Preserving Individual Seclusion In Social Media

[1] Sneha Chinivar, [2] Mr.Ramu.S
[1] Siddaganga Institute of Tchnology , [2] Siddaganga Institute of Tchnology

Abstract— **Social media is a platform where re sharing of post is allowed. This may lead to privacy conflict between the involved users as the post is shared without considering the actual owner's preference. In order to address this issue, here an algorithm is used to automatically detect and resolve the conflicts that occur between the negotiating users. Also tagging permissions are used here so that no user can be able to tag any other user without that user's permission both in textual content and photo. Face recognition system has been used here to recognize the face uploaded by user and to get permission of the user of whom the photo is uploaded. Only if that particular person gave permission then the post will be posted, otherwise it won't get posted. Here timing constraint is one more feature that is added so that up loader can set by how much time response should be received and what action to be taken if response is not received in that time constraint. Through this work an attempt has been done to preserve the privacy of individual users of social media.**

Index Terms—**Security, Tagging, Face recognition system**

I. INTRODUCTION

Social media has become an important part in most of our daily life. It has helped us to get connected with all the people in our life no matter how far they are physically. It has also become a great marketing place. It has also become a great platform to share ones view point on a particular issue and discuss on that. As everything as its own good and bad side even social media has its own vulnerabilities. Few people are misusing these vulnerabilities in order to harm others. Privacy issue is one of the important things that social media failed to address. In the current scenario any user can tag and upload any users post without their permission. And also if there are multiple users involved in a particular post, only the up loader is given a chance to set its privacy settings. All other involved users privacy preferences are ignored. This is leading to many severe cybercrimes. So it is very much important to preserve the privacy and to provide security to all the individual users of social media.

II. LITERATURE SURVEY

Very few researchers have done work related to solving multiparty privacy conflict in social media. In one of those work [1] proposed a method to define privacy policies collaboratively. In this approach all involved parties can define strong and weak privacy preferences. In this approach no automated method is used to solve conflicts. So this approach served only as a suggestion for the user who try to solve to solve the conflict manually.

In [2], they try to address multi party privacy conflict using incentive mechanism. Here users are rewarded with a quantity of numeraire every time when they share information or acknowledge the presence of other users who co-owns the same item. During the time of conflict of co-

owners policies users can spend their numeraire in the bidding process and can make their decision to be followed. In [3], users should manually define certain parameters and based on those parameters privacy risk and sharing loss on segments are calculated. Based on these measures all of the conflicting target users in each segment are assigned the same action. This means conflicts are solved by granting or denying access to all negotiating users. This method doesn't even consider that each individual conflict can have a different solution. That may leads to outcomes that are far from what the users would be willing to accept.

In [4], a third party used to collect the decision of either granting or denying access to be taken for a particular friend from each party. Here authors have proposed to aggregate final decision based on any one of the 3 voting rules. The 3 voting rules are up loader overwrites (UO), majority voting (MV), and veto voting (VV). These approaches are proved to be static i.e. this method aggregated individual votes in the same way by following the same voting rule. Hence this approach failed to adapt to different situations. This approach failed to match the actual behavior of users many times.

In [5], authors considered using different voting rules based on the situation. Here the user who uploads/posts the item chooses manually which one of the voting rules to apply for item to be posted. Here along with up loader choosing the voting rule manually, the choice of voting rule to be applied manually becomes unilateral as only the up loader is given chance to select the voting rule not considering the voting choice of all the negotiating users. It might also be difficult for the up loader to decide by choosing which voting rule he can be able to satisfy most of the user's preference.

In [6], authors tried to analyze the problem from game theoretic point of view. But this proposal failed to work well always as they can't be able to capture social idiosyncrasies considered by users in the real life when they face multi-

party privacy conflicts. The result obtained from this method is very far from what actually users do in real life when they face conflicts.

III. PROPOSED SYSTEM

There are three important modules this system. They are
* Automated conflict detection and resolution algorithm
* Tagging with textual content
* Uploading image post.

Automated Conflict Detection and Resolution Algorithm: This algorithm automatically recognizes the negotiating users. After knowing the negotiating users it looks for the priorities and friend type of all friends of negotiating users. For only those friends whose friend type is same as that of the friend type between the negotiating users and their priority given by the negotiating user is greater than the threshold 2, negotiating users are able to share the post.In this project this algorithm is used only during sharing of post. This algorithm can be used as a mediator in any of the social media like Facebook, Twitter ,Google+ etc. This algorithm can be integrated as a back-end of social media privacy control interface or it could be implemented as a social media application such as Facebook app that works as an interface to the privacy controls of social media infrastructure.Example: Assume a set of users U = {Alice; Bob;Charlie; Dan; Eve; Frank}. Negotiating users N ={Alice; Bob} are in the process of deciding to which target users T = {Charlie; Dan; Eve; Frank} they grant access to a photo in which both of them are depicted.Alice and Bob are of type close friends to one another. Negotiating users defined the following groups: Alice defined G Alice ={CloseFriends} so that CloseFriends = {Charlie; Dan; Eve}; and Bob defined G Bob = {CloseFriends; Family} so that CloseFriends = {Charlie; Eve} and Family ={Dan; Frank} .

