IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727
PP 80-84
www.iosrjournals.org

Automated Multi Party Privacy Conflict Detection and Resolution in Social Media

Dipali Dube[1], Prof. Kurhe B. S[2].
[1,2](Computer Engineering, SPCOE/ Pune, India)

Abstract: *Multiparty privacy is major issue in social media. In today's world, the item shared through the social media may affect more than one user's privacy- e.g. photos that are uploaded, comments on the photos which mention multiple user, event in which users are invited, etc. The absence of multi-party privacy management support in current mainstream Social Media infrastructures makes users unable to properly control to who cowned items are shared. Computational mechanisms that are able to merge the privacy preferences of multiple users into a single policy for these kind of items can help solve this problem. As privacy preferences may conflict, these mechanisms need to consider how users' would actually reach an agreement in order to propose acceptable solutions to the conflicts. We propose the first computational method to solve conflicts for multiparty privacy management in Social Media that adapts to different situations that may motivate different users' concessions and agreements. We also present result of a user study in which our proposed mechanism checkmate other existing methods and models in terms of how many times each method and model user's behavior.*

Keywords: *Social Media, Privacy, Conflict, Multiparty Privacy, Social Networking Services, Online Social Network, Computational Model, Privacy preserving.*

I. Introduction

In recent years, to seen unparalleled growth in the application of online social networks (OSN). For example, Facebook , LinkedIn and twitter to illustrative social network sites, claims that it has over 600 million active users and over 40 billion parts of shared contents of all month, including web site, uniform resource locator (URL) links, news articles, stories blog posts, personal notes and photo albums. Because of the public nature of many social networks and the Internet itself, satisfied can easily be disclosed to a wider viewer than the user planned. To defend all user data, access control has become an essential feature of OSNs.

Hundreds of billions of items that are uploaded to Social Media are co-owned by multiple users [1], yet only the user that uploads the item is allowed to set its privacy setting. This is a massive and serious problem as users' privacy preferences for own items usually conflict, so applying the preferences of only that users efforts such items being shared with undesired appropriator, which can lead to privacy violations with severe consequences [2]. Examples of items include photos that depict multiple people, comments that mention different users, events in which multiple users are evaluate, etc. Multi-party privacy management is, therefore, of crucial importance for users to appropriately preserve their privacy in Social Media. There is recent evidence that users very often negotiate collaboratively to achieve an agreement on privacy settings for co-owned information in Social Media [3][4]. In particular, users are known to be generally open to modulate other users' preferences, and they are willing to make some concessions to reach an agreement depending on the specific situation [4].

Computational mechanisms that can automate the negotiation process have been identified as one of the biggest gaps in privacy management in social media [3], [4], [5], [6],[7]. The main challenge is to propose solutions that can be accepted most of the time by all the users involved in an item (e.g., all users depicted in a photo), so that users are forced to negotiate manually as little as possible, thus minimizing the burden on the user to resolve multi-party privacy conflicts.

II. Objectives

1. Individual privacy policy setting to all users.
2. Conflict Detection.
3. Conflict Resolving

III. Literature Review

3.1Secure Multiparty Computation of a Social Network's: This existing system propose a multiparty computation protocol for securely constructing an unlabeled random isomorphic version of a graph that is distributively held by a set of n parties. The proposed protocol is information theoretic secure in the malicious

adversarial model, tolerating less than n=3 corrupt parties. The proposed protocol can be used to study the behavioral situations of individuals while guaranteeing the privacy of their sensitive data. Before releasing sensitive data in public, the data is generally anonymized. The current work performs naive anonymization, on a distributively held network, without the use of a trusted third party. One can further implement multiparty computation protocols for network specific anonymization techniques.

