Avoiding Malicious Behavior In Social Media By Conflict Detection Algorithm

Aarthi R
Student, B.E. ComputerScience and Engineering
Anand Institute of Higher Technology, Chennai, India
aarthiaadi94@gmail.com

Harinee V S
Student, B.E. ComputerScience and Engineering
Anand Institute of Higher Technology, Chennai, India
harinee0696@gmail.com

Stella Maduram S
Assistant Professor M.E, Anand Institute of Higher Technology, Chennai, India
stellasarkunam@gmail.com

***Abstract*— "Social Media are web-based communication tools to interact with each other by both sharing and consuming information. It includes popular networking websites like Facebook and Twitter; as well as bookmarking sites like Reddit. Facebook is a popular free networking that allow registered users to create profile, upload photos and videos and also send messages. Multiple user's privacy affected when files/images/videos are shared in Social Media-e.g., photos that depict multiple users, comments that mention multiple users, events in which multiple users are invited, etc. The lack of multi-party privacy management makes users unable to control to whom these files are actually shared. Merging multiple user's privacy may occur conflict. To resolve these conflicts for multi-party management, we propose computational mechanism to reach a solution by Conflict Detection Algorithm".**

Keywords –Social Media, Privacy, Conflicts, Multi-party Privacy, Social Networking Services, Online Networks.

I. INTRODUCTION

Networking is defined as the act of making contact and exchanging information with other people, groups and institutions to develop manually beneficial relationships, or to access and share information between computers. Many items that are uploaded to Social Media are co-owned by multiple users, yet not only the user that uploads the files is allowed to set its privacy settings. Multi-party privacy management is, therefore, of crucial importance for users to preserve their privacy in Social Media. Users are open to accommodate other's preferences. However, Social Media privacy controls solve this problem by applying the sharing preferences of the party that uploads the item, so users are forced to negotiate manually. In this paper, we present the first computational mechanism for Social Media that, given the individual privacy preferences of each user and also find and resolve conflicts by applying Conflict Detection method. Conflict Detection is one which provides for all the things that shared in Social Network.

RELATED WORK

A. Background

Implementing Conflict Detection for setting individual user's privacy.

II. EXISTING WORK

Operators of online social networks are increasingly sharing potentially sensitive information about users and their relationships with advertisers, application developers, and data-mining researchers. Privacy is typically protected by anonymization. They present a framework for analyzing privacy and anonymity in social networks and develop re-identification algorithm. [7].Agents usually encapsulate their principles personal data attributes, which can be disclosed to other agents during agent interactions, producing a potential loss of privacy. The sharing or public release of anonymized data without accidentally leaking personally identifiable information(PII).The anonymizing node identifies may not be sufficient to keep the network private[6].The concept deals with interaction rather than privacy of the images. The files shared in social media may not be secured due to lack of individual privacy preference. In this concept Interaction Algorithm was proposed.

The interaction is "What the system does". The interaction is implemented as Roles which are played by objects at runtime. The objects combine the states and methods of data (domain) objects with methods (but to state, as Roles are stateless) from one or more Roles. In good DCI style, a Role addresses neither object only in terms of its Role.

A. *Problem and shortcomings*

- Privacy of each items that shared in Social Media may not be secured.
- Unauthorized photos and items can be shared easily to their timelines.

III. OVERALL SYSTEM ARCHITECTURE

Facebook is mainly used for sharing the information among people. To connect with server user must give their username and password then only they can able to connect the server. If the user already exits directly can login into the server else user must register their details such as username, password and Email id, into the server. Server will create the account for the entire user to maintain upload and download rate. The user are able to post a image on their timeline and he/she is able to post a comment for the pictures posted on the time line. Once the user give the request the image will be viewed in an encrypted format. If the user responds to that request with a private key, then the image will be in a viewed

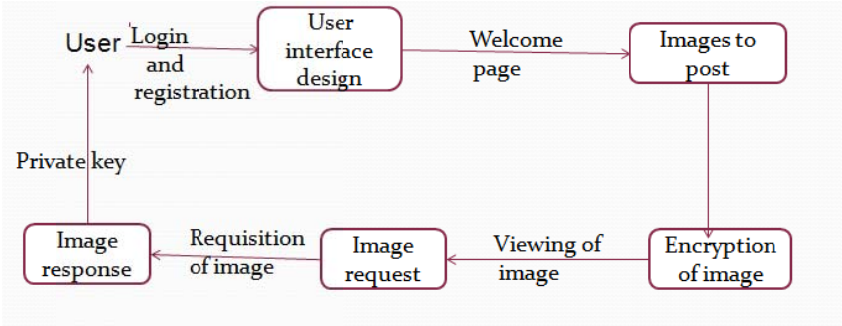

Figure 1: System Architecture

IV. PROPOSED SYSTEM

Our proposed mechanism outperformed other existing approaches in terms of how many times each approach matched user behavior. It need too much human intervention during the conflict resolution process, by requiring users to solve the conflict manually or close to manually; e.g., participating in difficult-to comprehend auction for each and every co-owned item.

A. Conflict Detection Algorithm

The individual assurance slants of every masterminding customer with a particular deciding objective to recognize conflicts among them. Nevertheless, every customer is obligated to have described unmistakable social affairs of customers, so security courses of action from different customers may not be particularly for all intents and purposes indistinguishable.

B. Modular Description

a) *User Interface Design.*

To connect with server user must give their username and password then only they can able to connect the server. If the user already exits directly can login into the server else user must register their details such as username, password and Email id into the server. Server will create the account for the entire user to maintain upload and download rate. Name will be set as user id. Logging in is usually used to enter a specific page.