Now, assume that negotiating users have given the following priorities to their friends. Alice has given priority 3, 4 and 2 to Charlie,Dan and Eve respectively. Bob has given priority 3 to all his friends .Then according to algorithm this post can be shared only with Charlie as he is the only one whose friend type is same as that of friend type between Alice and Bob and his priority is greater than 2.Even though Eve belongs to the same friend type of CloseFriend his priority number given by Alice is only 2 so this particular post can't be shared with him.
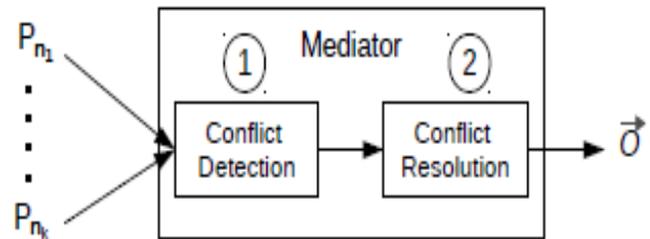

Fig 3.1 Mechanism Overview

Tagging with Textual content: Tagging is one of the common features that we can find in most of social media. People on social media use tagging feature for many reasons. Some of them are
To include someone who was at an event/happening
Vigilant someone when you talk about them
Give credit where credit is due
Increase the reach of social media marketing by encouraging others to share it
It would be a nice gesture to tag the people who attend the same event in a post relevant to that event. By this way they get to know that someone posted about that event and they can view whatever it is that is posted. It also let them know that someone is talking about them.
This is the polite thing to do online so that one is not talking behind other person's back. Whether they are saying something good or bad, they should still tag that person so that they know they are talking about them and have a chance to respond if needed.
Tagging others allow not only people following the user but also the tagged users follower to see the post. It is advantageous for both parties involved for more exposure.
As everything as its own good and bad sides even tagging feature can also be misused. There are lots of cases of cyber-crime where social media has been misused to defame others. Even more severe cases have happened by misusing these social media.
In the current scenario of social media anybody can tag anyone in any kind of post without that particular person's permission. This is giving an opportunity for users to harm other user. This harmful act can be defamation which in turn leads to many other severe crimes.
So in order to overcome the above mentioned problem, in this project I have implemented a method that does not allow anybody to tag anyone without their permission. If someone wants to tag other person in textual content, first that person need to type the content that he or she wants. After that they should select the persons they want to tag and next they should select to whom are all the other users

this tagging post should be viewed. Once this is done automatically alert will be sent to tagged people. If only that person give permission then that particular person will be tagged in that post. If that person does not give permission then that post won't get posted. If more number of people were tagged in a particular post and in that only few people give permission to be tagged then only the people who have given the permission will be tagged in that post .And remaining users who didn't give permission won't be tagged in that post.

Timing constraints can also be set by the up loader if he wants. If it is set then the up loader should receive the response from tagged people within the time that is mentioned by the up loader. If response is not received by the up loader, then he will do the action of either posting or not posting the text based on the action specified in the setting.

This whole tagging post will be viewed by all the other users that they selected to be viewed.

By implementing this method no other person can involve some other person in their post without their permission. This will help to reduce lot of crimes that is happening using social media and also increases the security and privacy of individual users on social media.

Uploading Image Post: Social media users uploads photo, it is one of the feature offered by almost all social media. That photo can be anything related to an event, tour photos that an up loader has gone with his friends or family or that photo can be anything personal or professional it is always a good habit to tag the people who are all included in the photo. It is nice gesture of acknowledging their presence.

If the persons in a photo are tagged, not only the up loaders follower but the entire tagged people follower can view that particular post. So it becomes a great platform for marketing. If the up loader wants the particular photo to be viewed by as many persons as possible then also by tagging all people included in that particular photo, up loader can be able to make it reach maximum number of people.

This technique can also be misused to defame one by uploading their private photo and tagging them in that post. By doing this up loader is not making only his friends but also that person's social media friend able to see that post and defaming that person in front of maximum users possible. It is one of the dangerous things that can happen on social media.

