International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 07
June 2019

Security and Resolution Control of Image Upload on Online Social Networks

[1]B Kiran Babu, [2]Dr.P.Pedda Sadhu Naik

Abstract: Online Social Networks (OSNs) have experienced tremendous growth in recent years and become a de facto portal for hundreds of millions of Internet users. With the development of social media technologies, sharing photos in online social networks has now become a popular way for users to maintain social connections with others information contained in a photo makes it easier for a malicious viewer to infer sensitive information about those who appear in the photo. Many social networking sites is featured with photo sharing which assists users in posting photo to their families, friends and close ones. It ensures the safe upload of the photo and makes every individual present in the photo be aware of the posting activity and as well make them actively take part in the activity of photo posting. We propose the design, implementation and evaluation of HideMe, a framework to preserve the associated users' privacy for online photo sharing. HideMe acts as a plug-in to existing photo sharing OSNs. We also design a distance-based algorithm to identify and protect the privacy of bystanders. Moreover, HideMe not only protects users' privacy but also reduces the system overhead by a carefully designed face matching algorithm. The photograph will be posted if all the individuals within the friend circle are accepting the notification and it will not be posted if any of them rejects the notification. We expect that this proposed system would be very useful in protecting users' confidentiality in photo/image sharing over online social networks.

Index Terms: K-Mean Clustering, Face Recognition, Privacy, Sharing, Online Social Network, Facial recognition, OSN, Security. policy specification and management.

1. INTRODUCTION

Online social networks (OSNs) such as Facebook, Google+, and Twitter are inherently designed to enable people to share personal and public information and make social connections with friends, co-workers, colleagues, family and even with strangers. In recent years, we have seen unprecedented growth in the application of OSN's [1]. A user can specify, usually based on his relationships with others, which users are allowed to access the photo he shares. It should be noted that the photo shared by a user may relate to other users [2]. The client transferring the picture is absolutely unconscious of the outcomes that emerge for the individual which is included in labeling or picture. Right now no one can stop such unavoidable circumstance [3]. . In the past there was a buzz regarding the privacy settings of Facebook as it was very complicated but later they have simplified it for better understanding and easy access to common people [4]. We develop a scenario-based photo sharing framework called HideMe, for privacy-aware users. HideMe preserves users' privacy with a scenario-based access control, where the scenario is defined based on various contexts related to temporal, spatial, and sharing behavior factors [5]. To prevent possible confidentiality outflow of a photograph, our designed mechanism allow each personality in a photograph be aware of the uploading photograph activity and take part in the decision making on the photograph posting [6],

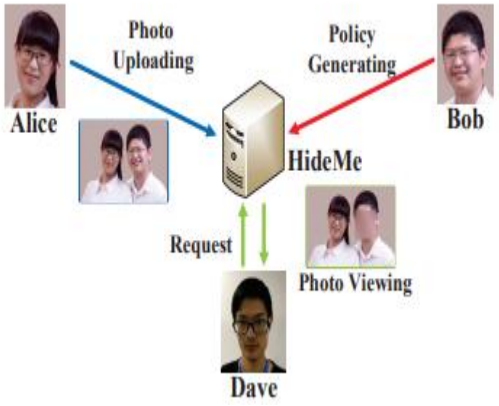

Fig. 1. Use case of HideMe

2. RELATED WORK

Photograph sharing is doubtlessly the most popular feature in online social networks. Unfortunately, casual photograph posting may reveal privacy of persons in a posted photograph. In this section first papers discuss various security issues and the available prevention methods related to group photo uploading [8]. There are also some work which focuses on the privacy of the metadata and facial feature in photo sharing and they are easily integrated into our framework these solutions to privacy conflicts are hard to be widely deployed since they require users to set privacy policy for each

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 07
June 2019

photo [9]. Through Facebook lots of data is being shared which may even be private and very sensitive so a prime concern is given to user privacy. Even it is been revealed that even the date and place of birth of a profile can be used to predict the Social Security Number (SSN) of a Facebook user and additional to that much more can be revealed through users friends list [10]. Sharing means that other users can view but not necessarily download images, and users can select different copyright options for their images [11]. It is generally believed that the sharing of the photo should be controlled by all the related users proposed a privacy-preserving photo sharing framework which uses visual obfuscation technique to protect users' privacy [12]. The trust relationship between users has been explored to deal with the access control problem. In the decentralized online social network proposed a user can tell another user with whom he trusts most to store his profile [13].

