SECURED ULTIMATE MULTI-PARTY CONFLICT RESOLUTION IN SOCIAL MEDIA

K.Abinaya, Mrs.N.Kousika
PG Scholar, Assistant Professor
Dept of Computer Science and Engineering,
Sri Krishna College of Engineering and Technology,
abiaparna94@gmail.com, kousika@skcet.ac.in.

Abstract

Facebook is an online social networking service that enables millions of users to share their views and photos. Items shared through Social Media might have an effect on additional than one user's privacy. Eg .Photos that portray multiple users, comments that mention multiple users etc. The absence of multi-gathering security bolster in current standard online networking makes clients not able to properly control to whom these things are really shared. To resolve this problem, various computational mechanisms are used which helps in merging the privacy preferences of multiple users into a single policy. However, merging multiple users' privacy preferences is not an easy task, so methods to resolve privacy conflicts are needed. This project proposes the first computational mechanism to resolve conflicts for multi-party privacy management in social media that is able to adapt to different situations by modelling the confessions that users make to reach a solution to the conflicts.

***Index Terms*—Web mining, Sentiment classification, Facebook. Social Media, Privacy, Conflicts, Multi-party Privacy, Social Networking Services, Online Social Networks**

I. INTRODUCTION

Data Mining is a process of mining information, knowledge from a data set and transforming it into an understandable structure for further use. Web mining is the application of data mining techniques to mechanically discover and extract knowledge from internet data, as well as internet documents, hyperlinks between documents, usage logs of internet sites, etc.

Web could be an assortment of billions of documents. Which is extremely monumental, diverse, flexible, and dynamic. The Web (WWW) continues to grow within the immense volume of traffic, size and complexness of Websites. Therefore it is difficult to identify relevant information present in the web. Most of the contents here are unstructured in nature, but there are less works which focus on unstructured and heterogeneous information.

The rising field of internet mining aims at finding and extracting relevant information hidden in Web, specifically text documents printed on the net. Web mining mines relevant data from numerous websites.

There are 3 general categories of knowledge which will be discovered by Web mining

•Web activity, from server logs and applications programme activity following.

•Web graph, from links between pages, folks and different information.

•Web content, for the information found on websites.Web Mining can be broadly divided into three distinct categories as shown in Figure.1.1.

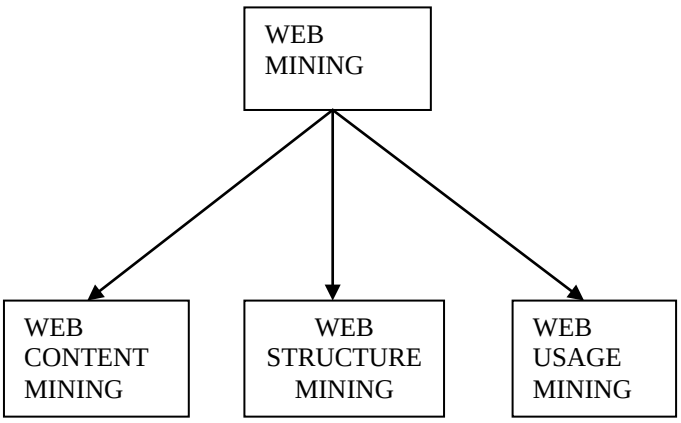

Fig. 1. Web Mining Taxonomy

Web Content Mining aims in extracting useful information from the contents of Web documents. Content data corresponds to collection of facts a Web page contained for users. It may consist of text, images, audio, video, or structured records such as lists and tables. Web content mining deals with majority of texts and audio, video etc. It helps in clustering and categorization of web page information based on titles, specific contents and images available. Problems addressed in text mining are topic discovery, cluster of net documents and classification of websites and extracting association patterns.

Web Structure Mining is a tool used to establish relationship between web pages coupled by its contents. The structure of a typical internet graph consists of web pages as nodes, and hyperlinks as edges connecting connected pages as shown in Fig .1.2. Web Structure Mining is that the method of discovering structure information from the net. In business world, Structure Mining is quite helpful in deciding the association between 2 or a lot of business websites.

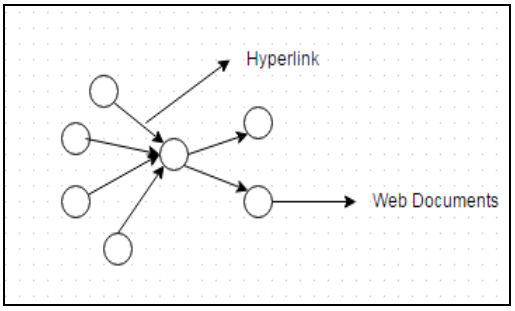

Fig.1.2. Web Graph Structure

Web Usage Mining a kind of net mining used to discover fascinating usage patterns from net information, so as to grasp and higher serve the requirements of Web-based applications. It provides the path resulting in accessed websites. Usage information captures the identity or origin of net users in conjunction with their browsing behaviour at web site.