3.2 Multi-party access control for online social networks: Model & mechanism: In this existing system, a group of users could assemble with one another so as to manipulate the final access control decision. An attack scenarios, anywhere a set of bitchy users may want to make a shared photo available to a large commune. Suppose they can access the photo, and then they all tag itself or fake their identities to the photo. In addition, they collude with each other to assign a very low sensitivity level for the photo and specify policies to grant a wider audience to access the photo with a large number of colluding users, the photo may be disclosed to those users who are not expected to gain the access. To avoid such an attack scenario from occurring, three conditions need to be satisfied: (1) there is no fake identity in OSNs; (2) all tagged users are real users appeared in the photo; and (3) all controllers of the photo are honest to specify their privacy preferences.

3.3 Resolving Multi-party Privacy Conflicts in Social Media: This existing system present the first mechanism for detecting and resolving privacy conflicts in Social Media that is based on current empirical evidence about privacy negotiations and disclosure driving factors in Social Media and is able to adapt the conflict resolution strategy based on the particular situation. In a nutshell, the broker firstly inspects the individual privacy policies of all users

Involved looking for possible conflicts. If conflicts are found, the mediator proposes a solution for each conflict according to a set of concession rules that model how users would actually negotiate in this domain. They conducted a user study comparing our mechanism to what users would do themselves in a number of situations. The results obtained suggest that our mechanism was able to match participants' connivance behavior significantly more often than other existing approaches. This has the potential to reduce the amount of manual user interventions to achieve a satisfactory solution for all parties involved in multi-party privacy conflicts.

Problem Statement

Now a day's world maintaining privacy for social media much difficult. Billions of items (photo, Comment,Sensitive data) that are upload to social media are co-owned(more than two user) by multiple users, yet only the user that uploads the item is allowed to set it's privacy settings(i.e. who can access the item). This is massive and serious problem as user's privacy preferances for co-owned item usually conflict.

IV. Proposed Work

In this paper we propose 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 different conflict resolution method based on the concessions users' may be willing to make in different situations. We also present a user study comparing our computational mechanism of conflict resolution and other previous approaches to what users would do themselves manually in a number of situations.

The results obtained suggest our proposed mechanism seriously perform better than other previously proposed approaches in terms of the number of times it matched members' behaviour in the study. We propose the conflict detection and conflict resolution resolution while algorithm for detecting and resolving the conflict which is uploading the own item.

We also purpose the user rule for privacy preference of each user, these user rules are used for conflict resolve those are:

1) **I do not mind (IDM) rule**: In this rule if any user want to upload own item in the network at that time another user no objection on that.
2) **I understand (IU) rule**: In this rule if one user want to share the photo and another one want can't share that photo at that time the user how want to share that photo they can't share that photo.
3) **No concession (NC) rule**: For the other situation in which neither I don't mind nor I understand applies, then the mediator judge that a negotiating user would not allow and would prefer to stick to her preferred action for the conflicting target user.

We also purpose the voting system for privacy preference of each user. The results combine through the web application were compared to the results that would have been obtained if our proposed mechanism was applied to the scenarios and if state-of-the-art automated voting mechanisms were applied. To this aim, we looked at the privacy policy defined by the participant and the conflict generated by the application for each

situation. This determined members most preferred action for the conflict (to be considered by our proposed mechanism and state of- the-art voting mechanisms), as well as the willingness to change it (used to determine the concession rule our mechanism would apply in each case). Those voting systems are as:

1) **Uploader overwrites** (UO): the conflict is solved selecting the action preferred by the user that uploads the item. This is the approaches currently followed by most Social Media Sites (Facebook, etc.).
2) **Majority voting** (MV): [8], the conflict is solved selecting the action most preferred by the majority of the negotiating users.
3) **Veto voting** (VV): [2], if there is one negotiating user whose most preferred action is denying access, the conflict is solved by denying access to the item.

