AUTOMATED DETECTION AND RESOLUTION OF CONFLICTS IN MULTIPARTY PRIVACY MANAGEMENT FOR SOCIAL MEDIA

[1]Monali Kachare, [2]Minal Gale, [3]Dhanashri Wagh, [4]Priya Chinchole

[1,2,3,4]Students
Bachelor of Engineering (Information Technology).
SKN Sinhgad Institute of Technology & Science, Lonavala, Maharashtra, India.

Abstract: **Hundreds of billions of loaded items in Social media are commonly owned by multiple users, however only the user who uploads the item can establish their privacy (i.e. who can access the item).Things shared through Social Media may influence more than one client's security-e.g., photos that delineate different clients, remarks that specify different clients, occasions in which numerous clients are welcomed, and so forth. The absence of multi-party security administration bolster in current standard Social Media foundations makes clients unfit to properly control to whom these things are as a matter of fact shared or not. Computational mechanisms that are able to combine the privacy preferences of multiple users into a single policy for an item can help resolve this problem. However, merging multiple users' privacy preferences is a difficult task, because privacy preferences may conflict, so methods to resolve conflicts are needed. Moreover, these methods need to consider how users' would actually reach an agreement about a solution to the conflict in order to present solutions that can be admissible by all of the users affected by the item to be shared. Current techniques are either too demanding or only consider fixed ways of aggregating privacy preferences. We propose the first computational mechanism to resolve conflicts for multi-party privacy management in Social Media that is able to acclimate to different situations by creating the concessions that users make to reach a solution to the conflicts. We give tagline to the original sender to overcome on no concession rule. We also recommend friends based on current users interest.**

Index Terms **- Social media, Privacy, Conflicts, Multi-Party Privacy, Social Networking Services, Online Social Networks, Friend Recommendation, User Willingness.**

I. INTRODUCTION

Social media sites nowadays have a pervasive presence in society. User can study a lot of useful data about human behavior and interaction by paying attention to the information and relations of social media users. This information can be open or private. Ensuring the confidential information of the clients in informal organizations is a genuine concern. It recommends various methods to solve these privacy conflicts. As of late we have been examining a tremendous increment in the development of on-line social systems. OSNs entrust individuals to share individual and open data and make social associations with companions, relatives and different people or groups. Notwithstanding the fast increment in the application of social organization, it raises various security and protection issues. While OSNs grant clients to restrain access to shared information, they as of now don't give any component to thoroughly authorize security issue solver connected with different clients. Existing system need too much human intervention during the conflict resolution process, by requiring users to solve the conflicts manually or close to manually; e.g., participating in difficult-to-assimilate auctions for each and every co-owned item. Other approaches to resolve multi-party privacy conflicts are more automated, but they only consider one fixed way of aggregating user's privacy preferences without considering how users would actually achieve compromise and the concessions they might be eager to make to achieve it depending on the specific situation. In this project, we present the first computational mechanism for social media that, given the individual privacy preferences of each user involved in an item, is able to find and resolve conflicts by applying a various conflict resolution method based on the concessions users' may be willing to make in different situations. Also we recommend friends to active user based on his/her interest.

II. LITERATURE SURVEY

Table 2.1 – literature survey table

SrNo	Author, Title and Journal Name	Advantages	Disadvantage	Refer Points
1	K. Thomas, C. Grier, and D. M. Nicol, "Unfriendly: Multi-party privacy risks in social networks," in Proc. 10th	1.Privacy must extend beyond single-owner model - Tags, links, mentions can	1.In absence of mutual friends, safe set of viewers tends towards empty set	1.Adapt privacy controls: - Grant users control over all personal references, regardless where it appears - Includes tags, mentions, links Allow users to specify global privacy settings

