A Collaborative Multi-Party Privacy Conflicts Framework used in Social Network Platform

Deepali D. Ahir[1] Sumiran Bhoyar[2] Snehal Holkar[3] Ashish Padyal[4] Shruti Ratul[5]
[1,2,3,4,5]Department of Computer Engineering
[1,2,3,4,5]Modern Educational Society's College of Engineering, Pune, India

Abstract— Photo sharing is an attractive component, which make social networking more popular. Sadly, it may leak user's security on off chance they granted to post, remark, label a photograph openly. We identify the problem and learn situation when user share photo-containing users of other than himself or herself. To ensure high security of photograph, we make a system that assure security of photograph post by every person at our system and self-determination on choice making of photograph sharing. For this, a proficient face recognition framework embedded in the system that can recognize every person in the photo. Not with standing, even more requesting security setting may restrain the photograph quality freely access to face recognition framework. The face of each individual user in photograph get extracted without destroying the image quality and facial structure of each user in image and verification of each extracted templates is done by users templates store in database . We also saw shared text post, which may sometime contain some unwanted word that is not acceptable by society. Therefore, to solve this issue we only allow the post, which contain the word that will not hurt users on social site. so for that we implement the text analysis feature that will analyze each post of different user and after verify it allow it display on social site. This media post on social site will be remain there for particular time set which user will decide.

Key words: Face Recognition, Text Analysis, Face Detection, Policies and Time Set

I. INTRODUCTION

The proposed system allow user to keep the privacy of photo by informing the other people in the photograph before posting the co-photograph. The system planned a security safeguarding Face-Recognition framework to recognize people in a co-photograph and text analyzer to analyze abused messages. At outlined a security protecting Face Recognition framework is used to differentiate user in a co-photograph. The system framework is of low expense. We expect that our proposed plan be extremely helpful in ensuring clients' security in photograph/picture sharing over online informal communities. Then again, there dependably exist exchange off in the middle of protection and utility. In our website the system, send the photograph with request to grant access to share the post to each people in photograph, nearby Face-Recognition verification and then sharing will reduce little bit performance of system.

The concept behind the system is that the user will register on the social media and user will only deal with his/her private photo set as train data used to learn training result. This result are exchange with user to form global knowledge. Then each user learn his/her data by reference of global knowledge. At last the information spread all over the user and concurrency could be reached. By learning data in parallel, efficient and private ness of data achieved at same time.

1) The owner of share post can be automatically identified.
2) System use the private photo by preserving the privacy and social context to execute the face recognition for any users.

II. LITERATURE REVIEW

In [1] photo-tagging authors examine the privacy of tag photos and mechanisms behind this tags photos in tag photo groups. We point out the needs and concerns of our users of set of design considerations behind our tagged photo policies. Then we design specific privacy policy for the tagged images on social media and validate that privacy policy this is based on our mechanism and different approaches. Our results identified the need of privacy policies on tagged images to address the social involvement of photo privacy management.

In [2] this general framework get used for constraint-based process modelling languages it support Ad-hoc and dynamic change and the transfer of instances which is done easier because of using traditional approaches.

In [5] survey authors draw from multi-agent learning work in a various areas including RL-evolutionary computation, game theory, complex system, agent modeling and robotics. This may broad view leads into two categories, the categories are with its own special issues like applying a single learner for multi-agent problems or multiple simultaneous learners. Also we discuss direct and indirect communication with learning and open issues with task evolutionary changes, decay, capacity to be changed in size or scale. At the end, we conclude with a presentation of this domain of multi-agent learning

III. PROBLEM DEFINITION

While going online on social media many of time logger post the image of different event, Event in which other people are also involved so it get directly post the image without informing them, so there may be privacy conflict of people get involve in the event .and also the logger may able to post any comments . Which may be same time abused message that can heart some people or society also.

To implement the system in which user can control on photo sharing and abused message of co-owners on Social networks. the system use private photo by keeping privacy to perform a personal Face Recognition engine for any particular user. To provide assurance of security people are get informed before posting a co-photograph. At outlined a security protecting Face Recognition framework is used to differentiate user in a co-photograph. The system framework is of low expense.

