might also have very one-of-a-kind residences like betweenness, connectivity, and diameter. Information loss and anonymity can be measured in one-of-a-kind ways.

3. Development of privacy preserving strategies in social community is hard than for relational data. Tabular micro-data has anonymized the use of divide-and-conquer strategies whereas social community is a structure of nodes and edges, any modifications in labels or edges may additionally have an impact on the neighborhoods of different vertices and edges.

The techniques proposed for tabular micro-data can’t be at once utilized to social community facts due to the connectivity between vertices in the layout community as compared to impartial nodes in tabular data. In micro-data, every tuple is independent; however the vertices and edges in a social community are linked to each other. An adversary can use the facts concerning network structure to violate the privacy of users. So there is a need is to strengthen the approach that can make privacy of the entities in social community while publishing data.

This paper focuses on protection of individual privacy preferences while publishing their data. Still there are different methods for data publication and user’s privacy but are effective only for some groups of people. Thus a new method where majority users are able to protect their identity from public is proposed in this paper.

The remainder of this paper is structured as follows: The related works is discussed in section II followed by methodology used in section III. Section IV is the implementation followed by the conclusion in section V.

**Related Works**

Multiparty Access Control for Online Social Networks[2], implemented a proof-of-concept Facebook application for the collaborative management of shared data, called MController. Their prototype application enables multiple associated users to specify their authorization policies and privacy preferences to co-control a shared data item. A multiparty access control model was formulated, along with a multiparty policy specification scheme and corresponding policy evaluation mechanism. In addition to the owner of data, other controllers, including the contributor, stakeholder and disseminator of data, need to regulate the access of the shared data have been identified as well. In MPAC system, a group of users could collude with one another so as to manipulate the final access control decision. It is worth noting that their current implementation was restricted to handle photo sharing in OSNs. Their approach can be generalized to deal with other kinds of data sharing and comments, in OSNs as long as the stakeholder of shared data are identified with effective methods like tagging or searching.

Collective Privacy Management in Social Network[3] model the problem of collaborative enforcement of privacy policies on shared data by using game theory is proposed. In particular, they propose a solution that offers automated ways to share images based on an extended notion of content ownership. Building upon the Clarke-Tax mechanism, they describe a mechanism that promotes truthfulness, and that rewards users who promote co-ownership. The design is integrated with inference techniques that free the users from the burden of manually selecting privacy preferences for each picture. In the paper, they also show a proof-of-concept application, which they implemented in the context of Facebook.

**Un Friendly:** Multi-Party Privacy Risks in Social Networks[4] examine how the lack of joint privacy controls over content can inadvertently reveal sensitive information about a user including preferences, relationships, conversations, and photos. They analyze Facebook to identify scenarios where conflicting privacy settings between friends will reveal information that at least one user intended remain private. Facebook uses friendship to distinguish between trusted and untrusted parties. Users can allow friends, friends of friends, or everyone to access their profile data, depending on their personal requirements for privacy[6]. Social networks are inherently designed for users to share content and make connections. When two users disagree on whom content should be exposed to, they say a privacy conflict occurs. Multiple privacy conflicts can occur between a user and his friends, each revealing a potentially unique sensitive detail. They specifically analyzed two scenarios in Facebook -friendship and wall posts to understand the types of information exposed by conflicts[5]. They then examined the accuracy of each classifier and whether the intuition behind each technique proved correct. Their results show classification using information gleaned from privacy conflicts consistently outperforms predictions that lack the auxiliary information, proving that conflicts can be analyzed to expose meaningful sensitive information. Further, they find that accuracy is directly related to the number of conflicts between a user and his friends. Having explored the extent that privacy conflicts appear throughout social networks and their potential risk, they now present a solution for
enforcing multi-party privacy. The framework enforces the mutual privacy requirements of all users referenced by a piece of data to prevent privacy violations, mitigating any risk of aggregating leaked information. They prototyped their solution as a Facebook application, that transparently enforces multi-party privacy without requiring interaction from users.

