A Survey On Privacy Conflict Detection And Resolution In Online Social Networks

Miss. Patare Tanuja Vilas[1], Prof.N.G.Pardeshi[2]

[1] *PG Student, SRES'COE, Kopargaon, SPPU, Maharashtra, India*
[2] *Assistant Professor of Computer department, SRES'COE, Kopargaon, SPPU, Maharashtra, India*

ABSTRACT

In recent years social media got huge growth with billions of users but they also have to face privacy violations. There are no of items are uploaded by multiple users on a social media like photos, comments etc but applying preferences of only one party may leads to privacy issues. Social media only considers the uploader's privacy preferences not other users who affected by that item. The affected users are those who having privacy issues regarding that uploading item in which they are depicted. To solve this problem proposed system have a set of negotiating users who co-own an item where one user(uploader) in that set wants to upload an item on a social network and other users affected by the item. All users have their individual privacy policies for that item and there is a set of target users, whom item will be shared. Policy includes either granting or denying access to the targeted users for that item. But there are some privacy policies that may have contradictory decisions. Contradictory policy contains one policy in which targeted user can access item and another policy in which he does not having access. Currently there are some approaches to solve this situation but it requires manual negotiation of user's. In this paper system introduces a mechanism to solve this privacy conflicts by inspecting all users' individual privacy policies and comparison between them. Based on that, system models concession rules for users and provides automatic resolution for it. Modelling of concession rules is based on user's behaviour in the existing privacy control approaches. System captures user behaviour based on their willingness to grant/deny access for particular user for that uploading item.

Keyword: - *Social Media, Privacy Conflicts, Multi Party Access Control, Conflict Resolution*

1. INTRODUCTION

Now a day's no of items upload by multiple users on online social media and users can set their privacy preferences for that items .But social media only allows uploader to set his privacy policy for that item i.e. who can have access to the item. This is may lead to privacy violations that other users who affected by that item cant set privacy preferences for it [2]. For example photo in which multiple users are included and one of the user wants to upload that photo on social media (uploader) then only he having rights about to whom he wants to share that photo. But here the other users in that photo may have privacy issues regarding this situation. The existing approach uses manual user negotiation to solve this problem by using email, SMSs, phone calls etc. But this approaches require more time to deal with situation manually because there are multiple uploader and accessor are present on social media. In this paper system introduces a new approach to deal with these privacy issues. Here system considering all users individual privacy preferences and identify at least two policies that having contradictory decisions about granting/denying access for that particular item i.e. privacy conflict. System provides a conflict solution by modelling access control in such a way that all users involved in that uploading item accept that solution and ensure about their privacy.

1.1 Scope
- Used in online social networking.
- Find out privacy conflicts and its solution.
- System does not provide a method to automatically detect which items are co-owned.

1.2 Objective
- To provide individual privacy policy settings to all users.
- To provide privacy conflict detection.
- To provide automated privacy conflict resolution.

2. LITERATURE SURVEY

There are some existing approaches present to solve privacy conflicts like Uploader Overwrites (UO), Majority Voting (MV) and Veto Voting (VV). Uploader Overwrite is not being collaborative as it does not consider other user's preferences involved in that item. It only considers uploader policy for item that he/she wants to upload. Majority voting is better that UO but one of the user/s may have privacy consequences. And veto voting (VV) is too restrictive and not suitable for all situations and sometimes may loss sharing opportunities. In this paper a proposed mechanism that is Automated Conflict Resolution (AR) provides better outcomes than other three by modeling user's behavior in a particular situation.

2.1 Kurt Thomas, Chris Grie[2]

In this paper the author approaches better understanding about type of information exposed by privacy conflicts on a social media. System analyzed mainly two factors that are friendship and wall posts of users. When a user posts a comment to a friend's wall, he does not have right to decide who sees the comment and if a user posts a photo by tagging friend in the photo, the friend cannot specify which users can view the photo. This leads to privacy conflicts so here system provides policy protection so that this information cannot be exposed against users will. Here system limits to Group membership, photo tagging where multiple parties cannot control data exposure.

2.2 J. M. Such, A. Espinosa, A. Garcia-Fornes [3]

In this paper the author approaches protection of privacy and its relation with multi-agent systems. This system is used to prevent undesired information collection by means of secure data transfer and storage. System also prevents undesired information processing by using anonymity techniques and prevents undesired information dissemination based on trust. This paper defines information privacy and its relation to multi-agent systems. Also represents a survey of privacy-preserving mechanisms developed against information collection.