II. RELATED WORK

H. Hu, G.-J. Ahn et al. [1], Proposed that social network like Facebook, twitter helps in expressing peoples opinion. To analyze the strategic behavior of rational controllers in multiparty access control, where each controller aims to maximize her/his own benefit by adjusting her/his privacy setting in collaborative data sharing in Online Social Networks.

Wishart et al. [2] first proposed a privacy-aware social networking service and then introduced a collaborative approach to authoring privacy policies for the service. In addressing user privacy, this approach takes into account the needs of all parties affected by the disclosure of information and digital content..

B. Carminati et al. [3], proposed Topology-based access control can be enhanced by exploiting the collaboration among OSN users, which is the essence of any OSN. The need of user collaboration during access control enforcement arises by the fact that, different from traditional settings, in most OSN services users can reference other users in resources (e.g., a user can be tagged to a photo), and therefore it is generally not possible for a user to control the resources published by another user.

Hu et al. [4] proposed an approach to enable the protection of shared data associated with multiple users in OSNs. They formulated an access control model to capture the essence of multiparty

authorization requirements, along with a multiparty policy specification scheme and a policy enforcement mechanism.

M. Sleeper et al. [5] explored users self-censorship decisions on Facebook, as well as the types of content they choose to self-censor. While self-censorship can be a desirable behavior both on and offline, users sometimes choose to self-censor on SNSs because available access-control tools don't meet their needs. For a subset of self-censored content, users choose not to share because they would like only specific audiences to see the content, and those audiences are difficult or impossible, to target given current interface design

L. Fang et al [6] proposed a template for the design of a social networking privacy wizard. The intuition for the design comes from the observation that real users set their privacy preferences (which friends should be able to see which information) based on an implicit set of rules. Thus, , it is possible to build a machine learning model that concisely describes a particular user's preferences based on a limited amount of user input, and then use this model to configure the user's privacy settings automatically. Identified that companies have identified social media as a rich mine of marketing knowledge.

Taigman Y et al [7] described an ideal face classifier which detects faces in accuracy that matches with humans. The underlying face descriptor would need to be invariant to pose, illumination, expression, and image quality. It should also be general, in the sense that it could be applied to various populations with little modifications, if any at all. In addition, short descriptors are preferable, and if possible, sparse features.

III. PROPOSED WORK

The proposed system has a user module where user will sign up with Facebook account in order to establish a connection. Connection process involves registering with it and getting keys and access tokens. With the help of which photos and comments which are posted by the user are retrieved dynamically. Conflict Detection module helps in filtering the conflict items posted or shared by the uploader. Conflict Resolution module analyses the privacy preferences of each negotiating user and the mediator suggests solution based on the sensitivity of the item shared. Based on the decision of the mediator, the willingness to change the action can be calculated and the conflict is resolved. As shown in Figure 4.1.

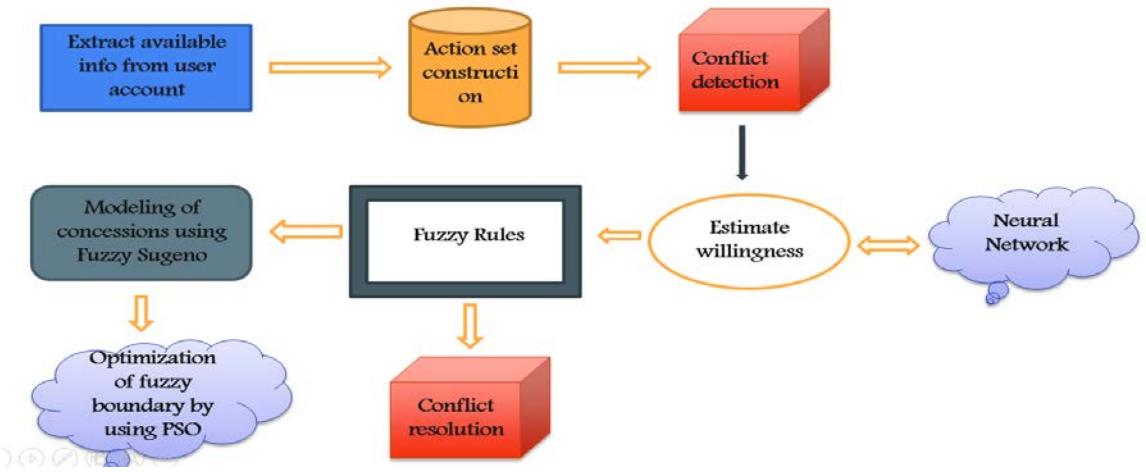

Fig. 4.1. System Architecture

The architecture explains the sequence as shown in Fig.4.2; first admin will sign up with facebook and establish a connection, by getting the keys and access tokens. After which based on the image posted by the user, conflicts will

be identified. Retrieved images will be preprocessed to remove conflicts present in it. Then preprocessed images will be analyzed by the mediator using Artificial Neural Networks. Based on the privacy preferences of the users in the posted image. There are three types of privacy namely public, my friends only and only me. During the profile setting process, users may set their privacy. The mediator decides whether the image can be further shared or not. The decision of the mediator must be acceptable by the uploader of the image. As shown in Figure.4.2.

