Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 4, April : 2023

TRUST-BASED PRIVACY-PRESERVING PHOTO SHARING IN ONLINE SOCIAL NETWORKS

Lt.M.Krishna Kishore, Associate Professor, Dept. of Computer Science and Engineering, Raghu Engineering College, Visakhapatnam

A.Supriya , C.N.N.N.K.Vara Prasad Raju, Ch.Vamsi 4th B.Tech Students, Dept. of Computer Science and Engineering, Raghu Engineering College, Visakhapatnam

Krishnakishore.m@raghuenggcollege.in,19981a0512@raghuenggcollege.in,
19981a0534@raghuenggcollege.in,19981a0532@raghuenggcollege.in

Abstract:

As technological developments in social media advanced, Users now frequently use online social networks to share photos and keep social relationships with one another. The information contained in a photograph, on the other hand, helps it simpler for a suspicious viewer to deduce that data about the people in the picture. There has been a lot of debate about how to handle the problem of data protection. In recent years, there has been an increase in photo sharing. When sending a picture that includes a number of users and the photo's publisher should consider the privacy of all associated users. To share these co-owned photos, we recommend a confidentiality trust-based system. In this paper. The fundamental idea is to photos based on the owners' approval are trusted. A user can provide friends and friends of friends with trust, value, and acceptance and the photographs will be viewable based on trust, acceptance, and friends of friends. The simulation's outcomes show that the mechanism for sharing photos based on trust is effective in reducing privacy loss, and the proposed minimum optimization technique provides an effective result to the user.

Keywords: Social trust, privacy protection, photo sharing, and online social networks

Introduction

Online social networks are digital platforms that enable users to connect and interact with each other through the internet. These networks allow individuals to create profiles, share content such as photos and videos, and communicate with other users through various means such as messaging, commenting, and sharing. Social media users produce a significant amount of data in the form of digital photos, videos, and text posts. Client-created content is the backbone of online entertainment [2]. Sharing user-generated content may compromise the privacy of the creator due to the fact that it typically contains private information about the author. How to deal with concerns about privacy raised by exchanging data has for some time been a hotly debated issue in online entertainment research [4], [5]. On social media websites, one popular method of sharing content is by sharing digital photos. Instagram and Facebook, two of the most widely used online social networking services, are primarily intended for photo sharing. When compared to textual information, photos provide the viewer with more detailed information, which violates an individual's right to privacy. Furthermore, a malicious viewer may use a photograph's background information to disclose confidential information. Image processing, on the other hand, makes it simpler for a person to use conceal without revealing sensitive information causing excessive harm to personal data than text editing. We evaluate the users' privacy raised by online photo-sharing networks in this paper. Present internet-based informal organization's protection strategies are primarily concerned with how the service provider will access a user's information and how a user can limit the information shared. The majority of online social networks provide a task for their User can change their privacy settings [6]. A user can specify which users have access to the photo he shares, usually based on his relationships with others. It should be noted that a user's photo may be related to other users. If one user has full control over the sharing of such photos, other related users' privacy may be negatively impacted.

The following example will help to clarify the privacy issue. Assume Alice sends an image she took of herself and her friend Bob to her colleague. Charlie did not inform Bob. It would be an invasion of Charlie's privacy if Bob shared the photo with someone he does not know well. In the prior illustration, Alice and Bob share ownership of the photograph. Alice ought to either seek Bob's approval before sharing the photo with others or, at the very least, take measures to safeguard Bob's privacy. Alice can, for instance, blur Bob's face using a photo editing program so that Charlie cannot identify him. When it comes to a picture or, more frequently, a data item and associated users frequently disagree about whether or not a user should have access to it. Conflicts between users' access control policies have been the subject of numerous research proposals [7, 8, and 9].