3. SYSTEM MODEL

Graph Representation of an Online Social Network Consider an online social network (OSN) which consists of N users. The network can be represented by a directed graph G represents a user. Throughout this paper unless otherwise stated, we use the two terms vertex and user interchangeably to refer to a real entity in an OSN [14]. Once the photo-uploaded uploads a photo, Hide Me extracts the metadata, processes the face information and computes the aforementioned factors in turn. Each associated friend in the photo has the right to decide whether to blur face or not setting policies for each photo may be hard and time wasting [15]. In HideMe, permissions can be acquired through scenarios, which are related to the context that a photo-viewer can obtain from a photo [16].

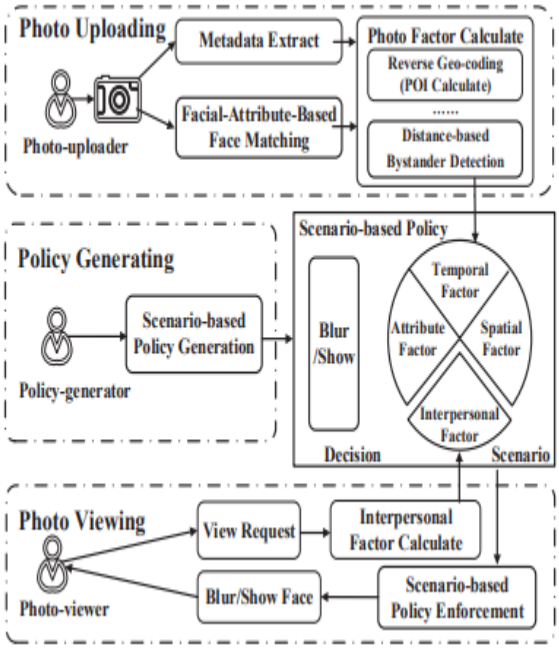

Fig. 2. Data flow of HideMe

4. PROPOSED SYSTEM

The Proposed system architecture is uses Haar cascade classifier for face detection and CBIR algorithm for image training and face recognition the advantages of Haar cascade classifier and CBIR algorithm are applied in the social networking sites for better performance [17]. Each associated friend in the photo has the right to decide whether to blur/show his/her face or not. However setting policies for each photo may be hard and time wasting. To prevent possible privacy leakage of a photo, we design a mechanism to enable each individual present in a photo be aware of the posting activity and participate in the decision making on the photo posting [18]. Homomorphism encryption would permit the tying together of various administrations without presenting the information to each of those administrations. In the proposed mechanism, we introduce a threshold θi to quantify how much user cares about other users' privacy. If user vi does not care about others' privacy then whenever user wants to share a photo d related to user with a third user [19]. We pursue a systematic solution to facilitate collaborative management of shared data in OSNs. We begin by examining how the lack of multiparty access control (MPAC) for data sharing in OSNs can undermine the protection of user data

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 07
June 2019

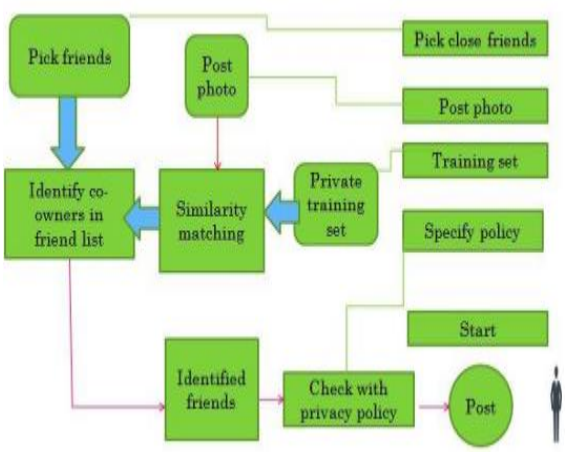

Fig.3 Proposed system architecture

Algorithm for K Means Clustering:

1. Determine the initial centroid coordinate
2. Determine the distance of each object to the centroid
3. Group the object based on minimum Euclidean distance

A. Proposed Algorithm

More over we set a time limit for the notification acceptance, the reason behind this is if co-photo owners are not login to this system for long, the one who trying to upload a photograph will be a failure, if the time limit is exceeded the photo will be uploaded automatically [20].