Privacy Preserving Data Mining for Social Networks[7] focuses on determining whether the public data present in the social networks are vulnerable to correct inference of sensitive private information and thereby suggested a sanitization technique to the use to avoid the same[8].

Face/Off: Preventing Privacy Leakage from Photos in Social Networks[5] proposed, to rethink access control when applied to photos, in a way that allowed individuals to effectively prevent unwanted individuals from recognizing users in a photo. The core concept behind this approach was to change the granularity of access control from the level of the photo to that of a user's Personally Identifiable Information (PII). In this work, they focused on the face as the PII. When another user attempts to access a photo, the system determines which faces the user has not provided permission to view, and the photos of the restricted faces are blurred out. This study revealed the misconceptions about the privacy offered by existing mechanisms, and demonstrated that users are positive towards the adoption of an intuitive, straightforward access control mechanism that allowed them to manage the visibility of their face in published photos.

**METHODOLOGY**

The proposed system deals with computational mechanism for social media, given the individual privacy preferences of each user involved in a data. Here users willing to make decisions in different situations are considered. Once a user registered he/she can change initial privacy settings [9]. After that privacy settings are done automatically according to the user preferences. Admin can view all users, user details; files shared, and also can block users.

**Start**

User registers to Online Social Network by entering the details like name, gender, email, mobile number, username, password etc. Once registered successfully the user can login his/her account. User or admin can login if they have valid username and password. Admin can login with a valid password, once login admin can view the user details. Also admin can block the users.

**Specify policy**

Each user has a privacy policy and a exposure policy for a specific photo. Two options are set, one “view public” and “view my friends”. Exposure policy indicates the set of users who can access when user “u” is involved. Identity disclosure happens when an adversary is in a position to decide the mapping from a profile “v” in the social network to a unique real-world entity “p”. Considering questions related to the identity of “p” in which an adversary may be interested.

- **Mapping query**- In a set of individual profiles V in a social network G, find which profile v maps to a particular individual p. Return v.
- **Existence query**- For a particular individual p, find if this individual has a profile v in the network G. Return true or false.
- **An easy way of defining identification disclosure is to say that the adversary can reply the mapping question correctly and with full certainty. However, unless the adversary knows special attributes of individual p that can be matched with the determined attributes of profiles in v, this is challenging to achieve.** One way of formalizing identity disclosure for an individual p is to partner a random variable p which degrees over the profiles in the network.
- **Identity disclosure with confidence t**- In a set of individual profiles V in a social network G, identity disclosure occurs with confidence.
- **Social hyperlink disclosure occurs when an adversary is in a position to find out about the existence of a touchy relationship between two users,** a relationship that these users would like to stay hidden from the public.

Another kind of privacy breach in relational data is affiliation hyperlink disclosure, whether or not a character belongs to a specific affiliation group. Whether two users are affiliated with the same team can additionally be of sensitive nature. Sometimes, affiliation link disclosure can lead to attribute disclosure, social hyperlink disclosure, or identity disclosure. Thus, hiding affiliations is a key to keeping the privacy of individuals. The k-anonymity technique ensures that humans cannot be uniquely identified by means of a linking attack. However, it does now not necessarily forestall sensitive attribute disclosure. Here, we present two viable assaults on k-anonym data. The first one can manifest when there is little variety in the sensitive attributes interior an equivalence class. In this case, the touchy attribute of anybody in the equivalence class turns into known with high certainty.

**Search friends**

User can search through this social networking site to get friends, there is an search friend option to find friends, user needs to make friends among their Social Network friends either by sending friend request or accepting others friend request. For interactive application the fast response of the system will needed.