Literature Review

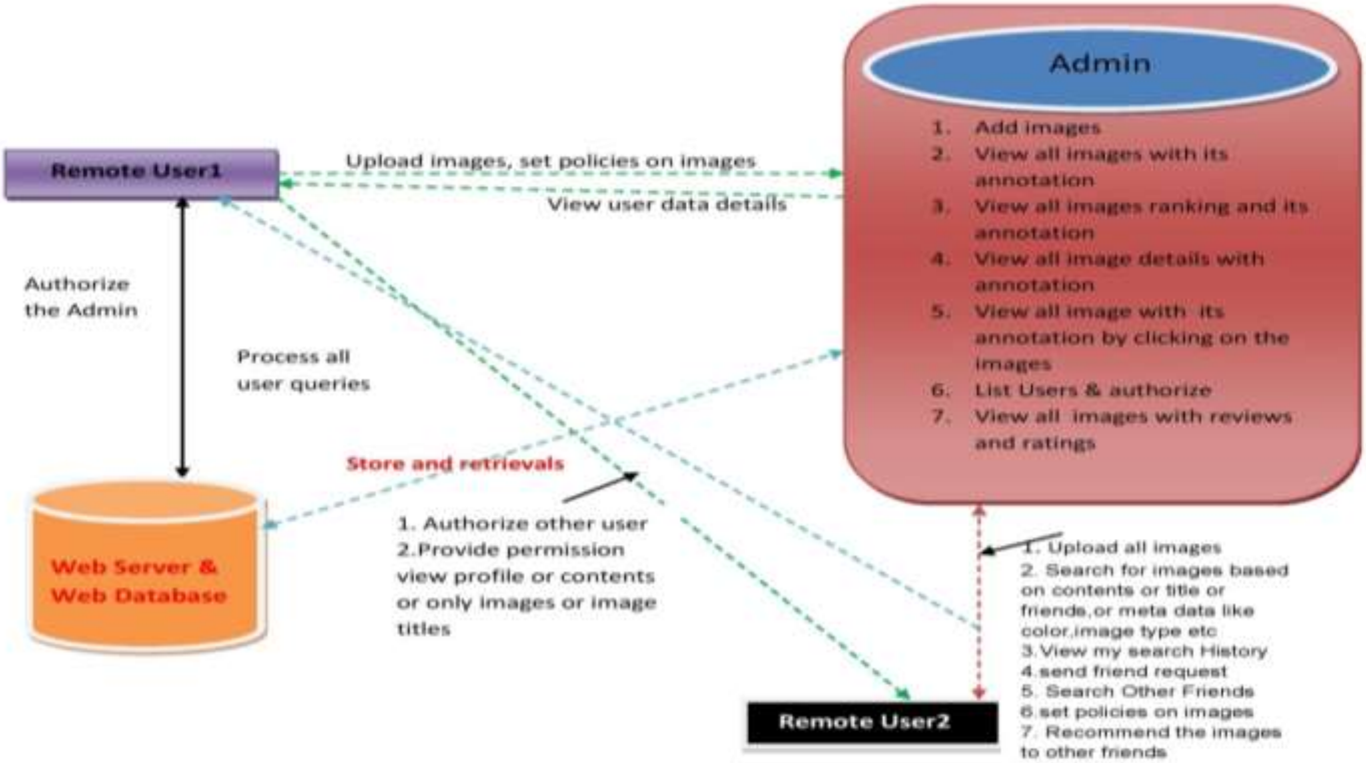
Xu et al. developed a system for achieving collaborative privacy management. Mainly, an individual wants to publish a data point according to the combined opinion of every associated person [1]. The faith results among users are applied to specify the values and opinions of users and are modified based on users' loss of privacy. Furthermore, by adjusting the parameters of the proposed mechanism, the user is able to find a compromise between privacy and data sharing preservation. The policy of the top trust restriction is used to discuss the parameter selection issue, which they model as the issue of the multi-armed bandit.

Yuan et al. suggested an encrypted, privacy-preserving photo-sharing design that considers the subject and setting of a photo while including privacy and security within the JPEG file on its own [2]. They show the suggested architectural style with ProShare, a technology demonstrator mobile iOS implementation that offers searching as a tool for setting privacy settings for a specific part of a photograph, secure messaging, access to encrypted photos, and maintaining Facebook photo sharing.