2.3 Lujun Fan, Kristen LeFevre [4]

In this paper the author approaches the problems related to the average users of the social media who cannot set their privacy in detail. So here system build a machine learning model that gives details about preferences of particular user's, and then provide automatic configuration of user's privacy settings based on some limited no of user inputs like asking few no of questions to the users. Based on that, system builds the privacy preference model which is used to automatically configure user's privacy settings. Here system keeps user's interaction as simple as possible. This model accounts only few no of situations and user's willingness to spend time into the specification process of policy is also a main concern.

2.4 F.Faziyudeen, T .Nalini, Ayyappan. G [5]

In this paper the author approaches the system that considers the access request against the policy specified for every user and provides a decision for the access. If a user posts a comment in a friend's space, he/she can specify which users can view the comment. The authorization decisions are based on the relationship between the resource owner and the resource accessor in a social network.

2.5 Jose M. Such, Michael Rovatsos [6]

In this paper the author approaches that user privacy preferences for the same item on a social media may conflict and provide unsatisfactory results regarding user's privacy. So here system proposes a mechanism of negotiation for users, to provide aggregation on highest action vector utility which is based on the preferred privacy policies of each agent and the relationship between the negotiating agents and other target agents.

2.6 R. Wishart, D. Corapi, S. Marinovic [7]

In this paper author approaches a collaborative method to define privacy policies. Here the owner of the item is responsible for uploading it to the social networking site and then specify privacy policy for the content. Here owner can nominate a number of friends on the social networking site to modify the scope of the policy. Based on that system refer to these individuals as co-owners of the item and assume that they will be affected by the disclosure of the item. System analyzes the privacy conflict and modifies the content as per co-owner's wish based on policy authoring process. Here if one of the co-owner is having malicious behavior then with the help of owner and co-owner voting he will get removed from the policy authoring process.

3. SYSTEM OVERVIEW

Strategy of proposed system is to develop social networking site with recommended functionalities where user can utilize the application and main core can process under it. The social media have multiple no of users. The system proposes mainly two types of users either from same or different groups. Firstly negotiating users is a set of users who co-own an item. One of them wants to upload an item and other users become affected users for that same item. Second one is targeted users set to who item will be shared based on negotiating user's privacy preferences.

The proposed system includes following phases:
- User Authentication
- Data Uploading
- Individual Privacy Policy
- Conflict Detection
- Conflict Resolution

3.1 Modules

- User

  Authentication:
  Every user will have a registration phase where they will register and can login into the application using their credentials. During registration they need to upload their face front clear photo which will term as their training data to match it with other captured instances. Their credentials will be verified from the server side and every user will be validated during login to maintain the genuineness of the user. After login they can view their profile and can add their information. They can add friends and can post images or text.

  Data Uploading:
  Every user can upload image or can post text in the application. When a user post an image then there is an option to select the names from their friend list as to tag the image with multiple selection. Once the Image is uploaded it won't be posted instantly it goes for verification in the admin side. Also a notification is sent to other users who are tagged in with that image.

  Individual Privacy Policy Settings:
  The uploader of item and other users who are depicted or affected by the item can have their individual privacy settings for that item. They can decide to grant/deny access to the targeted user for that item.

- Admin

Conflict Detection
If users don't want that image to be uploaded then they can convey their message or else they can grant access to post that image. Compare the individual privacy preferences of each negotiating (uploader and affected) user in order to detect conflicts among them. If all the action vectors of all negotiating users assign the same action for all target users, then there is no conflict. Otherwise, there are at least two action vectors that assign different actions to the same target user then there is a conflict.