	Int. Symp. Privacy Enhancing Technol., 2010, pp. 236–252.	reference multiple users - Rely on these existing features to distinguish who is at risk 2.Allow each user to specify global privacy policy 3.Enforce policy on all personal content, regardless page it appears	2.Assume friends will consent to not sharing with wider audience 3.Content must be tagged; no other way to distinguish privacy-affected parties 4.Censorship; prevents negative speech	2.Prototype solution as a Facebook application - Satisfies privacy requirements of all users referenced - Determines mutually acceptable audience
2	A. Lampinen, V. Lehtinen, A. Lehmuskallio, and S. Tamminen, "We're in it together: Interpersonal management of disclosure in social network services," in Proc. SIGCHI Conf. Human Factors Comput. Syst., 2011, pp. 3217–3226.	1.The effective privacy management. In collaborative strategy, asking another person to delete content 2.Reporting inappropriate content to service administrators 3.Supporting a non-serious interpretation 4.Interpreting content to be non-serious		1.This paper considers SNS-users' concerns in relation to online disclosure and the ways in which they cope with these both individually and collaboratively. 2.A framework of strategies for boundary regulation that informs both theoretical work and design practice related to management of disclosure in SNSs.
3	P. Wisniewski, H. Lipford, and D. Wilson, "Fighting for my space: Coping mechanisms for SNS boundary regulation," in Proc. SIGCHI Conf. Human Factors Comput. Syst., 2012, pp. 609–618.	1.Privacy through effective interpersonal boundary regulation serves as a way to improve how individuals connect and share with others 2.Improved interface design to better support interpersonal boundary regulation could serve to improve, instead of prevent, higher levels of social interaction.	1.InterpersonaL boundary regulation within online social networks as a means to align interactional privacy needs.	1.This paper, investigates users' SNS boundary regulation behavior. 2.In this paper, filtering, ignoring, blocking, withdrawal, aggression, compliance, and compromise represent coping mechanisms individuals use within SNSs to maintain their interpersonal boundaries.
4	A. Besmer and H. Richter Lipford, "Moving beyond untagging: Photo privacy in a tagged world," in Proc. SIGCHI Conf. Human Factors Comput. Syst., 2010, pp. 1563–1572.	1.The proposed system is a lightweight means for users to negotiate desired sharing. 2.Help users to achieve more desired	1.To improve privacy management in online social networking communities.	1.In this paper, using a focus group, we explored the needs and concerns of users, resulting in a set of design considerations for tagged photo privacy. 2.This paper results identify the social tensions that tagging generates, and the needs of privacy tools to address the social

		privacy.		implications of photo privacy management.
5	J. M. Such, A. Espinosa, and A. Garc_ıa-Fornes, "A survey of privacy in multi-agent systems," Knowl. Eng. Rev., vol. 29, no. 03, pp. 314–344, 2014.	1.InteroperabiliTy and Openness 2.Pseudonym changer Agent 3.Disclosure Decision Making based on Multiple Criteria 4.Collective Disclosure Decision Making 5.Learning the privacy sensitivity of personal information 6.Personal Data AttributeInference 7.Information dissemination detection 8.Integration of trust, reputation, and norms for protecting against information dissemination 9.Avoiding collusion for protecting information dissemination 10.Protection Against information collection and dissemination		1.In this paper, we have introduced the issue of privacy preservation and its relation to Multi-agent Systems. To prevent undesired information dissemination based on trust and reputation on the one hand, and normative multi-agent systems on the other hand.
6	R. L. Fogues, J. M. Such, A. Espinosa, and A. Garcia-Fornes, "Open challenges in relationship-based privacy mechanisms for social network services," Int. J. Human-Comput. Interaction, vol. 31, no. 5, pp. 350–370, 2015.	1.Including a content type as a new attribute of access control can improve the flexibility and expressiveness of privacy policies. 2.ReBAC models in popular SNSs will improve the control of privacy for the users.	1.ReBAC models are complex 2.ReBAC model is not flexible	1. This paper presents a list of privacy threats that can affect SNS users, and what requirements privacy mechanisms should fulfill to prevent these threats. 2. Visualization tools should explain to the users in an understandable way how their information is disseminated according to a specific type of relationship.
7	R. Wishart, D. Corapi, S. Marinovic, and M. Sloman, "Collaborative privacy policy authoring	1. The collaborative policy authoring process more user-friendly	1.The scope of the policy can only be decreased by the nominated parties.	1.In this paper, propose a privacy-aware social networking service and then introduce a collaborative approach to authoring privacy policies for the service.