K. Xu et al. developed a system that allows every person in a picture to be informed of the photo's posting activity and take part in the choice process [3]. They require an efficient system for facial recognition (FR) that recognizes everyone in the picture for this reason. Moreover, more stringent privacy settings may restrict the amount of available public photos used to train the facial recognition system. To address this issue, this method makes an attempt to use users' own photographs to create a more personalized FR system that has been trained specifically to make a distinction possible for image founders without making compromising their privacy.

C. Ma et al. proposed a scalable media access control system to facilitate such a structure in a secure and accurate method [4]. The suggested scalable media access control framework runs on the configurable SCP-ABE (cipher text strategy essential element encryption) and a detailed key distribution scheme. To illustrate the safety in terms of the suggested method SMAC framework, we provide official security properties. Besides this, we carry out extensive testing to show off the smartphone’s effectiveness.

Workflow


Admin
1. Add images
2. View all images with its annotation
3. View all images ranking and its annotation
4. View all image details with annotation
5. View all image with its annotation by clicking on the images
6. List Users & authorize
7. View all images with reviews and ratings
Remote User1
Upload images, set policies on images
View user data details
Authorize the Admin
Process all user queries
Store and retrievals
Web Server & Web Database
1. Authorize other user
2.Provide permission view profile or contents or only images or image titles
1. Upload all images
2. Search for images based on contents or title or friends,or meta data like color,image type etc
3.View my search History
4.send friend request
5. Search Other Friends
6.set policies on images
7. Recommend the images to other friends
Remote User2

Methods

System Construction Method

There are two components to the A3P system: A3P-social and A3P-core.The following is the overall flow of data When an individual uploads an image, it is first routed to the core of A3P The image is classified by the A3P-core, which then decides whether the A3P-social is required. Most of the time, the A3P-core forecasts policy initiatives for users according to their previous behavior. On the off chance that either will call A3Psocial: (i) The user doesn't have enough details about the kind of photo that was uploaded to be able to predict policies; ii) The A3P-core works by finding major changes that have happened recently in the user's community in terms of privacy practices, as well as the user's increased social networking activities.

