Detection of Collusion and Malicious Activities in OSN Using MPAC

J.Rini Esther Shirly¹, K.Kalpana²

¹ II yr M.E Student, ² Assistant Professor
1, 2 CSE Department, Gnanamani College of Technology, Namakkal, Tamilnadu, India
Anna University

ABSTRACT: Online Social Network’s (OSN especially Facebook) has experienced a growth in recent years. A social networking service is an online service, platform, or site that focuses on facilitating the building of social networks or social relations among people who, for example, share interests, activities, backgrounds, or real-life connections. A social network service consists of a representation of each user (often a profile), his/her social links, and a variety of additional services. Most social network services are web-based and provide means for users to interact over the Internet, such as e-mail and instant messaging. Online community services are sometimes considered as a social network service, though in a broader sense, social network service usually means an individual-centered service whereas online community services are group-centered. Social networking sites allow users to share ideas, activities, photos, videos, statuses, events, and interest within their individual networks.

Keywords- Collaboration management, malicious activities, multiparty access control, social network.

I. INTRODUCTION

Online Social networking is the grouping of individuals into specific groups, like small rural communities or a neighborhood subdivision, if you will. Although social networking is possible in person, especially in the workplace, universities, and high schools, it is most popular online. This is because unlike most high schools, colleges, or workplaces, the internet is filled with millions of individuals who are looking to meet other people, to gather and share first-hand information and experiences about cooking, golfing, gardening, developing friendships professional alliances, finding employment, business-to-business Marketing and even groups sharing information about baking cookies to the Thrive Movement. The topics and interests are as varied and rich as the story of our universe. When it comes to online social networking, websites are commonly used. These websites are known as social sites. Social networking websites function like an online community of internet users. Depending on the website in question, many of these online community members share common interests in hobbies, religion, politics and alternative lifestyles. Once you are granted access to a social networking website you can begin to socialize. This socialization may include reading the profile pages of other members and possibly even contacting them. The friends that you can make are just one of the many benefits to social networking online. Another one of those benefits includes diversity because the internet gives individuals from all around the world access to social networking sites. This means that although you are in the United States, you could develop an online friendship with someone in Denmark or India. Not only will you make new friends, but you just might learn a thing or two about new cultures or new languages and learning is always a good thing.

As mentioned, social networking often involves grouping specific individuals or organizations together. While there are a number of social networking websites that focus on particular interests, there are others that do not. The websites without a main focus are often referred to as “traditional” social networking websites and usually have open memberships. This means that anyone can become a member, no matter what their hobbies, beliefs, or views are. However, once you are inside this online community, you can begin to create your own network of friends and eliminate members that do not share common interests or goals.

One of the major disadvantages of using social networking websites are the students get addicted to it. They used to spend hours in those social networking sites which can obviously degrade the student’s academic performance. Some students may tend to use to these social networking sites till mid night or even more which can obviously lead to health related problems. Some students may spend time in Facebook through which they lack to spend time with their family members. This can also be a disadvantage also. Some students may provide detailed information like phone numbers, address which is very dangerous because they can...
easily tracked down by strangers. Access control has become a central feature in OSN [1].

1.1 Limitations of OSN

Although OSN provides simple access control mechanisms in their own spaces, but no control over others spaces in which he/she is tagged or posted a status. Every user has their own privacy control in their space. Since original control policies cannot be changed, users still addicted to OSN and suffer from privacy issues in others space. On the other hand, removing a photo can only prevent others from seeing the photo but, it can be seen via association link. Although reporting to OSN will take binary decision based upon the complaints they receive from each person. Hence we must develop a secured model from which user can get rid of unauthorized users from seeing the photo. Malicious activities within the photo can also be tracked using anomaly detection technique.

1.2 Need for MPAC

This MPAC mechanism will resolve the issues discussed in earlier section. This section describes how to secure the photo or video which you uploaded to unseen from unauthorized Users. Disadvantage of simple access control is, the person who is tagged can be seen via association link, in this technique, users can opt from seeing the photo. The person can see the photo only after getting permission from the owner, and malicious activities can also be prevented. This technique addresses issues that have not been solved by previous method. [2], [3], [4].

II. OSN REQUIREMENTS

2.1 Profile Creation

Facebook is better known for finding old friends, playing games and connecting with people you know. There’s another angle to Facebook though. Facebook can also be used to promote you. Whether you have a small business that you want to promote, are a band of some sort, are an artist, are a public figure, or an organization, you can use Facebook to promote yourself. The cost to create a Facebook profile for your hobby or organization is free. Facebook also offers the option to create an ad, for a small fee, that will be displayed on Facebook. This will help promote you even more. This profile is different than creating a Facebook group. A Facebook group does not have a news feed on the page that you can add messages and comments to. It does however allow you to send a message to everyone in your group at once. You have to decide which is better for you. Creating your professional Facebook profile is easy, just log into Facebook and go to Facebook’s create a page tool. Then decide which category your hobby or organization fits into and follow the directions to create your Facebook profile.