Figure 4.2. Model Representation of System Architecture

ALGORITHM 1

CONFLICT DETECTION

Input : N, Pn1 , . . . , Pn|N| , T Output: C
1: for all n ∈ N do
2: for all t ∈ T do
3: vn[t] ← 0
4: for all G ∈ Pn.A do
5: if ∃u ∈ G, u = t then
6: vn[t] ← 1
7: end if
8: end for
9: end for
10: for all e ∈ Pn.E do
11: vn[e] ← ¬vn[e]
12: end for
13: end for
14: C ← ∅
15: for all t ∈ T do
16: Take a ∈ N
17: for all b ∈ N \ {a} do
18: if va[t] 6= vb[t] then
19: C ← C ∪ {t}
20: end if
21: end for
22: end for

ALGORITHM 2

CONFLICT RESOLUTION

Input: N, Pn_1 ; : : : ; Pn_{jNj} , C
Output: ~o
1: **for all** c 2 C **do**
2:
3: **if** 8n 2 N; W(n; c) is HIGH **then**
4: o[c] modified majority(P_{n1} ; : : : ; P_{njNj} ; c)
5: **continue** –
6: **end if**
7:
8: **if** 9a 2 N; W(a; c) is LOW **then**
9: **if** 9b 2 N; W(b; c) is LOW ^ v_a[c] 6= 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**

IMAGE EXTRACTION

Admin has to sign up with Facebook inorder to establish a connection. Connection establishment involves registering with Facebook and getting consumer keys and access tokens, which is to be embedded in the program and executed inorder to retrieve all the images with conflicts.

PREPROCESSING

Retrieved images will be preprocessed, in order to filter out the conflict images such as photos which involve multiple persons, comments that mention multiple users. This phase also retrieves the personnel and group information of the uploader. This is given as input to the conflict resolution phase.

CONFLICT DETECTION

The preprocessed images of conflict users will be analyzed by checking the privacy preferences of each user involved in the photo. Based on the privacy preferences, the conflict users are grouped separately.

CONFLICT RESOLUTION

The conflict detection result will be taken and the conflict is resolved by using the optimization algorithm. The mediator is responsible for resolving the conflict and the willingness to change the action of the uploader is done using a machine learning approach called neural network.

PRINCIPLE 1: An image should not be shared if it causes harm to one of the co-owners involved
PRINCIPLE 2: If an image doesn't cause harm to any of the co-owners involved and there is any user for whom sharing is important, the item can be shared.
PRINCIPLE 3: For the rest of cases, the solution should be consistent with the majority of all users' individual preferences.

MODELLING CONCESSIONS

As suggested by existing research [3], [4], [5], negotiations about privacy in social media are collaborative most of the time. That is, users would consider others' preferences when deciding to whom they share, so users may be willing to concede and change their initial mostpreferred option. Being able to model the situations in which these concessions happen is of crucial importance to propose the best solution to the conflicts found — one that would be acceptable by all the users involved. To this aim, the mediator models users' decision-making processes during negotiations based on the willingness to change an action (defined above) as well as on findings about manual negotiations in this domain, like the ones described in [3], [4], [5]. Users' decision making on continuous variables, like the willingness to change an action, is commonly modelled using fuzzy sets that characterize intervals of the continuous variables [32]. Figure 2 depicts the intervals the mediator considers for the willingness to change an action, which can be low or high8 . Based on this, the following fuzzy IF-THEN rules to model concessions in different situations as described below according to the three principles stated above.

I DO NOT MIND (IDM) RULE

Users are generally willing to accommodate others' sharing preferences [3], [4], so if they do not mind much about which action is finally applied, they will concede and accept applying the action that is not the most preferred for them. In particular, if the willingness to accept the action that is not the preferred one is high, then this may mean that the user would not mind much conceding and accepting that action for the conflicting target user.