Purpose: Retrieving most matching images to input image.

Input: Image of a group photograph

Output: Most matching image to the input image.

Procedure:

Step 1: The input image, which containing one or more faces.

Step 2: Detecting all faces in the image.

Step 3: Create feature vector for all detected faces in the input image

Step 4: Calculate the weighted features vectors for the input image.

Step 5: Find the smallest distanced image by calculating the distance between the query image and the images in the cluster file

Step 6: The most similar image to the input image is retrieved, send acceptance notification to co -photo owners within the close circle.

B. Local Binary Pattern algorithm:

Local Binary Patterns is used for person-independent face recognition. The face area is first divided into small regions from which Local Binary Patterns (LBP), histograms are extracted and concatenated into a single feature vector [21]. This feature vector forms an efficient representation of the face and is used to measure similarities between images. Better facial feature extraction method can be applied to our system to obtain a better recognition ratio.

Input: Training Image set.

Output: Feature extracted from face image and compared with centre pixel and recognition with unknown face image.

1. Initialize temp = 0
2. FOR each image I in the training image set
3. Initialize the pattern histogram, H = 0
4. FOR each center pixel tc ϵ I
5. Compute the pattern label of tc
6. Increase the corresponding bin by 1.
7. END FOR
8. Find the highest LBP feature for each face image and combined into single vector.
9. Compare with test face image.
10. If it matches it most similar face in database then successfully recognized

The privacy policy status is set for individual users. The policy should satisfy both the privacy policy and the exposure policy of the individuals [22].

5. PERFORMANCE ANALYSIS

This section, analyse the overall performance of the proposed system by computing the performance score for each module in the system. The performance analysis graph. X coordinates includes the main modules used in the system .Y coordinates represent the time taken for each modules in X coordinates. The modules used for the performance analysis are image training, face detection, face recognition. Then plot the performance graph with time in milliseconds. The system proposed depends on the number of the train images. As the number of train images increases the recognition of the owners and co-owners photo is done more easily and quickly.

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 07
June 2019

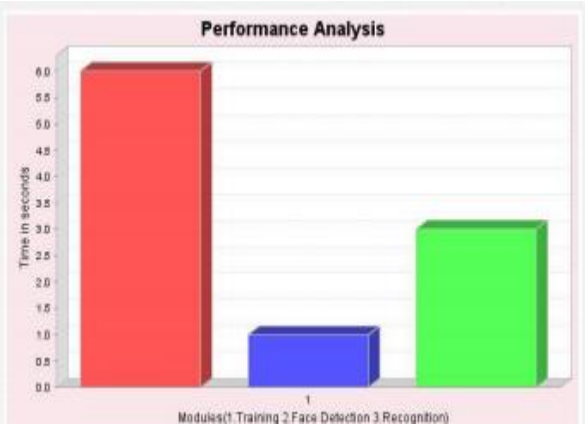

Fig.4 Performance analysis of proposed system

6. CONCLUSION

Photograph sharing is one of the most popular features in online social networks such as Facebook. Lamentably, careless photograph posting may expose security of humans in a posted photograph. We designed, implemented and evaluated a privacy-preserving photo sharing framework, called HideMe, which could help associated friends preserve their privacy in different scenarios in online photo sharing. The system can reduce the privacy leakage by using this design as it provides intimation to the co-owners and even to the owners through random OTP generation. we have introduced an approach for representing and reasoning about our proposed model. A proof-of-concept implementation of our solution called Controller has been discussed as well, followed by the usability study and system evaluation of our method. Our future work could be the way to move the proposed plans to individual mists like Dropbox and/or icloud.and the same face recognition concept can be used to prevent privacy leakage while uploading videos.

7. REFERENCES

[1] I. Altman. Privacy regulation: Culturally universal or culturally specific? Journal of Social Issues, 33(3):66–84, 1977.

[2] A. M. Kaplan and M. Haenlein, "Users of the world, unite! the challenges and opportunities of social media," Business horizons, vol. 53, no. 1, pp. 59–68, 2010.

[3] J. A. Obar and S. S. Wildman, "Social media definition and the governance challenge-an introduction to the special issue," 2015.

[4] L. Xu, C. Jiang, J. Wang, J. Yuan, and Y. Ren, "Information security in big data: Privacy and data mining," IEEE Access, vol. 2, pp. 1149–1176, 2014.