Once you have the Facebook profile for your hobby or organization all set up, you’ll need to spend a little time adding content to it. Don’t worry, this is easy. Add something to the Info tab of your Facebook profile. This will tell people what your hobby or organization is about and what you can do for them. Make sure you send the link to all your friends, fans and clients so they can all come to your Facebook profile and sign up. Then whenever you add a message to your Facebook profile page, they will all see your message from their Facebook page.
2.2 Profile Sharing

A primary characteristic of OSN is to help social requisitions composed by third-party developers to create additional functionalities built on the top of users profile for OSNs [5]. Profile sharing will get the users attributes such as name, birthday, and interests and so on. OSN platforms will also consume users friends profile attributes [6]. So users must select particular pieces of attributes that they are willing to share with the third party applications. View your Facebook profile as the public and your friends see it, and then use Facebook's global settings to restrict access to and use of your posts, photos, and other information.

2.3 Relationship Sharing

Users can share their relationships with other members in Facebook. Relationships are bidirectional and have sensitive information. Users can regulate the display of their friends list. They can only control one direction of their relationships [7].

2.4 Content Sharing

OSN provide a built-in mechanism that enables users to communicate and share the contents with the other members. The shared contents can be connected with multiple members. Depending on whom you’d like to share with, there are different ways to share content on Facebook: Sharing with a broad audience, sharing with a small group of friends - the Groups feature to share content with a select group of people, like family members, your soccer team or your book club, and sharing with an individual. Tips for content sharing: Post content directly to Facebook. If you don’t have time to do this, try popular third-party apps to automatically post content (i.e. Networked Blogs).

1. Be creative in sharing content to catch people’s attention. Use clever headlines and attention-grabbers.

2. Never apologize for sharing content. If you have to apologize for it, you shouldn’t be sharing it.

III. IMPLEMENTATION

3.1 Collaborative Authorization Management

To enable a collaborative authorization management of data sharing in OSNs, it is essential for MPAC policies to be in place to regulate access over shared data, representing authorization requirements from multiple associated users [8]. Our policy specification scheme is built upon the proposed MPAC model.

**Accessor specification:** Accessors are a set of users who are granted to access the shared data. Accessors can be represented with a set of user names, a set of relationship names (RNs) or a set of group names (GNs) in OSNs [9].
3.2 Description:

Online Social Networks have been used for sharing our personal information with friends, colleagues, even with stranger’s. Although they having simple access control mechanism, still now we don’t have full security to our data shared with others. Users can have control to information contained in their own spaces, users; unfortunately, has no control over data residing outside their spaces. For instance, if a user posts a comment in a friend’s space, she/he cannot specify which users can view the comment. In another case, when a user uploads a photo and tags friends who appearing the photo, the tagged friends cannot restrict who can see this photo, even though the tagged friends may have different privacy concerns about the photo. To address such a critical issue, preliminary protection mechanisms have been offered by existing OSNs.

For example, Facebook allows tagged users to remove the tags linked to their profiles or report violations asking Facebook managers to remove the contents that they do not want to share with the public. However, these simple protection mechanisms suffer from several limitations. On one hand, removing a tag from a photo can only prevent other members from seeing a user’s profile by means of the association link, but the user’s image is still contained in the photo, since original access control policies cannot be changed, the user’s image continues to be revealed to all authorized users. On the other hand, reporting to OSNs only allows us to either keep or delete the content. Then the photo or video can be viewed by everyone depends upon the owner’s permissions who tagged them. So it can be viewed, or downloaded from strangers also. We don’t get information about who downloaded or viewed or done malicious activities with it. In the Collaborative authorization management technique, it can be protected by setting the permission with the owner. Even the friends who don’t have permission to view or download must give request to the owner, to get the photo. So strangers from seeing /downloading the photo can be controlled with this technique. This technique can be used to prevent fraudulent activities in the online social networks. Even though it lags from usability, it provides security to users, who want to control it.

3.3 Anomaly Detection in OSN

Anomaly detection places an important task in OSN (Online Social Network). Even though we have simple access control mechanism in our OSN we don’t have full security for the data in our or others space. Although having security in the previous section (4.2). It’s easy for strangers to overcome from that. As they know cryptographic algorithms, they can be able to access it without the permission from the owner. This hacking must be avoided to prevent fraudulent activities in the OSN. These activities can be prevented even controlled by monitoring those activities, means of frequency of use from them [10].

A security analyst is interested in determining if the frequency with which a user executed a particular sequence of commands is higher (or lower) than an expected frequency. The sequence login, password, login, password corresponds to a failed login attempt followed by a successful login attempt. Occurrence of this sequence in a user’s daily profile is normal if it occurs occasionally, but is anomalous if it occurs very frequently, since it could correspond to an unauthorized user surreptitiously attempting an entry into the user’s computer by trying multiple passwords. To detect such intrusions, the analyst can use the third formulation, in which the sequence of commands is the query pattern, and the frequency of the query pattern in the user sequence for the given day is compared against the expected frequency of the query pattern in the daily sequences for the user in the past, to detect anomalous behavior. Photo owner can control any controller who is suspected to be malicious.

3.4 Architecture Diagram

IV. CONCLUSION

In this paper, we researched analysis services for collaborative management of shared data in OSNs. Likewise, we might investigate more criteria to assess the characteristics of our proposed MPAC model. We efficiently incorporated the thought of trust and notoriety into our MPAC display and research an extensive answer for adapt to arrangement ambushes for furnishing a strong MPAC benefit in OSNs. Besides, we systematically integrate the notion of trust and reputation into our MPAC model and investigate a comprehensive solution to cope with collusion attacks for providing a robust MPAC service in OSNs. Based on the
collaboration activities; we also prevented malicious activities in our work.

REFERENCES