	in a social networking context," in Proc. IEEE Int. Symp. Policies Distrib. Syst. Netw., 2010, pp. 1–8.	and accessible to average users of social networks.	2.The inability of a user to claim co-ownership of a resource. 3.Provides limited help with authoring policies.	2.The approach permits the originators of content on the social network to specify policies for the content they upload.
8	H. Hu, G.-J. Ahn, and J. Jorgensen, "Detecting and resolving privacy conflicts for collaborative data sharing in online social networks," in Proc. 27th Annu. Comput. Security Appl. Conf., 2011, pp. 103–112. [Online]. Available: http://doi.acm.org/10.1145/2076732.2076747	1.An effective and flexible mechanism to support privacy control of shared data in OSNs.	1.Does not provide location security.	1.In this paper, we propose an approach to enable collaborative privacy management of shared data in OSNs. 2.Provide a systematic mechanism to identify and resolve privacy conflicts for collaborative data sharing.
9	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.	1.Flexible for regulating data sharing in OSNs. 2.System Usability is more. 3.Performance evaluation is more.	1.Time consumption task.	1.An MPAC model was formulated, along with a multiparty policy specification scheme and corresponding policy evaluation mechanism. 2.MController is functional proof-of-concept implementation of collaborative privacy management.
10	P. Fong, "Relationship-based access control: Protection model and policy language," in Procs. 1st ACM Conf. Data Appl. Security Privacy, 2011, pp. 191–202.	1.Multiple inheritances is more flexible when relationships can be activated.	1.Model checking could become intractable.	1.ReBAC is characterized by the explicit tracking of interpersonal relationships between users, and the expression of access control policies in terms of these relationships. 2.ReBAC model to capture the essence of the paradigm, that is, authorization decisions are based on the relationship between the resource owner and the resource access or in a social network maintained by the protection system.

III. SOFTWARE REQUIREMENT SPECIFICATION

User Classes and Characteristics

To design products that satisfy their target users, a deeper understanding is needed of their user components and product properties in development associated with unexpected issues that the user's faces every now and then while developing a project. The study will lead to an interaction model that provides an analysis of the interaction between user characters and the classes. It reveals both positive and negative patterns in text documents as higher level features and deploys them over low-level features (terms). In recommended work is designed to implement above software requirement. To implement this model following software requirements and hardware requirements are used.

Software Requirements

- Operating System - Windows XP/7
- Programming Language - Java/J2EE
- Software Version - JDK 1.7 or above
- Tools - Eclipse
- Front End - JSP

- Database - Mysql

Hardware Requirements

- Processor - Pentium IV/Intel I3 core
- Speed - 1.1 GHz
- RAM - 512 MB (min)
- Hard Disk - 20GB
- Keyboard - Standard Keyboard
- Mouse - Two or Three Button Mouse
- Monitor - LED Monitor

IV. COMPARISON BETWEEN EXISTING SYSTEM AND PROPOSED SYSTEM

Existing systems need too much human intervention during the conflict resolution process, by requiring users to solve the conflicts manually or close to manually; e.g., participating in difficult-to-comprehend auctions for each and every co-owned item. Other approaches to resolve multi-party privacy conflicts are more automated but they only consider one fixed way of aggregating user's privacy preferences without considering how users would actually achieve compromise and the concessions they might be willing to make to achieve it depending on the specific situation.

In proposed system, we present the first computational mechanism for social media that, given the individual privacy preferences of each user involved in an item, is able to find and resolute conflicts by applying a different conflict resolution approach based on the concessions users' may be willing to make in different situations. We compare the individual privacy preferences of each negotiating user in order to detect conflicts among them. Each user is likely to have prescribed different groups of users, so privacy policies from different users may not be directly comparable. To compare privacy policies from different negotiating users for the same item, it considers the effects that each particular privacy policy has on the set of target users. Privacy policies dictate a particular action to be performed when a user tries to access the item. It assumes that the available actions are either 0 for denying access or 1 for granting access. The mediator figures the answer for every contention found by applying the concession rules through conflict resolution mechanism and the arrangement will be encoded into an activity vector.

