SURVEY ON DETECTING AND RESOLVING PRIVACY CONFLICTS IN SOCIAL MEDIA

[1]Priya Chinchole, [2]Dhanashri Wagh, [3]Minal Gale, [4]Monali Kachare,[5]Satyendra Kothari
[1]Student, [2]Student, [3]Student, [4]Student, [5]Assistant Professor.
[1]Bachelor of Engineering (Information Technology).
[1]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 merge the privacy preferences of multiple users into a single policy for an item can help solve this problem. However, merging multiple users' privacy preferences is not an easy 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 propose solutions that can be acceptable by all of the users affected by the item to be shared. Current approaches are either too demanding or only consider fixed ways of aggregating privacy preferences. In this paper, we propose the first computational mechanism to resolve conflicts for multi-party privacy management in Social Media that is able to adapt to different situations by modeling 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.

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

I.INTRODUCTION

Social media sites have an extensive presence in nowadays society. User can learn a lot of useful information 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 private data of the clients in informal organizations is a genuine concern. It proposes different method to solve these privacy conflicts. As of late we have been viewing a huge increment in the development of on-line social systems. OSNs empower 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 utilization of interpersonal organization, it raises various security and protection issues. While OSNs permit clients to confine 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-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 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 different 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.REVIEW OF LITERATURE SURVEY

K. Thomas, C. Grier, and D. M. Nicol, presents "Unfriendly: Multi-party privacy risks in social networks" [1]. Authors examine how the lack of joint privacy controls over content can inadvertently reveal sensitive information about a user including preferences, relationships, conversations, and photos. Specifically, they analyze Facebook to identify scenarios where conflicting privacy settings between friends will reveal information that at least one user intended remain private. From this paper we refer adapt privacy controls and prototype solution as a Facebook application.

A. Lampinen, V. Lehtinen, A. Lehmuskallio, and S. Tamminen, proposed "We're in it together: Interpersonal management of disclosure in social network services" [2]. This paper considers SNS-users' concerns in relation to online disclosure and the ways in which they cope with these both individually and collaboratively. From this paper we refer a framework of strategies for boundary regulation that informs both theoretical work and design practice related to management of disclosure in SNSs. We also refer an effective privacy management.

P. Wisniewski, H. Lipford, and D. Wilson, presents “Fighting for my space: Coping mechanisms for SNS boundary regulation” [3]. This paper presents results from a qualitative interview-based study to identify "coping mechanisms" that users devise outside explicit boundary-regulation interface features in order to manage interpersonal boundaries. From this paper we refer filtering, ignoring, blocking, withdrawal, aggression, compliance, and compromise represent coping mechanisms individuals use within SNSs to maintain their interpersonal boundaries.

A. Besmer and H. Richter Lipford, presents “Moving beyond untagging: Photo privacy in a tagged world” [4]. Authors examine privacy concerns and mechanisms surrounding these tagged images. Using a focus group, they explored the needs and concerns of users, resulting in a set of design considerations for tagged photo privacy. Then designed a privacy enhancing mechanism based on our findings, and validated it using a mixed methods approach. From this paper we study how we explored the needs and concerns of users, resulting in a set of design considerations for tagged photo privacy.

J. M. Such, A. Espinosa, and A. Garc_ıa-Fornes, proposed “A survey of privacy in multi-agent systems” [5]. In this paper, authors 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. From this paper we study Disclosure Decision Making based on Multiple Criteria, Learning the privacy sensitivity of personal information, Integration of trust, reputation, and norms for protecting against information dissemination, Protection against information collection and dissemination.

R. L. Fogues, J. M. Such, A. Espinosa, and A. Garcia-Fornes, proposed “Open challenges in relationship-based privacy mechanisms for social network services” [6]. This paper presents a list of privacy threats that can affect SNS users, and what requirements privacy mechanisms should fulfill to prevent these threats. Visualization tools should explain to the users in an understandable way how their information is disseminated according to a specific type of relationship.

R. Wishart, D. Corapi, S. Marinovic, and M. Sloman, proposed “Collaborative privacy policy authoring in a social networking context” [7]. In this paper, propose a privacy-aware social networking service and then introduce a collaborative approach to authoring privacy policies for the service. The approach permits the originators of content on the social network to specify policies for the content they upload. From this paper we refer an effective and flexible mechanism to support privacy control of shared data in OSNs.

H. Hu, G.-J. Ahn, and J. Jorgensen, presents “Detecting and resolving privacy conflicts for collaborative data sharing in online social networks” [8]. In this paper, author proposes an approach to enable collaborative privacy management of shared data in OSNs. They provide a systematic mechanism to identify and resolve privacy conflicts for collaborative data sharing.From this paper we study an effective and flexible mechanism to support privacy control of shared data in OSNs.

