Multiparty Privacy Management and Cluster Analysis in Social media (MPMC)

Sreekutty J.S., Hamil Stanly, Archa A.T.

Abstract— The current mainstream Social Media infrastructures without multi-party privacy management do not preserve the privacy of each users as they are unable to appropriately control to whom co-owned items are shared. For solving this issue, here introduce a automatic conflict resolution mechanism with the help of a mediator; it could be integrated as back end as a service; which detect conflict by inspecting all the privacy policies of negotiating users. If any contradictory decision is arises it solve the conflict by detecting that Items sensitivity and Users prioritization to that item. Through determining "Co-owners desire to change an action" by generating appropriate solution. The solution based on some principle which checks whether the uploaded item may cause any detrimental action to one of the user involved in that; apply Concession rules, instantiates based on users willingness to change an action(Granting/Denying). For comparing the uploaded pictures cluster analysis is used to group all the picture that are uploaded. Similarities are detected in terms of their color, edge etc and Kmeans clustering is used to recognize communities within large group of people. In short this mechanism is implemented as a proof of preserving all negotiating users privacy management.

***Index Terms*— Conflict, Multiparty privacy, Online social network, Social networking services.**

I. INTRODUCTION

Social media are computer-mediated technologies that allow creating and sharing of information, ideas, career interests and other forms of expression via virtual communities and networks. Photos are a proven way to increase your engagement on social media. In terms of both likes and comments photos far exceeded other post types in engaging consumer responses. Only the uploader's privacy preferences are considered by the social media ;it does not concern about other user affected by that item. The affected users are the co-owners and they have their own privacy settings that sometimes it conflict uploaders privacy. The existing approaches needs manual negotiation techniques for solve this problem but it is very time consuming one.

Recent survey explains a number of important design considerations for photo privacy tools around the importance of identity and impression management and the tensions of ownership. "Restrict Others Tool" explicitly dealt with the natural tension that arises between the owner of the photo, and those tagged in it. Here created a lightweight means for users to negotiate desired sharing, complementing the existing privacy coping mechanisms that users currently employ. In manipulating these ownership tensions, and believe their tool would help users achieve more desired privacy while still maximizing the social value of sharing. But this design technique only inspects 2 parties privacy policy but we need to set the members manually[2]. Another mechanism is called "Face Recognition system" - is to be used to solve this issue by recognize everyone in the photo(co-owners) . After recognition system will automatically send the messages to the each of the person involved in an item and asking for them whether they are agree to reveal this item to public(The information will be spread over users and consensus could be reached).

But the problem is that FR engine with higher recognition ratio demands more training samples (photos of each specific person), but online photo resources are often insufficient[3]. For solving these issues an agent is needed to inspect all the users privacy policies automatically. Hence "J. M. Such and M. Rovatsos", introduce, negotiating agents are inspected to identify any conflict. If conflicts are found, then agents run the negotiation mechanism to resolve every conflict found. Detecting each agents intimacy to the target one,it solve the dispute. But Negotiation however do not always succeed in reaching solutions to dispute. So third party interventions are needed[4]. Another research by "H. Hu, G. Ahn, and J. Jorgensen" for solving multiparty access control by the use of a policy. This paper generate a systematic solution to facilitate collaborative management of shared data in OSNs through a policy called MPAC(Multiparty Access Control) Policy. This policy is set based on controller, ctype, accessor, data and effect. But it is very difficult to ascertain the limits among relations[5].

This is the reason for an automatic computational mechanism that does not need any user interaction, so here suggests first computational mechanism which automatically inspects all the privacy preferences , if any conflict is detected, solve it.

II. OBJECTIVE

The main objective is to provide individual privacy policy settings to all users. Also provide privacy conflict detection and automated privacy conflict resolution

Manuscript received Mar 07, 2017.

***Sreekutty J.S**, Computer Science and Engineering, Sarabahi Institute of Science and Technology, Trivandrum, India, Mobile No:8281892943*

***Hamil Stanly**, Computer Science and Engineering, Sarabahi Institute of Science and Technology.*

***Archa A.T.**, Computer Science and Engineering, Sarabahi Institute of Science and Technology.*

III. System Overview

Number of individual using the social media increases dramatically . This system is to be set up for two types of users either having same privacy policies or having that of different. Firstly identifying the users and co-owner of an item. One of them wants to upload an item and other users become affected users for that same item. So here use a mediator which could be integrated as backend, it detect all the privacy policies of negotiating users and if any conflict found ,it flags off all. The proposed system includes following phases:

- User Activities
- Conflict Detection
- Conflict Resolution

1.USER ACTIVITIES

i. Registration

User can register into these media by entering his Name, DOB, Address, Phone num, Email Id, Password, Security questions etc. The registered user can login into the system by using this E-mail Id and Password.

ii. Data Uploading

Every user can upload the data especially pictures and comments that mention multiple users through these social networking services. User can provide an optional message or heading with this image. Image can be selected from the existing resources or taken instantly. Users wants more likes and share, Because they want to popularize themselves.

iii. Privacy settings

Select friends and add them to a group. Both uploader and users who all are affected by the item have their own privacy settings for it. They can decide to grant/deny access to the targeted user for that item.