IV. PROPOSED SOLUTION

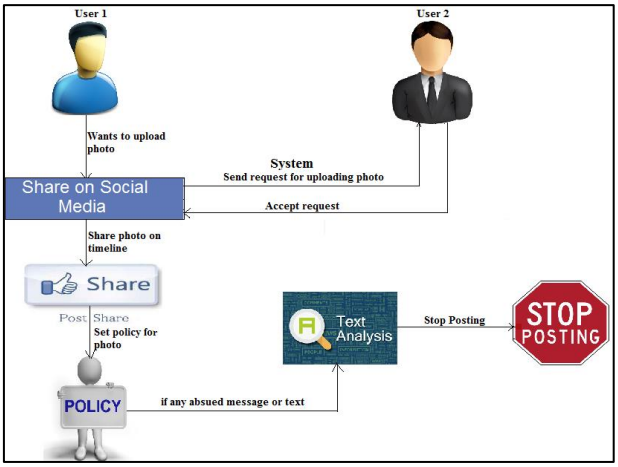

Fig. 1: System Architecture

The proposed system having four major features like

1) Providing security while uploading pictures
2) Policies
3) Time set on Timeline
4) Text Analysis

A. Providing Security While Uploading Pictures

In proposed system if user1 wants to share the photo of user 2 on timeline, then user1 have to send the request to user2 by using face detection system. If user2 accept the request from user1 then and then user1 will be able to upload the photo. If the request gets rejected then photo will does not upload on timeline. In case of user not connected then first of all friend request will send to another user. It will help to increase the security while sharing photos.

B. Policies

While uploading photo user will able to set some policies on photo. Policies are like which peoples will see their pictures on timeline. Policies having many options like only one person or selected persons otherwise all.

C. Time Set on Timeline

User also having facility to set the timestamp while sharing the photo. After timestamp picture will automatically remove from timeline.

D. Text Analysis

User having another feature like Text Analysis. If any message contains abusing word then those words are analysed by using text analysis and if that message is abused then it will does not post message or any Post on timeline.

V. CONCLUSION

This system mainly present mechanism for detect and resolve privacy conflicts in Social site. System proposed a Privacy Policy framework that assists clients with computerizing the security arrangement settings for their transferred images. The system provides a comprehensive structure to infer protection inclinations taking into account the information access for a given user. And additionally viably handled the issue of utilizing social setting data. Our exploratory study demonstrates that our My Privacy Policy and My Decision is a tool that offers significant improvements over current approaches to privacy.

Photograph sharing is a mostly done task in online informal organizations, Ex - Facebook, Instagram; without informing the other users in photograph. Posting uncover security of other users in a posted photograph. To provide the security, proposed system allow people in a photograph to get informed about posting before posting a co-photograph. The system planned a security safeguarding Face-Recognition framework to recognize people in a co-photograph and text analyzer to analyze abused messages. The system framework is of low expense. Examination and trials were done to show adequacy and effectiveness of the system. Expectations will be proposed plan exceptionally helpful in ensuring clients' protection in photograph/picture sharing over online informal organizations. Then again, there dependably exist exchange off in the middle of protection and utility.

VI. FUTURE SCOPE

The plan is to implement the system on individual mist as drop box and cloud. In addition, we try to implement the UID (Unique identification) based system that allow user to register on system to avoid fake identity on Social media. Also, provide the OTP based login to system to avoid the unauthorized access to system, which also include notification of post on Mobile to avoid privacy conflict.

REFERENCES

[1] Altman. Privacy regulation: Culturally universal or culturally specific? Journal of Social Issues, 33(3):6684, 1977.
[2] M. E. Newman. The structure and function of complex networks. SIAM review
[3] L. Palen. Unpacking privacy for networked world. Pages 129149-2003136. Press, 2003.
[4] B. Goethals, S. Laur, H. Lipmaa, and T. mielikinen. On private scalar product computation for privacy-preserving data mining. In Proceeding of the 7th annual International Conference in Information Security and Cryptology, pages 2412527.Springer, 2005.
[5] L. Kissner and D. Song. Privacy-preserving set operations. In Advances In Cryptology - Crypto 2005, Lncs, pages 241257. Springer, 2005.
[6] K. Choi, H. Byun and K. A. Toh. A collaborative face recognition framework on a social network platform. In Automatic Face Gesture Recognition, 2008. FG 08. 8 th IEEE International Conference on, pages 16, 2008.