V. MATHEMATICAL MODULE

The following terms shows in detail working of project.

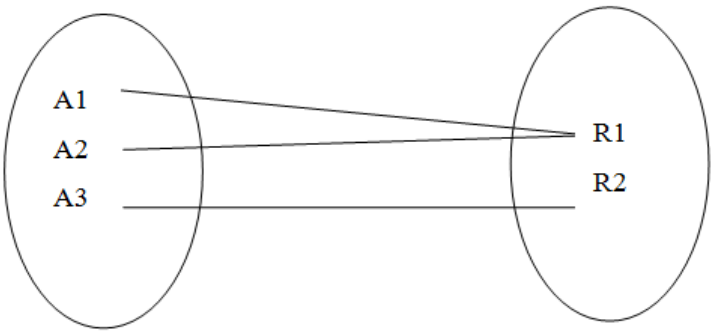

Figure 5.1-Relation

Where,
A1: Share files with privacy policies provided by the user
A2: Share files with privacy policies provided by the user
R1: Resulted web snippets provided by the sharing file process
A3: Share files with privacy policies provided by the user
R2: Error (Conflict) routine in the accessing file process.

Given a set of negotiating users N = $\{n_1, \ldots, n_k\}$ who co-own an item i.e., there is one uploader ∈ N who uploads the item to social media and the rest in N are users affected by the item; and their individual (possibly conflicting) privacy policies $P_{n1}, \ldots, P_{nk}$ for that item; how can the negotiating users agree on with whom, from the set of the target users T = $\{t_1, \ldots, t_m\}$, the item should be shared?

This problem can be decomposed into: (1) Given the set of individual privacy policies $P_{n1}, \ldots, P_{nk}$ of each negotiating user for the item, how can we identify if at least two policies have contradictory decisions—or conflicts—about whether or not granting target users T access to the item. (2) If conflicts are detected, how can we propose a solution to the conflicts found that respects as much as possible the preferences of negotiating users N.

We defined the set of target users as a subset of the users to remain as general as possible; i.e., without forcing it to satisfy a particular property. However, the set of target users could be further qualified as a particular subset of users satisfying any property without changing the subsequent formalization; e.g., the set of target users could be defined as the union of all of the negotiating users' online friends.

Conflict Detection:

Given a user n ∈ N, her groupsG_n, her individual privacy policy $P_n =< A, E >$, and a user t ∈ T; we define the action function as:

$$act(P_n, t) = \begin{cases} 1\ if \exists G \in G_n : t \in G \wedge \in P_n.A \wedge t \notin P_n.E \\ 1\ if \exists G \in G_n : t \in G \wedge \notin P_n.A \wedge t \in P_n.E \\ 0\ Otherwise \end{cases}$$

Note that the definition of this function will vary according to the access control model used, but it will be defined in a similar way. That is, the idea is to be able to know, given a target user t, whether the privacy policy will grant/deny t access to the item regardless of the access control model being used. In particular, we assume that the available actions are either 0 (denying access) or 1 (granting access).

Given a set of negotiating users N and a set of target users T; a target user t ∈ T is said to be in conflict iff ∃a, b∈N with individual privacy policies P_a and P_b respectively, so $V_a[t] \neq V_b[t]$

Further, we say that the set of users in conflict C ⊆ T is the set that contains all the target users that are in conflict.

Input:

N = {negotiating users}

$P_{n1}, \ldots, P_{nk}$= {privacy policies}

T = {target users}

Output:

C = {conflict}

Recall groups are disjoint. Otherwise, the complexity is$O(|\ U\ |^4)$.