**Post photo and videos**

The user can post messages and photos in timeline of the users, which is visible to friends, friends of friends or public then they planned. So there is an option public message for send messages and photos to each of friends in friend list of the user. The posts on timeline maybe shared or views than planned. Thus the public message option will help user to share their post messages, photos and videos privately every friends without showing on timeline. As we see nowadays users are interest to share items on OSNs. But sometimes it will be forwarded to public even the privacy settings are done. So the proposed will provide method to share items with more privacy. The user needs to share the items but not disclose to the public. Thus, provides an option for sharing to friends public msg(). It will share images, videos to the friends with more security. And will not show public by sharing or commenting of the photos or videos.
Pattern matching and mining: Perform a systematic investigation on pattern matching, pattern mining with wildcards, and application problems as follows: Exploration of the NP-hard complexity of the matching and mining problems, Multiple patterns matching with wildcards, Approximate pattern matching and mining, and Application of our research onto ubiquitous personalized information processing and bioinformatics.

Message

The user can send messages using the option msg(). The messaging option can be used by user to send messages, photos, and videos to friends. By msg() user can maintain the communication with friends. There are two options provided, private() and public(). The private option is used for sending messages privately to individual friends. The public option is used for sending the messages, photos and videos for all friends in the friend list of the user[10]. The user may not be able to maintain the communication with all friends always. For private messaging the user needs to selecting friends from the friend list to whomwith need to chat. But by using the public() option the user can share the feelings, photos and videos to all friends without selecting or making groups. In existing systems, the user needs to select or broadcast messaging to friends makes consuming time and more manual intervention.

Conflict message

Others (not friends) trying to access the user account data the system will provide only chat option and request option. When sending a message it will be viewed as the conflict message. In conflict message, displays the messages of those who are not friends of the user. The conflict message shows that relation of the user with another person is that not friend. Each time checks the user bio data for identifying the relation. If a person not friend of the user, then only option for chat and will added conflict chat()

Identify friends in friend list

When the user try send messages publicly the system checks who are friends of the user. After finding the friends of the user the privacy sets to zero because all friends of the user can get the message. If the user privately sends message it will set as one. For sharing the messages, photos, and videos the user needs to check the friend list. It will be updated automatically before sharing[11].

Implementation

User Registration page

To exploit the features of this Online Social Networks every users need to create an account.

User can create a user name and password. For registration the user needs to fill the personal information. User should enter gender, email id, mobile number, user name, password etc. at the time of registration. After registration the user can login to their account.

Login page

If registration done successfully user can login to his/her account to explore the features of online social networking. User can login with user name and password.

Search friends page

Once user login with an valid username and password, user is able to send friend request and accept friend request. To send a friend request user can use send request option in the given system, the name and profile picture with chat option will be displayed and now logged user can send request and messages.

Conflict chat page

When a person, who is not already friend of the user sends a message it will display on the conflict chat page. When user searches for a friend the only option available will be for chatting. There is no option for seeing the profile and personal details of the user he will be friend with that person.

Friend List page

Once user is login with a valid user name and password, user is able to view his/her friendlist using the option view friend list in this system. The friends list pages shows list of friends of user. He/she can view the friends profile using “Details” button. Then the friends profile and timeline for the user is shown.

Messaging page

After making friends, user can send messages. There are two options. “Public message” and “private message”. In public message option the user can send message, photo and videos to all friends of the user friend list while posting on timeline of the user. Thus, it ensures more privacy because no one can see that posts on the timeline, can view only as private messages. The private message option is same as the ordinary messaging. Send messages for individual friends.

Video sharing page

When user login, by sending request friends are made by the user. After accepting request of the user can send messages and videos with friends. The videos can send privately to friends also can share with every friends of the user. The video sharing will done using the share video option. The public share option will used share video with every friends of the user. Also, user can send messages to friends privately.

CONCLUSION

In this approach implement a secured way to posting and sharing messages with friends. The multiparty privacy preserving is important in social networks. In proposed method, can share message, photos and videos securely with friends without disclosing to the public which is different from existing approaches. Also, implement the method to hide personal information of users for others, this method used as a friend book, which can share the messages and videos to every one of friends in list without selecting. The proposed method helps user to reduce manual intervention and provides privacy and security.

References


How to cite this article:

*******