Conflict Resolution:
In this phase admin identifies the conflicted users. System models concession rules by estimating about uploader and affected user's willingness and tie strength with targeted user automatically provides solution for conflict. After that a message is thrown to the user who posted that item about the final conclusion.
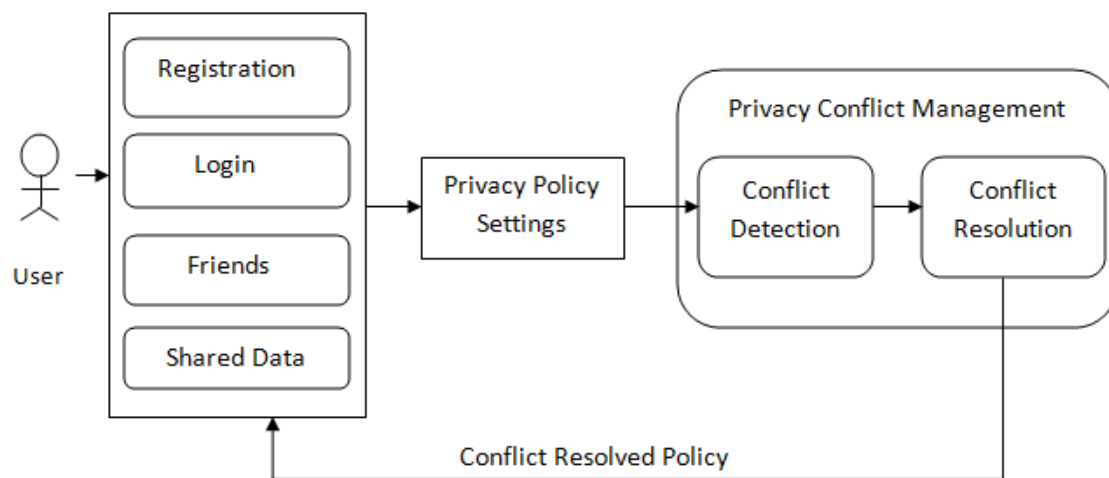

Fig -1: System Architecture

3.2 Implementation Details

- Conflict Detection Algorithm:
  System compares all negotiating user's privacy preferences for uploading item in order to detect conflicts between them. It find outs at least two conflicted policies in which one policy giving grant to the targeted user for item and another one denying for the same.

- Conflict Resolution Algorithm:
  The conflicted user is given as input to the algorithm. System find outs user's willingness to change their preferred action (grant/deny) for particular targeted user. Based on that system models concession rules and finally user will get the solution as a conflict resolved policy.

4. CONCLUSIONS

Online social media have billions of users and also having no of privacy issues. Users uploads no of items on a social media and granting/denying access to other users for that particular item is based on their privacy preferences. Here system concerns uploader's as well as affected user's policy for that item to grant/deny access to the targeted users. For that, system provides new mechanism of conflicts identification with atomic solution on a social media.

5. ACKNOWLEDGEMENT

6. REFERENCES

[1] "Resolving Multi-Party Privacy Conflicts in Social Media" by Jose M. Such,Natalia Criado, IEEE Transactions on Knowledge and Data Engineering,2016,pp. 1851-1863.

[2] "Unfriendly: Multi-party privacy risks in social networks," by K. Thomas, C. Grier, and D. M. Nicol, in Proc. 10th Int. Symp. Privacy Enhancing Technol., pp. 236–252.2010.

[3] "A survey of privacy in multi-agent systems," by J. M. Such, A. Espinosa, and A. Garc_ıa-Fornes, Knowl. Eng. Rev., vol. 29, no. 03, pp. 314–344, 2014.

[4] "Privacy wizards for social networking sites," by L. Fang and K. LeFevre, in Proc. 19th Int. World Wide Web Conf. , pp. 351–360, 2010.

[5] "Multiparty access control for online social networks: Model and mechanisms," by H.Hu, G. Ahn, and J. Jorgensen ,IEEE Trans. Knowl. Data Eng., vol. 25, no. 7, pp. 1614–1627, Jul. 2013.

[6] "Privacy policy negotiation in social media," by J. M. Such and M. Rovatsos, ACM Trans. Auton. Adaptive Syst., vol. 11, no. 1, Art. no. 4, Feb. 2016.

[7] "Collaborative privacy policy authoring in a social networking context," by R. Wishart, D. Corapi, S. Marinovic, and M. Sloman, in Proc. IEEE Int. Symp. Policies Distrib. Syst. Netw., pp. 1–8, 2010.

[8] "Are you close with me? Are you nearby? Investigating social groups, closeness, and willingness to share," by J. Wiese, P. Kelley, L. Cranor, L. Dabbish, J. Hong, and J. Zimmerman, in Proc. 13th Int. Conf. Ubiquitous Comput. , pp. 197–206 2011.