Conflict Resolution:

Given user n ∈ N, her preferred privacy policyP_n, the maximum tie strength valueδ, a conflicting target userc ∈ C, the willingness of user n to accept changing her most preferred action for c is a function: $W: N \times C \longrightarrow [0,1]$

$$W(n,c) = \frac{1}{2}.\left(\frac{|\ \delta - I_n(c)\ |}{\delta + I_n(c)} + \frac{|\ \delta - S_n\ |}{\delta + S_n}\right)$$

1. I Do Not Mind (IDM) Rule

Assuming a negotiating user a ∈ N, and a conflicting target user c ∈ C, this concession can be formalized as the following fuzzy IF-THEN rule:

IF $W(a,c)$ IS high THEN concede.

Concede means that user would accept changing her initial most preferred action to reach an agreement.

2. I Understand (IU) Rule

Assuming a negotiating user a ∈ N, and a conflicting target user c ∈ C, this concession can be formalized as the following fuzzy IF-THEN rule:

$$IFW(a,c)\ \text{IS low} \wedge V_a[c] = 1 \wedge \exists b \epsilon N, W(b,c) IS\ low\ \wedge V_b[c] = 0\ THEN\ concede$$

3. No Concession (NC) Rule

For the other cases in which neither IDM nor IU applies, then the mediator estimates that a negotiating user would not concede and would prefer to stick to her preferred action for the conflicting target user. For completeness, this can be formalized as the following fuzzy IF-THEN rule assuming a negotiating user a ∈ N, and a conflicting target user c∈ C:

$$\text{IF} W(a,c)\ \text{IS low} \wedge \left(V_a[c] = 0 \vee (\nexists b \epsilon N, W(b,c) \text{IS low} \wedge V_b[c] = 0)\right) \text{THEN do not concede}$$

Input:

N = {negotiating users}

$P_{n1}, \ldots, P_{nk}$= {privacy policies}

C = {conflict}

Output:

$\vec{O}$= {action vector}

The complexity of Algorithm 2 is $O(|\ C\ | \times |\ N\ |^2)$

Φ = Failures and Success conditions.

Failures:

- Huge shared files with privacy policies can lead to more time consumption to detect and resolve the conflicts.
- Hardware failure & Software failure.

Success:

- Negotiating users share files with privacy policies to the only targeted users can access them.
- Search the required information from available in Datasets.
- User gets result very fast according to their needs.

Space Complexity:

The space complexity depends on Presentation and visualization of shared files. More the storage of files more is the space complexity.

Time Complexity:

Check No. of conflicts available in the sharing files= n
If (n>1) then retrieving of information can be time consuming.
So the time complexity of conflict detection and resolution algorithm is $O(n^3)$.

VI. ALGORITHM FOR RELEVANT FEATURE DISCOVERY

- **Conflict Detection**

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

for all $n \in N$ **do**
  for all $t \in T$ **do**
    $v_n[t] \leftarrow 0$
    for all $G \in P_n.A$ **do**
      if $\exists u \in G, u = t$ **then**
        $v_n[t] \leftarrow 1$
      end if
    end for
  end for
  for all $e \in P_n.E$ **do**
    $v_n[e] \leftarrow \neg v_n[e]$
  end for
end for
$C \leftarrow \emptyset$
for all $t \in T$ **do**
  Take $a \in N$
  for all $b \in N \setminus \{a\}$ **do**
    if $v_a[t] \neq v_b[t]$ **then**
      $C \leftarrow C \cup \{t\}$
    end if
  end for
end for

- **Conflict Resolution**

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

```
1: for all c ∈ C do
2:
3:     if ∀n ∈ N, W(n, c) is HIGH then
4:         o[c] ← modified_majority(P_{n_1}, ..., P_{n_|N|}, c)
5:         continue
6:     end if
7:
8:     if ∃a ∈ N, W(a, c) is LOW then
9:         if ∃b ∈ N, W(b, c) is LOW ∧ v_a[c] ≠ v_b[c] then
10:            o[c] ← 0
11:        else
12:            o[c] ← v_a[c]
13:        end if
14:    end if
15: end for
```