H. Hu, G. Ahn, and J. Jorgensen, presents “Multiparty access control for online social networks: Model and mechanisms” [9]. In paper authors propose an approach to enable the protection of shared data associated with multiple users in OSNs. They formulate an access control model to capture the essence of multiparty authorization requirements, along with a multiparty policy specification scheme and a policy enforcement mechanism. Besides, they present a logical representation of our access control model that allows us to leverage the features of existing logic solvers to perform various analysis tasks on our model. From this paper we study multiparty policy specification scheme and corresponding policy evaluation mechanism.

P. Fong, proposed “Relationship-based access control: Protection model and policy language” [10]. Social Network Systems pioneer a paradigm of access control that is distinct from traditional approaches to access control. Gates coined the term Relationship-Based Access Control (ReBAC) to refer to this paradigm. Authors formulate an archetypical 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 accessor in a social network maintained by the protection system. From this paper we study 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.

2.1. : Table of Literature Survey.

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 Int. Symp. Privacy Enhancing Technol., 2010, pp. 236–252.	1.Privacy must extend beyond single-owner model - Tags, links, mentions can reference multiple users - Rely on these existing features to	1.In absence of mutual friends, safe set of viewers tends towards empty set 2.Assume friends will consent to not sharing with wider audience	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 2.Prototype solution as a Facebook application

		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	3.Content must be tagged; no other way to distinguish privacy-affected parties 4.Censorship; prevents negative speech	- 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 privacy.	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 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		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.

		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		
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	. 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 in a social networking context,” in Proc. IEEE Int. Symp. Policies Distrib. Syst. Netw., 2010, pp. 1–8.	1. The collaborative policy authoring process more user-friendly and accessible to average users of social networks.	1.The scope of the policy can only be decreased by the nominated parties. 2.The inability of a user to claim co-ownership of a resource. 3.Provides limited help with authoring policies.	1.In this paper, propose a privacy-aware social networking service and then introduce a collaborative approach to authoring privacy policies for the service. 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	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.

	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.	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.

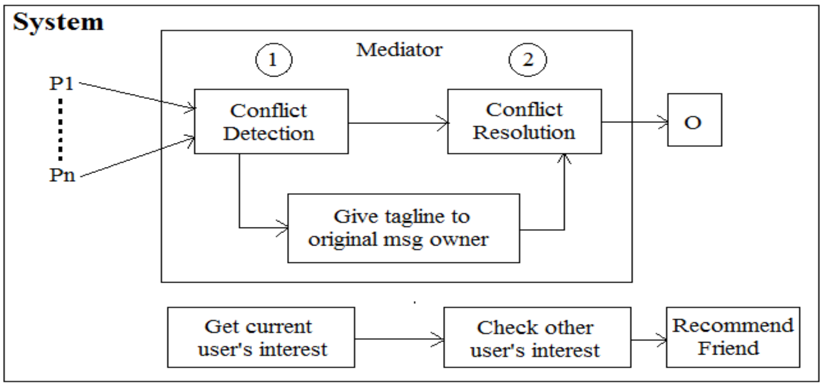
III.EXISTING SYSTEM APPROACH

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.

DISADVANTAGES OF EXISTING SYSTEM

1. Given the set of individual privacy policies Pn1 , . . . , Pnk 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.

IV.SYSTEM ARCHITECTURE


System
Mediator
1
2
P1
Pn
Conflict Detection
Conflict Resolution
O
Give tagline to original msg owner
Get current user's interest
Check other user's interest
Recommend Friend

The proposed system, the use of a mediator that detects conflicts and suggests a possible solution to them. For instance, in most Social Media infrastructures, such as Facebook, Twitter, Google+ and the like, this mediator could be integrated as the back-end of Social Media privacy controls' interface; or it could be implemented as a Social Media application such as a Facebook app that works as an interface to the privacy controls of the underlying Social Media infrastructure. Above architecture depicts an overview of the mechanism proposed:

1. The mediator inspects the individual privacy policies of all users for the item and flags all the conflicts found. Basically, it looks at whether individual privacy policies suggest contradictory access control decisions for the same target user. If conflicts are found the item is not shared preventively.
2. The mediator proposes a solution for each conflict found. To this aim, the mediator estimates how willing each negotiating user may be to concede 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 applied. 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 suggested solution.

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

4. System recommends friends to current active user according to current users interest.

V.CONCLUSION

In this paper, 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 reduce the amount of manual user interventions to achieve a satisfactory solution for all parties involved in multi-party privacy conflicts. In this paper 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 influenced by previous negotiations with the same negotiating users or the relationships between negotiators themselves.

VI.FUTURE SCOPE

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 influenced by previous negotiations with the same negotiating users or the relationships between negotiators themselves.

VI.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.