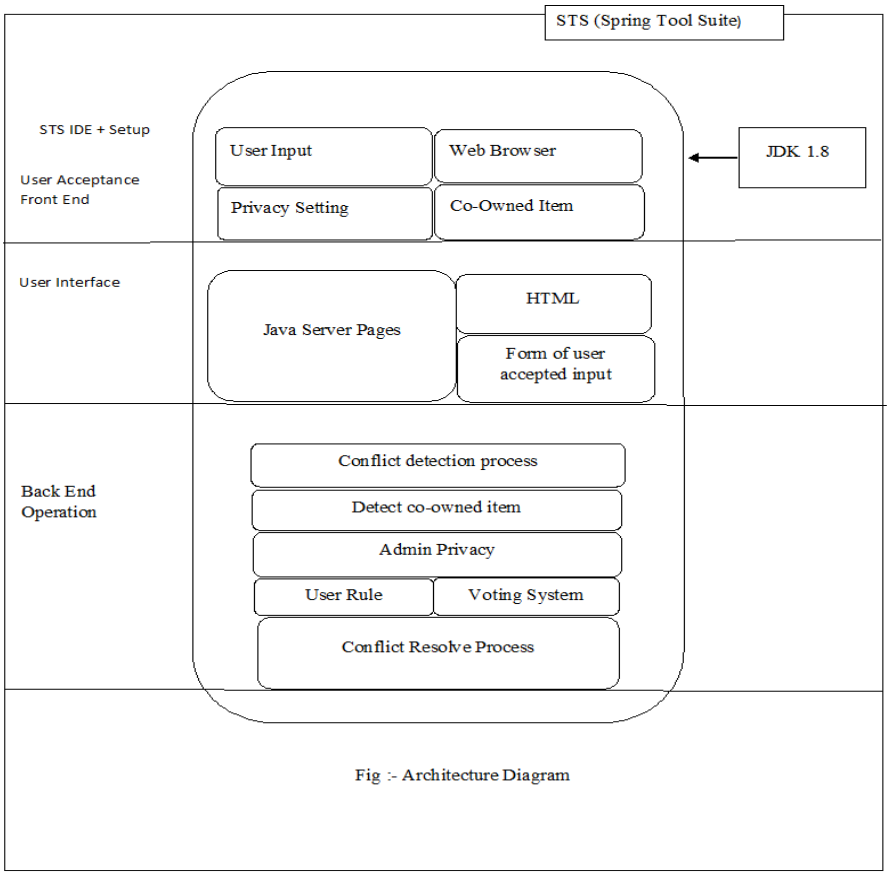

Fig :- Architecture Diagram

Algorithm

1) Conflict Detection

Following algorithm used in order to detect the conflict in multiparty user:

Input: N= Set of negotiating users
T= Set of target users
Pn =Individual privacy policy of the negotiating user
V(t)= action vector for target user t
P= (A,E)
v(t)= act(P,t)

Output: Set of conflicting users, C.

1. for all n Ɛ N do
    2: for all t Ɛ T do
    3: v_n [t] ← 0
    4: for all G Ɛ P_n.A do
    5: if ∃ u Ɛ G,u = t then
    6: v_n [t] ← 1
    7: end if

8: end for
9: end for
10: for all e Ɛ P_n.E do
11: v_n [e] ← ¬ v_n [e]
12: end for
13: end for
14: C ← φ ;
15: for all t Ɛ T do
16: Take a Ɛ N
17: for all b Ɛ N \ {a} do
18: if v_a [t] ≠ v_b [t] then
19: C ←C U {t}
20: end if
21: end for
22: end for

2) Conflict Resolved
Following algorithm used in order to resolve the conflict in multiparty user:

Input: N, Pn1,……Pn[N], C
Willingness to change decision W(n,c)

Output: O
1: **for all** c Ɛ C **do**
2: **if** n ƐN; W (n, c) is HIGH **then**
3: ⊎o[c] ← modified_majority (P_{n1} ,…,P_{n1lNl} , c)
4: **continue**
5: **end if**
6: **if** ∃a Ɛ N, W (a, c) is LOW **then**
7: **if** ∃b Ɛ N; W (b, c) is LOW ^ v_a[c] ≠ v_b[c] **then**
8: o[c] ← 0
9: **else**
10: o[c] ←v_a[c]
11: **end if**
12: **end if**
13: **end for**