VII. SYSTEM ARCHITECTURE

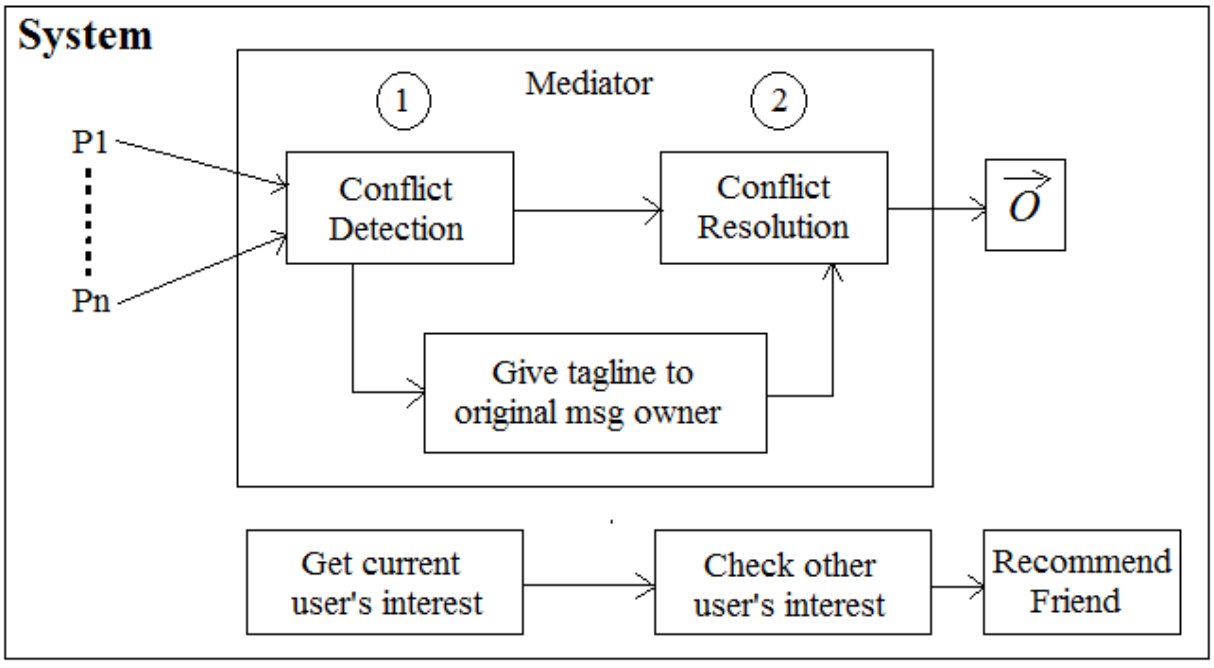

Figure 7.1 : System Architechture

Figure 7.1 shows the system architecture of the proposed system. It compares the individual privacy preferences of each negotiating user in order to detect conflicts among them. Each user is likely to have prescribed different groups of users, so privacy policies from different users may not be directly comparable. To compare privacy policies from different negotiating users for the same item, it considers the effects that each particular privacy policy has on the set of target users. Privacy policies dictate a particular action to be performed when a user tries to access the item. It assumes that the available actions are either 0 for denying access or 1 for granting access. The mediator figures the answer for every contention found by applying the concession rules through conflict resolution mechanism and the arrangement will be encoded into an activity vector. Also we recommend friends to active user based on his/her interest.

Figure 7.1 depicts an overview of the mechanism proposed:

1. The mediator investigates the individual privacy policies of all users for the item and flags all the conflicts found. Basically, it looks at whether individual privacy policies recommends contradictory access control decisions for the same target user. If conflicts are detected the item is not shared preventively.
2. The mediator proposes a solution for each conflict detected. To this aim, the mediator estimates how willing each negotiating user may be to accept by considering: her individual privacy preferences, how sensitive the particular item is for her, and the relative importance of the conflicting target users for her.
3. If all users accept the solution proposed, it will be enforced. Otherwise, users will need to turn into a manual negotiation by other means.