In the current scenario of social media anybody can tag any user in any kind of images. This is increasing the risk of privacy violation and security issues. When someone is being tagged in a photo, the tag not only reveals that someone is in the photo, it also links to that persons specific

social media profile and, if done well, is positioned across that persons face. This means everyone who has access to the photo can see who that person is and learn more about that person via that person's profile. This can be fun, but it also raises privacy concerns.

In order to avoid this and to increase the security and privacy of all the individual users of social media I have included face recognition system in this project. Face recognition is an application used to identify or verify person from an image or video stream.

In this project, when any user uploads an image face recognition system recognizes the face in that image and compares that face with the profile picture database it has. If any match is found then to that matched user an alert is sent. If that person gave permission then only that particular post gets posted. If not that post won't get posted. If no match is found then that post will get posted automatically.

Face recognition system implemented in this project is able to recognize only a single face. If there are multiple faces in the image, the implemented face recognition system is not able to recognize rest of the faces. In order to cope up with the computational speed a single face recognition system has been used here.

Timing constraint can also be integrated with this module in order to improve the working of overall system.

Here through implementation of this, a method has been proposed to improve the security and privacy of individual users. This can be extended to recognize multiple faces in an image in the actual social media interface.

IV. RESULTS

The following results are tabulated by considering only ten users.

Constraints	Matched percentage
Priority	80%
Friend type	20%
Priority and friend type	20%

Only for those users whose priority and friend type constraints match, algorithm allows the item to further re share otherwise re share of post can't be done to that user.
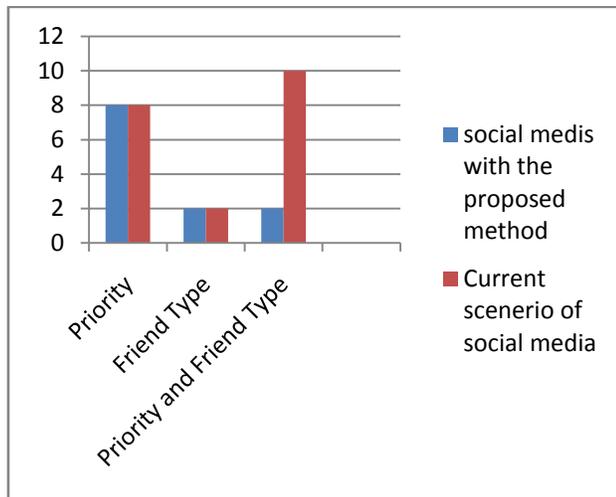
The above graph has been drawn by comparing the proposed method with the current scenario of social media. As shown in graph, in the current scenario of social media any user can re share the post he/she has on their timeline without considering the original post owners preference.

Whereas in the proposed method only for users whose priority and friend type constraints matches, the post can be re shared.

Since without getting permission no user can tag or upload image post of another user in the proposed method, individual user security has also improved compared to current scenario of social media.

V. CONCLUSION AND FUTURE WORK

Through this project I have tried to increase the security and privacy of individual users on social media by implementing algorithm and tagging permissions. Sharing of someone else's post is made more draconian .Algorithm checks for friend type parameter and the specified threshold. Only to those users who match these constraints, the post can be shared. By integrating tagging permission feature no one can comment, tag or upload photos of users without their permission .This whole project can be integrated as a mediator in any social media and make it the most secure platform.

This entire mediator is only giving importance for security. In the midst of this, the fun part of social media is missing which is one of the main purposes of social media. One can try to balance between the security and fun of social media in future.

REFERENCES

Wishart, Ryan, et al. "Collaborative privacy policy authoring in a social networking context." Policies for distributed systems and networks (POLICY), 2010 IEEE international symposium on. IEEE, 2010.

Squicciarini, Anna Cinzia, Mohamed Shehab, and Federica Paci. "Collective privacy management in social networks." Proceedings of the 18th international conference on World wide web. ACM, 2009.

Hu, Hongxin, Gail-Joon Ahn, and Jan Jorgensen. "Detecting and resolving privacy conflicts for collaborative data sharing in online social networks." Proceedings of the 27th Annual Computer Security Applications Conference. ACM, 2011.

Carminati, Barbara, and Elena Ferrari. "Collaborative access control in on-line social networks." Collaborative computing: networking, applications and worksharing (CollaborateCom), 2011 7th international conference on. IEEE, 2011.

Hu, Hongxin, Gail-Joon Ahn, and Jan Jorgensen. "Multiparty access control for online social networks: model and mechanisms." IEEE Transactions on Knowledge and Data Engineering 25.7 (2013): 1614-1627.

Hu, Hongxin, et al. "Game theoretic analysis of multiparty access control in online social networks." Proceedings of the 19th ACM symposium on Access control models and technologies. ACM, 2014