[5] S. K. N, S. K, and D. K, "On privacy and security in social media a comprehensive study," Procedia Computer Science, vol. 78, pp. 114 – 119, 2016, 1st International Conference on Information Security and Privacy 2015.

[6] C. Fiesler, M. Dye, J. L. Feuston, C. Hiruncharoenvate, C. Hutto, S. Morrison, P. Khanipour Roshan, U. Pavalanathan, A. S. Bruckman, M. De Choudhury, and E. Gilbert, "What (or who) is public?: Privacy settings and social media content sharing," in Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing, March 2017, pp. 567–580.

[7] A. C. Squicciarini, M. Shehab, and F. Paci, "Collective privacy management in social networks," in Proceedings of the 18th ACM International Conference on World Wide Web, April 2009, pp. 521–530.

[8] H. Hu, G.-J. Ahn, and J. Jorgensen, "Detecting and resolving privacy conflicts for collaborative data sharing in online social networks," in Proceedings of the 27th ACM Annual Computer Security Applications Conference, December 2011, pp. 103–112.

[9] Kerr, D.A.: The proper pivot point for panoramic photography. The Pumpkin 2(8), 1–15 (2008)

[10] Li, A., Du, W., Li, Q.: Politecamera: Respecting strangers' privacy in mobile photographing. In: Proc. of EAI SecureComm 2018

[11] Li, A., Li, Q., Gao, W.: Privacycamera: Cooperative privacy-aware photographing with mobile phones. In: Proc. of IEEE SECON 2016

[12] Li, F., Li, H., Jia, Y., Yu, N., Weng, J.: Privacy computing: concept, connotation and its research trend. Journal on Communications 37(4), 1–11 (2016)

[13] Li, F., Li, Z., Han, W., Wu, T., Chen, L., Guo, Y., Chen, J.: Cyberspaceoriented access control: A cyberspace characteristics based model and its policies. IEEE Internet of Things Journal (to appear)

[14] Li, F., Sun, Z., Niu, B., Guo, Y., Liu, Z.: Srim scheme: An impressionmanagement scheme for privacy-aware photo-sharing users. Engineering 4(1), 85–93 (2018)

[15] Olejnik, K., Dacosta, I., Machado, J.S., Huguenin, K., Khan, M.E., Hubaux, J.P.: Smarper: Context-aware and automatic runtimepermissions for mobile devices. In: Proc. of IEEE SP 2017

[16] Pallas, F., Ulbricht, M.R., Jaume-Palas´ı, L., Hoppner, U.: Offlinetags: A ¨ novel privacy approach to online photo sharing. In: Proc. of ACM CHI 2014
[17] Roesner, F., Molnar, D., Moshchuk, A., Kohno, T., Wang, H.J.: Worlddriven access control for continuous sensing. In: Proc. of ACM CCS 2014
[18] Divyalaxmi , R. Nampalli and Trupti Dange," A Survey Paper on Photo Sharing and Privacy Control Decisions , "International Journal on Re- cent and Innovation Trends in Computing and Communication ,Vol.3, pp.6327-6331, 2015.
[19] Nishant Singh, Shiv Ram Dubey, Pushkar Dixit, Jay Prakash Gupta ,"Semantic Image Retrieval by Combining Color, Texture and Shape Feat- ures," International Conference on Computing Sciences, Vol.3, pp.116-120, 2012.
[20] K. Thomas, C. Grier and D. M. Nicol, "Unfriendly: Multi-party privacy risks in social networks", Proc. 10th Int. Symp. Privacy Enhancing T- echnoogiesl, Vol.4, pp.236-252, 2010.
[21] J. Y. Choi, W. De Neve, K. Plataniotis, and Y.-M. Ro., "Collaborative face recognition for improved face annotation in personal photo colle- ctions shared on online social networks, " IEEE Transactions on Multimedia, Vol.13, pp.14–28, 2011.
[22] K. Choi, H. Byun, and K.-A. Toh." A collaborative face recognition framework on a social network platform",. 8th IEEE International Conf- erence on Automatic Face and Gesture Recognition, Vol.8, pp. 1–6, 2008.

Authors details:
B KIRAN BABU
bollavaramkiranforu@gmail.com
Dr.Samuel George Institute of Technology,
Markapur, AP.
Dr.P.Pedda Sadhu Naik, Professor & HOD,
Dr.Samuel George Institute of Technology,
Markapur, AP.