A. First, privacy visualization tools already proved to be highly usable for social media could be used to show and/or modify the recommended solution.

B. Second, users could define a default acknowledgement to the solutions suggested, e.g., always accept the recommended solution without asking me.

4. System recommends friends to current active user according to current user's interest.

VIII. EXPERIMENTAL SET UP AND RESULT TABLE

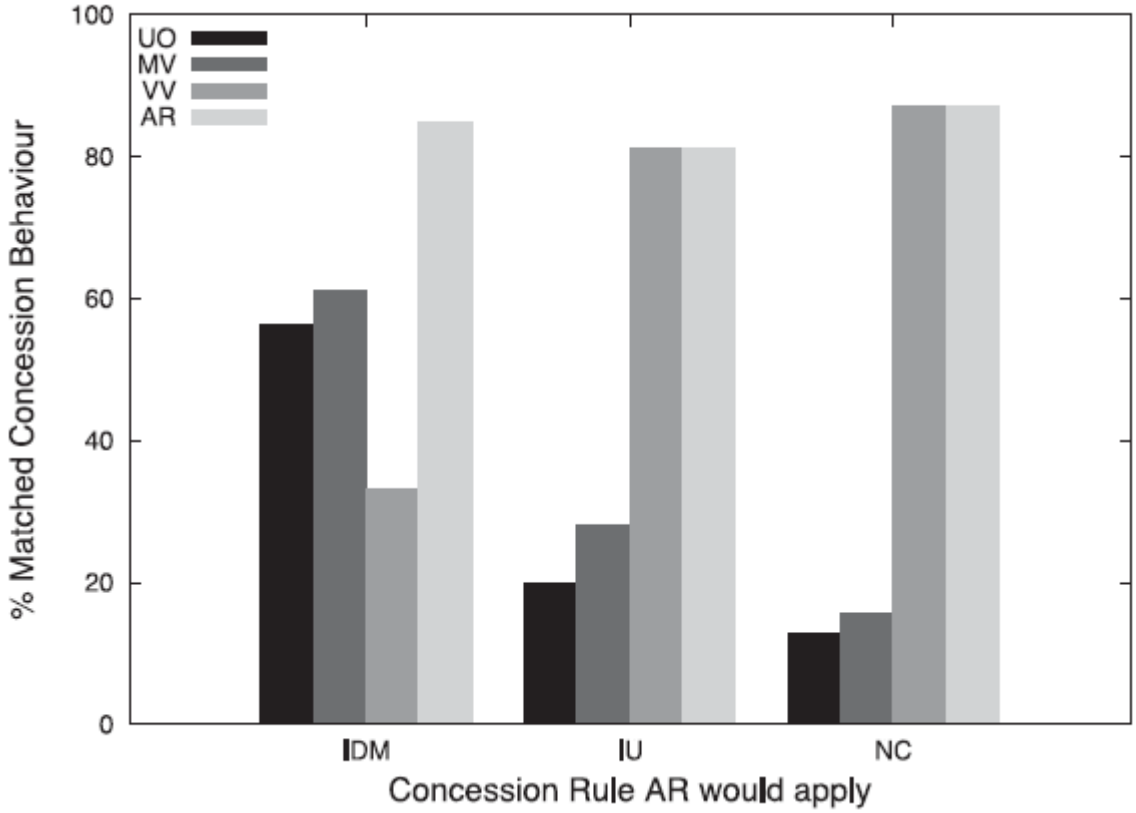

Figure 8.1: Percentage of times each approach matched concession behavior broken down by the concession rule AR would apply (IDM - I do not mind, IU - I understand, NC - No concession).

Above Figure 8.1 shows the performance of each approach broken down by the concession rule that would have been applied for each situation. We can observe that performance was similar across concession rules for our proposed mechanism AR; i.e., once a particular concession rules instantiated for a situation, it usually matched users' behavior with respect to concessions. In particular, we observe that the three concession rules in our mechanism obtain better results than the state-of-art approaches. We can also observe that the performance of state-of-the-art voting mechanisms significantly varied according to the concession rule AR would apply.