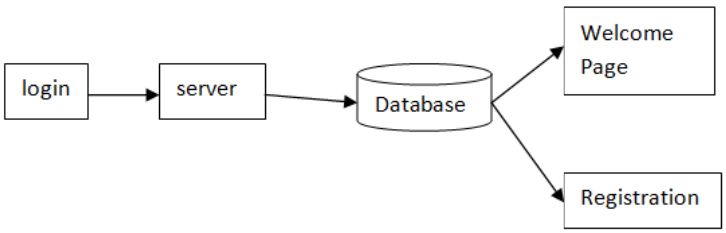

Figure 2:User Interface Design

b) *Posting Image*

In this module, the user are able to post a image on their timeline and he/she is able to post a comment for the pictures posted on the time line.

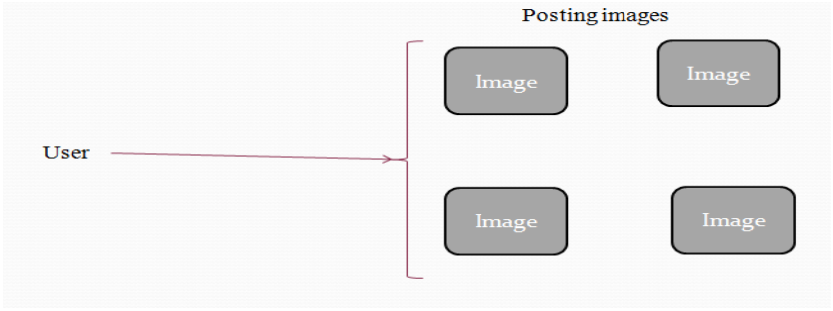

Figure 3: User Posting Images

c) *Image Encryption*

In this module, the image uploaded by the user can only view the image other users such as friends and other persons are not able to view the image as the image has been already decrypted itself thus providing security for the users.

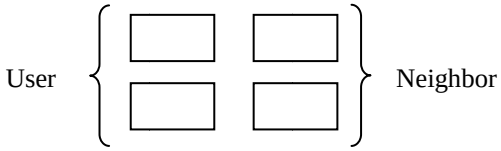

Figure 4: Encryption of image

d) *Image Request*

In this module, as user is unable to view the neighbor's pictures that have been shared by the person on their timeline. So the neighbor user can able to send a request to the owner of the image.

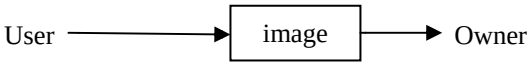

Figure 5: Requisition of image

e) *Image Response*

In this module, the users who need the image that has request in the request box of the owner if he/she accept the request then the neighbor is able to view the image.

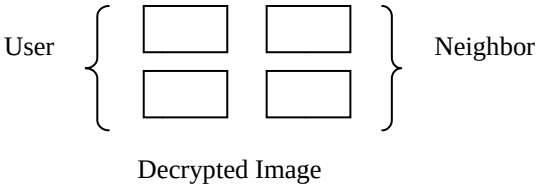

Figure 6 : Response of image

V. CONCLUSION

In this paper, we display the main system for identifying furthermore, determining protection clashes in social media that depends on current exact proof about security arrangements furthermore, divulgence driving variables in social media furthermore, can adjust the contention determination technique based on the specific circumstance. Basically, we go between firstly reviews for the individuals of protection approaches of all clients included searching for conceivable clashes. On the off chance that contentions are found, the middle person propose an answer for every contention as indicated by an arrangement of concession decides that model how clients would really arrange in this area.

VI. FUTURE ENHANCEMENT

As of not long ago, not very many scientists considered the issue of determining clashes in multiparty protection administration for social media. Wishart etal. [9] proposed a strategy to characterize protection approaches cooperatively. In their methodology the majority of the gatherings included can characterize solid and feeble protection inclination. In any case, this methodology don not include any robotized strategy to explain clashes , as it were a few proposals that the clients might need to consider when they attempt to settle the contentions physically.

REFERENCES

[1] 09/2014, Internet.org, "A focus on efficiency," http://internet.org/efficiencypaper, Retr.
[2] 2010, K. Thomas, C. Grier, and D. M. Nicol, "unfriendly: Multi-party privacy risks in social networks," in Privacy Enhancing Technologies. Springer, pp. 236–252.
[3] 2011, A. Lampinen, V. Lehtinen, A. Lehmuskallio, and S. Tamminen, "We're in it together: interpersonal management of disclosure in social network services," in Proc. CHI. ACM, pp. 3217– 3226.
[4] P.Wisniewski, H. Lipford, and D.Wilson, "Fighting for my space: Coping mechanisms for sns boundary regulation," in Proc. CHI.ACM, 2012, pp. 609–618.
[5] 2010, A. Besmer and H. Richter Lipford, "Moving beyond untagging: photo privacy in a tagged world," in ACM CHI , pp. 1563–1572.
[6] 26/06/2013, Facebook NewsRoom, "One billion- key metrics," http://newsroom.fb.com/download-media/4227, Retr..
[7] 2014, J. M. Such, A. Espinosa, and A. Garcia-Fornes, "A survey of privacy in multi-agent systems," The Knowledge Engineering Review, vol. 29, no. 03, pp. 314–344,.
[8] 2015, R. L. Fogues, J. M. Such, A. Espinosa, and A. Garcia-Fornes, "Open challenges in relationship-based privacy mechanisms for social network services," International Journal of Human-Computer Interaction, no. in press.
[9] 2010, R. Wishart, D. Corapi, S. Marinovic, and M. Sloman, "Collaborative privacy policy authoring in a social networking context," in POLICY. IEEE, pp. 1–8.
[10] 2009, A. Squicciarini, M. Shehab, and F. Paci, "Collective privacy management in social networks," in WWW. ACM, pp. 521–530.