IV.EXPERIMENTAL RESULTS

We compared the results that would have been obtained applying our proposed mechanism to those that would have been obtained applying the general voting mecha-nisms used in state-of-the-art automated approaches:

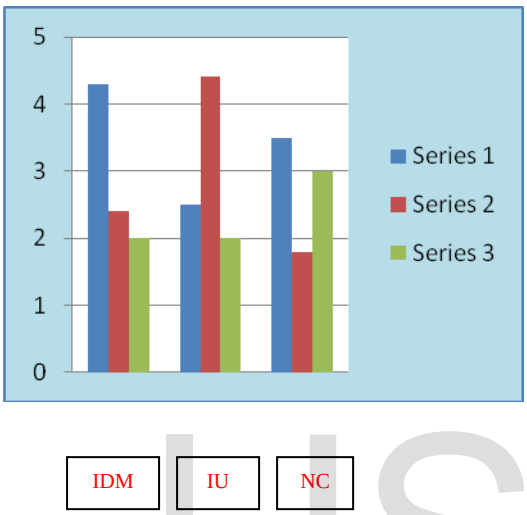

Figure.4.3. Percentage of times each approach matched con-cession behaviour broken down by the concession rule AR would apply (IDM - I do not mind, IU - I understand, NC - No concession)

Uploader overwrites (UO), the conflict is solved se-lecting the action preferred by the user that uploads the item. This is the strategy currently followed by most Social Media Sites (Facebook, etc.).

Majority voting (MV) [11], the conflict is solved selecting the action most preferred by the majority of the negotiating users.

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.

Concession Rule	Instantiations
I do not mind (IDM)	172
I understand (IU)	111
No concession (NC)	217
Total	500

Table. 5..Number of times concession rule have been applied

V.CONCLUSION

In this system connection with facebook has been established and conflict images are retrieved with the help of keys and access tokens provided by facebook. And retrieved images have been taken and pre-processing is done to remove the conflicts present in it. In this system, a mediator is developed to resolve the conflicts of the co-owners who co-own the item. The mediator decides whether the item can be shared or not. Based on the decision of mediator, the uploader shares the item when there is no conflict users or do not share when conflict users arise. This eliminates the security issues of many users who are involved in the photo.

VI. REFERENCES

[1] H. Hu, G.-J. Ahn, Z. Zhao, and D. Yang, “Game theoretic analysis of multiparty access control in online social networks”, WISDOM ’12, August 12 2012, ACM.

[2] R. Wishart, D. Corapi, S. Marinovic, and M. Sloman “Collaborative privacy policy authoring in a social networking context”, 2011.

[3] B. Carminati and E. Ferrari. “Collaborative access control in online social networks”, International Journal of Scientific and Research Publications, Volume 5, Issue 6, June 2015.

[4] H. Hu, G. Ahn, and J. Jorgensen,"Multiparty access control for online social networks: model and mechanisms" IEEE International Conference on Data Mining Workshops 2011.

[5] M. Sleeper, R. Balebako, S. Das, A. L. McConahy, J. Wiese, and L. F. Cranor, "The post that wasn't: exploring self-censorship on facebook", ACM 2011.

[6] L. Fang and K. LeFevre, "Privacy wizards for social networking sites", IJCSN International Journal of Computer Science and Network, Volume 4, Issue 4, August 2015.

[7] Y. Taigman, M. Yang, M. Ranzato, and L. Wolf, "Deep face: Closing the gap to human-level performance in face verification", 2014.

[8] H. R. Lipford, A. Besmer, and J. Watson, "Understanding privacy settings in facebook with an audience view," in UPSEC. USENIX, 2008, pp. 1–8.

[9] A. Mazzia, K. LeFevre, and E. Adar, "The pviz comprehension tool for social network privacy settings," in Proceedings of the Eighth Symposium on Usable Privacy and Security. ACM, 2012.

[10] R. W. Reeder, L. Bauer, L. F. Cranor, M. K. Reiter, K. Bacon, K. How, and H. Strong, "Expandable grids for visualizing and au-thoring computer security policies," in Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. ACM, 2008.

[11] E. Toch, N. M. Sadeh, and J. Hong, "Generating default privacy policies for online social networks," in CHI'10 Extended Abstracts on Human Factors in Computing Systems. ACM, 2010, pp. 4243– 4248.

[12] J. Watson, H. R. Lipford, and A. Besmer, "Mapping user prefer-ence to privacy default settings," ACM Transactions on Computer-Human Interaction (TOCHI), vol. 22, no. 6, p. 32, 2015.

[13] R. Hirschprung, E. Toch, and O. Maimon, "Simplifying data disclosure configurations in a cloud computing environment," ACM Transactions on Intelligent Systems and Technology (TIST), vol. 6, no. 3, p. 32, 2015.

[14] C. Sierra and J. Debenham, "The LOGIC negotiation model," in AAMAS '07: Proceedings of the 6th international joint conference on Autonomous agents and multiagent systems. ACM, 2007, pp. 1–8.

[15] Y. Taigman, M. Yang, M. Ranzato, and L. Wolf, "Deepface: Closing the gap to human-level performance in face verification," in Computer Vision and Pattern Recognition (CVPR), 2014 IEEE Conference on. IEEE, 2014, pp. 1701–1708.