IX. CONCLUSION

We have exhibited the technique for Detecting and Resolving Privacy Conflicts in Social Media. We make an attempt to use Conflict detection and conflict resolution techniques in social media. To lessen the amount of manual user interventions to achieve a satisfactory solution for all parties involved in multi-party privacy conflicts. This project is a stepping stone towards more automated resolution of conflicts in multiparty privacy management for Social Media. Also we recommend friends to active user

based on his/her interest. As future work, the proposed system, we plan to continue researching on what makes users concede or not when solving conflicts in this domain. In particular, we are also interested in exploring if there are other factors that could also play a role in this, like for instance if concessions may be altered by previous negotiations with the same negotiating users or the relationships between negotiators themselves.

REFERENCES

[1] 1K. Thomas, C. Grier, and D. M. Nicol, "Unfriendly: Multi-party privacy risks in social networks," in Proc. 10th Int. Symp. Privacy Enhancing Technol., 2010, pp. 236–252.
[2] A. Lampinen, V. Lehtinen, A. Lehmuskallio, and S. Tamminen, "We're in it together: Interpersonal management of disclosure in social network services," in Proc. SIGCHI Conf. Human Factors Comput. Syst., 2011, pp. 3217–3226.
[3] P. Wisniewski, H. Lipford, and D. Wilson, "Fighting for my space: Coping mechanisms for SNS boundary regulation," in Proc. SIGCHI Conf. Human Factors Comput. Syst., 2012, pp. 609–618.
[4] A. Besmer and H. Richter Lipford, "Moving beyond untagging: Photo privacy in a tagged world," in Proc. SIGCHI Conf. Human Factors Comput. Syst., 2010, pp. 1563–1572.
[5] J. M. Such, A. Espinosa, and A. Garc_ıa-Fornes, "A survey of privacy in multi-agent systems," Knowl. Eng. Rev., vol. 29, no. 03, pp. 314–344, 2014.
[6] R. L. Fogues, J. M. Such, A. Espinosa, and A. Garcia-Fornes, "Open challenges in relationship-based privacy mechanisms for social network services," Int. J. Human-Comput. Interaction, vol. 31, no. 5, pp. 350–370, 2015.
[7] R. Wishart, D. Corapi, S. Marinovic, and M. Sloman, "Collaborative privacy policy authoring in a social networking context," in Proc. IEEE Int. Symp. Policies Distrib. Syst. Netw., 2010, pp. 1–8.
[8] H. Hu, G.-J. Ahn, and J. Jorgensen, "Detecting and resolving privacy conflicts for collaborative data sharing in online social networks," in Proc. 27th Annu. Comput. Security Appl. Conf., 2011, pp. 103–112. [Online]. Available: http://doi.acm.org/10.1145/2076732.2076747.
[9] 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.
[10] P. Fong, "Relationship-based access control: Protection model and policy language," in Procs. 1st ACM Conf. Data Appl. Security Privacy, 2011, pp. 191–202.
[11] B. Carminati and E. Ferrari, "Collaborative access control in onlinesocial networks," in Proc. 7th Int. Conf. Collaborative Comput.: Netw. Appl. Worksharing, 2011, pp. 231–240.
[12] L. Fang and K. LeFevre, "Privacy wizards for social networking sites," in Proc. 19th Int. World Wide Web Conf., 2010, pp. 351–360.
[13] A. C. Squicciarini, S. Sundareswaran, D. Lin, and J. Wede, "A3p: Adaptive policy prediction for shared images over popular content sharing sites," in Proc. 22nd ACM Conf. Hypertext Hypermedia, 2011, pp. 261–270.
[14] E. Gilbert and K. Karahalios, "Predicting tie strength with social media," in Proc. Conf. Human Factors Comput. Syst., 2009, pp. 211–220.
[15] A. Acquisti and R. Gross, "Imagined communities: Awareness, information sharing, and privacy on the Facebook," in Proc. 6th Int. Conf. Privacy Enhancing Technol., 2006, pp. 36–58.