Advantages
1. To maintain the privacy
2. To detect and resolve the conflict occur in the multiparty

V. Result

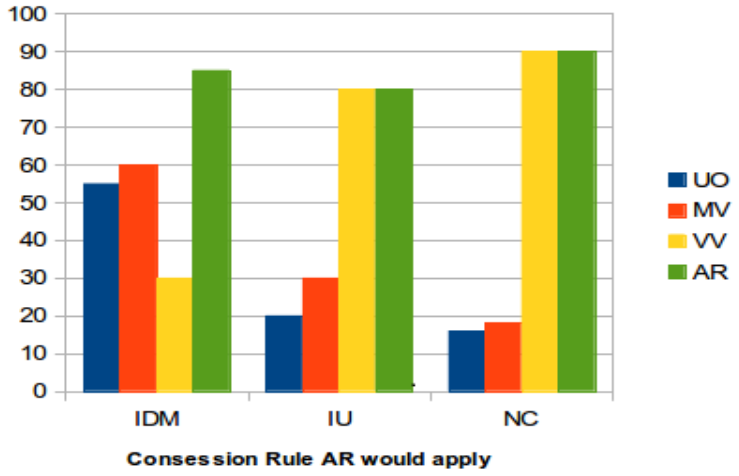

Fig:- All times conession match using rules: I don't Mind(IDM) I Understand(IU) No Conession(NC)

VI. Conclusion

This paper present the first mechanism for identify and resolving privacy conflicts in Social Media that adapt the conflict resolution strategy based on the particular situation. . The broker firstly inspects the individual privacy policies of all users involved looking for possible conflicts. If conflicts are found, the broker proposes a solution for each conflict according to a set of concession rules that model how users would actually negotiate in this domain. Also we define the admin privacy setting to take any decision related to group. We conducted a user study comparing our mechanism to what users would do itself in a number of situations. The results obtained suggest that our mechanism was able to match participant concession behavior. Siginificantly more often than other existing approaches. This has the potential to reduce the amount of manual user interventions to achieve a satisfactory solution

Acknowledgements

We express our sincere thanks to our project guide Prof. Kurhe B.S. who always being with presence & constant, constructive criticism to made this paper. We would also like to thank all the staff of COMPUTER DEPARTMENT for their valuable guidance, suggestion and support through the project work, who has given co-operation for the project with personal attention. Above all we express our deepest gratitude to all of them for their kind-hearted support which helped us a lot during project work. At the last we thankful to our friends, colleagues for the inspirational help provided to us through a project work.

References

[1] Resolving Multi-party Privacy Conflict in Social Media. Jose M. Such; Natalia Criado. IEEE transaction on knowledge and data engineering. 2016, volume:28,Issue:7, pages:1851-1863, DOI: 10.1109/TKDE.2016.2539165,Cited by :Papers(1)

[2] VarshaBhatKukkala,S.R.SIyengary and Jaspal Singh Saini," Secure Multiparty Graph Computation", 8th International Conference on Communication Systems and Networks (COMSNETS).2016

[3] Hongxin Hu, Gail-JoonAhn and Jan Jorgensen," Multiparty Access Control for Online Social Networks: Model and Mechanisms", ieee transactions on knowledge and data engineering, vol. 25, no. 7, july 2013

[4] VarshaBhatKukkala, S.R.S Iyengary and Jaspal Singh Saini," Secure Multiparty Computation of a Social Network", International Association for Cryptologic Research (IACR).2012

[5] Matthew Smith, Christian Szongott, "Big Data Privacy Issues in Public Social Media", 6th IEEE International Conference on 2012.

[6] K. Thomas, C. Grier, and D. M. Nicol, "unfriendly: Multi-party privacy risks in social networks," in Privacy Enhancing Technologies. Springer, 2010, pp. 236–252.

[7] A. Squicciarini, M. Shehab, and F. Paci, "Collective privacymanagement in social networks," in WWW. ACM, 2009, pp. 521–530.