Format, P = ({A}.{E})

Where, A represent the groups that are granted to access an item, E is the excluding member in the group that need policies.

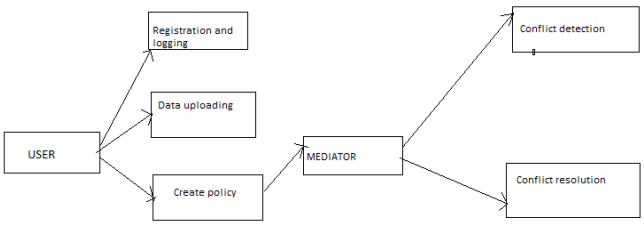

Fig.1: Mechanism overview

2. CONFLICT DETECTION

Mediator inspects all the privacy policies of each negotiating users. For comparing each privacy policies, consider the effect in which particular policies has on target user .The owner has availing two actions granted the access and deny the access. so here consider an action vector v(t). if all the negotiating users assign same action to the particular item , it means that there is no conflict if else there occurs a conflict in the implementation section mediator runs the conflict detection algorithm and find out the conflict[1].

Algorithm 1 Conflict Detection

Input: $N, P_{n_1}, \ldots, P_{n_{|N|}}, T$
Output: C

1: **for all** $n \in N$ **do**
2: **for all** $t \in T$ **do**
3: $v_n[t] \leftarrow 0$
4: **for all** $G \in P_n.A$ **do**
5: **if** $\exists u \in G, u = t$ **then**
6: $v_n[t] \leftarrow 1$
7: **end if**
8: **end for**
9: **end for**
10: **for all** $e \in P_n.E$ **do**
11: $v_n[e] \leftarrow \neg v_n[e]$
12: **end for**
13: **end for**
14: $C \leftarrow \emptyset$
15: **for all** $t \in T$ **do**
16: Take $a \in N$
17: **for all** $b \in N \setminus \{a\}$ **do**
18: **if** $v_a[t] \neq v_b[t]$ **then**
19: $C \leftarrow C \cup \{t\}$
20: **end if**
21: **end for**
22: **end for**

Here N is the set of negotiating users, P's are the policies, T is the target user. Consider a single negotiating user from a set of Negotiating users and assume a particular target user t. If action vector of all negotiating user is Assigns) value(deny the access) Then the system disallow the sharing process. On the contrarily if the action vector assigns as !(granted the access) the system will grant it. If at least two users action vector is disagreeing one (1 and 0)it means of a conflict.

For example, assume that Anju is the owner of a comment or picture uploaded (content), The content may contains other peoples such as Appu, Arya, Arun, Veena and Anusree. So Arya is one of the negotiating user in this content. Anju wants to share this content to her "Myfriends" group. It contains {Appu, Arun, Anusree}. But arya wants to share this content to her "Family". It contains {Appu, Arun and Veena}.

Hence P1 = { 1,0,1,0,1}
P2 = {1,1,1,1,0}

This means that P1 ≠ P2 (A conflict in both privacy policies).

3. CONFLICT RESOLUTION

The mediator suggest the solution based on three principles:

1. If an item may cause any detrimental action to one of the user involved , that item should not be shared
2. An item should be shared if it is not generating any harm to all negotiating users and also it is vital for one person
3. In the conflicting section, the mediator automatically solve the conflict based on concession rule.[1]

If the conflict is to be detected the mediator runs the conflict resolution algorithm and the output is generated.

Let N be the set of negotiating users, P's are their policies, C is the conflict which is to be taken as the output of first algorithm. Consider a particular negotiating user n whose willingness to change an action is very high, then the output is to be calculated based on the modified majority of policies. If there is an another negotiating user a whose willingness to change an action is very low, and their action vector towards the conflict is an disagreeing one, then take the decision

based on concession rule – either deny the sharing or action vector of particular target users decision is accepted.

Algorithm 2 Conflict Resolution

Input: $N, P_{n_1}, \ldots, P_{n_{|N|}}, C$
Output: $\vec{o}$
1: **for all** $c \in C$ **do**
2:
3: **if** $\forall n \in N,\ \mathcal{W}(n,c)$ is HIGH **then**
4: $o[c] \leftarrow$ modified_majority$(P_{n_1}, \ldots, P_{n_{|N|}}, c)$
5: **continue**
6: **end if**
7:
8: **if** $\exists a \in N,\ \mathcal{W}(a,c)$ is LOW **then**
9: **if** $\exists b \in N,\ \mathcal{W}(b,c)$ is LOW $\wedge\, v_a[c] \neq v_b[c]$ **then**
10: $o[c] \leftarrow 0$
11: **else**
12: $o[c] \leftarrow v_a[c]$
13: **end if**
14: **end if**
15: **end for**

For solving the conflict, the mediator first inspect all negotiating users privacy preferences and determine what makes the users to change their decision(grant or deny the access). For this purpose, the mediator first inspect the sensitivity of an item and Prioritization of an item.

a. Sensitivity of an item

If an item is very sensitive for a user, he/she will not share this item to others. For example, Ammu is a co-owner of a photo sharing activity. Her friend Achu Upload a picture regarding a night party which shows the intimate relationship between Achu and Ammu or comment that mention about Ammu. Achu and Ammu are cousins. Achu set the privacy preference as his "Family". It contains Ammus Mother. Ammu doesn't want to disclose this secret to her mother. So, for Ammu, this item is very sensitive to her.

The sensitivity of an item is to be calculated by

$S_n = (1/G_n) \sum T_n(G)$[1]

Where S_n = Sensitivity of an item
$T_n(G)$ = Tie strength between two parties
G_n = Groups

Tie strength between groups can be determined by estimating the minimum strength needed for an item to shared in a group ṕ(n,c).

$S_{ammu} = (1/G_{ammu}) \sum T_{ammu}(family)$
$T_{ammu}(family)=5$.

b. Prioritization of an item

This section deals with conflicting areas. It determines about different negotiating users assigns different actions to the same target user. For example, Appu planned to provide a surprise party to his close friend Vinu. He wants to invite all his other close friends to Vinus home except Vinu. The relationship between the user and target user is high. Geethu is another member in this group. She is Vinus sister and she disclose every matter to her brother, she doesn't want to hide anything from her brother. The relationship between Geethu and Vinu is high. Hence prioritization can be determined by the formula,

$P_n© = S_n - ṕ(n,c)$ [1]

Where $P_n©$ = Prioritization of an item
S_n = Sensitivity of an item
ṕ(n,c).= Minimum strength needed for an item to shared in a group

ṕ(n,c) can be calculated by an example:
where n denotes negotiating user and c denotes target user.
If Anju wants to share an item to three peoples – Anu, Achu, Allu. Anu is her best friend, Achu is her good friend and allu is her friend.so

ṕ(Anju,Anu) = 5
ṕ(Anju,Achu) = 4
ṕ(Anju, Allu) = 3.

c. Determine the Desire

The desire to change an action can be determined by above two criteria.

If sensitivity of an item and its prioritization is very high-the negotiating user wont share the item to target user. O the contradictory, if sensitivity of an item and its prioritization is very loe-the negotiating user will ready to share the item to the target user.

$D = 0.5\ (((\partial - P_n©) / (\partial + P_n©)) / (\partial - S_n) / (\partial + S_n))$

Where D = Determine the Desire
∂ = Tie strength maximum value.

In the above example tie strength maximum value goes to 5(Best friends).

4. Cluster analysis

Cluster analysis is used in this media for grouping all the photos that uploaded in such a way that these pictures are in the same group(called a cluster) are more similar(in sense of their color, edge etc) to each other than to those in other groups(clusters). Here clustering is used to recognize communities within large groups of people. Centroid based clustering is used in which clusters are represented by a central vector, which may not necessarily be a member of the dataset. When all these pictures are considered to k, kmeans clustering gives optimization as: k cluster on center and assign the object to the nearest cluster center,such that the squared distance from the clusters are minimized.

Algorithmic steps for kmeans clustering

Let X= {x1,x2,……,xn} be the set of datapoints and V={v1,v2,….,vc}be the set of centers.

i. Randomly select "c" cluster centers.
ii. Calculate the distance between each datapoint and cluster centers.
iii. Assign the datapoint to the centerwhose distance from the cluster center is minimum of all the cluster centers.

iv. Recalculate the new cluster using datapoints.

$$V_i = (1/c_i)\sum x_i$$

Where c_i representsthe number of datapoints in ith cluster.

v. Recalculate the distance between each datapoint and new optained cluster centers.

vi. If no datapoint was reassigned ,then stop, otherwise repeat from stepiii.

IV. CONCLUSION

In recent years social media got huge growth with billions of users but they also have to face privacy violations. 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. The system having a graphical representation which shown that the percentage of people who have contradictory decision in an area - who accept the solution and reject the solution.

REFERENCES

[1] J.M.Such, Jose M., and Natalia Criado. "Resolving multi-party privacy conflicts in social media." IEEE Transactions on Knowledge and Data Engineering 28.7 (2016): 1851-1863.

[2] Besmer and H. Richter Lipford, Moving beyond untagging: Photo privacy in a tagged world, in Proc. SIGCHI Conf. Human Factors Comput. Syst., 2010, pp. 15631572 [6] J. M. Such and M. Rovatsos, Privacy policy negotiation in social media, ACM Trans. Auton. Adaptive Syst., vol. 11, no. 1, Art. no. 4, Feb. 2016

[3] Yuanxiong Guo,Kaihe Xu"My Privacy My Decision: Control of Photo Sharing on Online Social Networks",IEEE Transactions on Dependable and Secure Computing.Florida,aug.2015

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

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