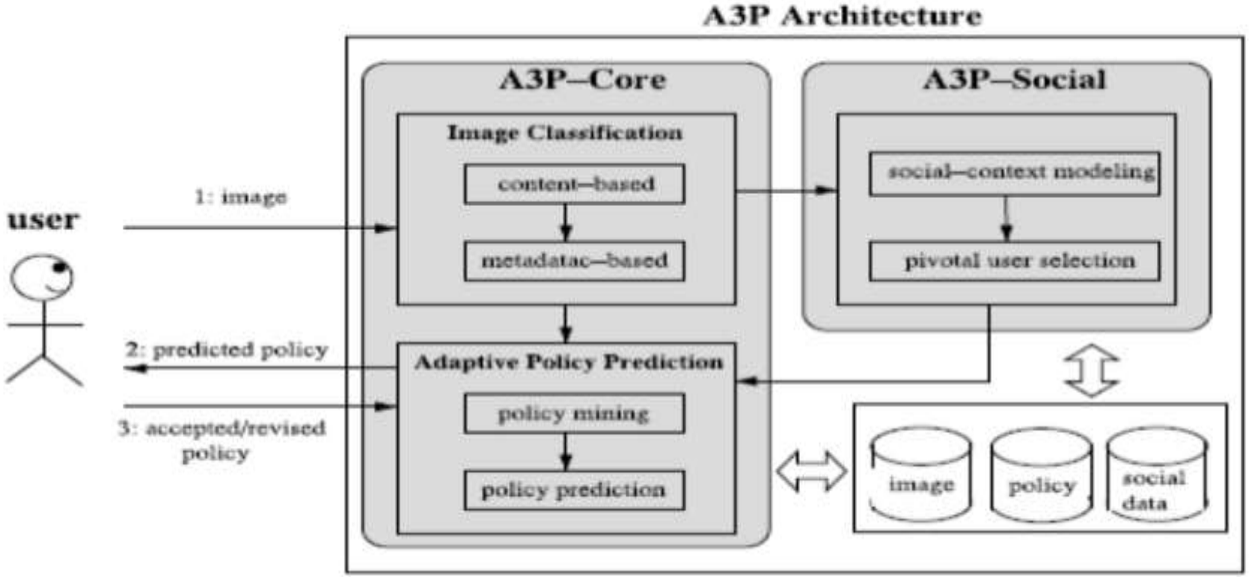


Figure.1

Content-Based Classification

We suggest a hierarchical classification method that determines the order of images based on their components and then modifies based on their metadata, each classification is subdivided into groups to produce groups of images with similar privacy preferences. Images with There will be no content-exclusive grouping of metadata. This type of classification in a hierarchy prefers image information and reduces the impact of unused tags. It should be noted that a few pictures may be included in more than one category if they have the typical metadata or content features for those categories. The foundation of our content-based classification strategy is an image similarity approach that is both efficient and accurate. Our method of classification, in particular, thinks about picture marks characterized using a quantized variant of the Haar wavelet transformation cleaned up. Each photo’s color, size, invariant transform, shape, texture, and symmetry are all encoded by the wavelet transform in frequency and space. The image's signature is then formed by selecting a small number of coefficients. The distance between signatures on an image determines the content similarity between images.

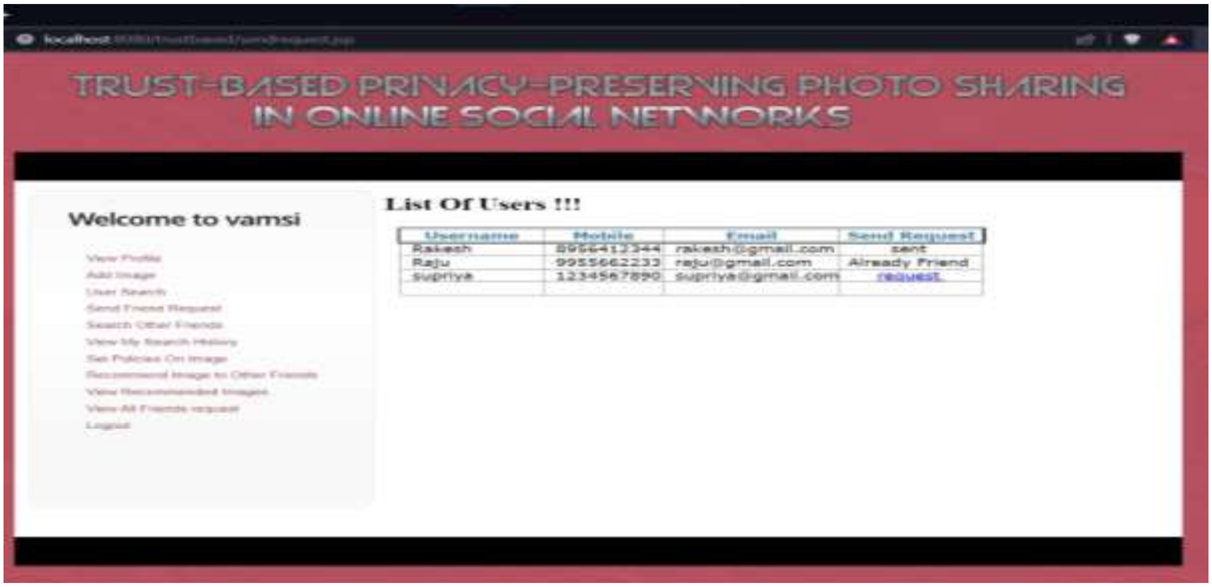
Metadata-Based Classification

The metadata-predicated category divides pictures into subcategories that fall under the preliminarily mentioned birth orders. There are three major steps in the procedure. The first step is to find keywords in an image's metadata. Tags, captions, and comments are examples of metadata considered in our work. The following step is to choose a hypernym representative of each communications data vector that is unique. The final step is to assign an image to a subcategory. This is a sequential process. Initially, the first image is a subcategory in and of itself, additionally; the subcategory's representative hypernyms are those of the image.

Adaptive Policy Prediction

For the user's future reference, the policy prediction algorithm suggests a policy for a user-submitted image. All the more critically, the expected strategy will mirror any progressions in a client's protection concerns. There are three stages to the prediction process: policy normalization, policy mining, and policy prediction are the first three.

Results

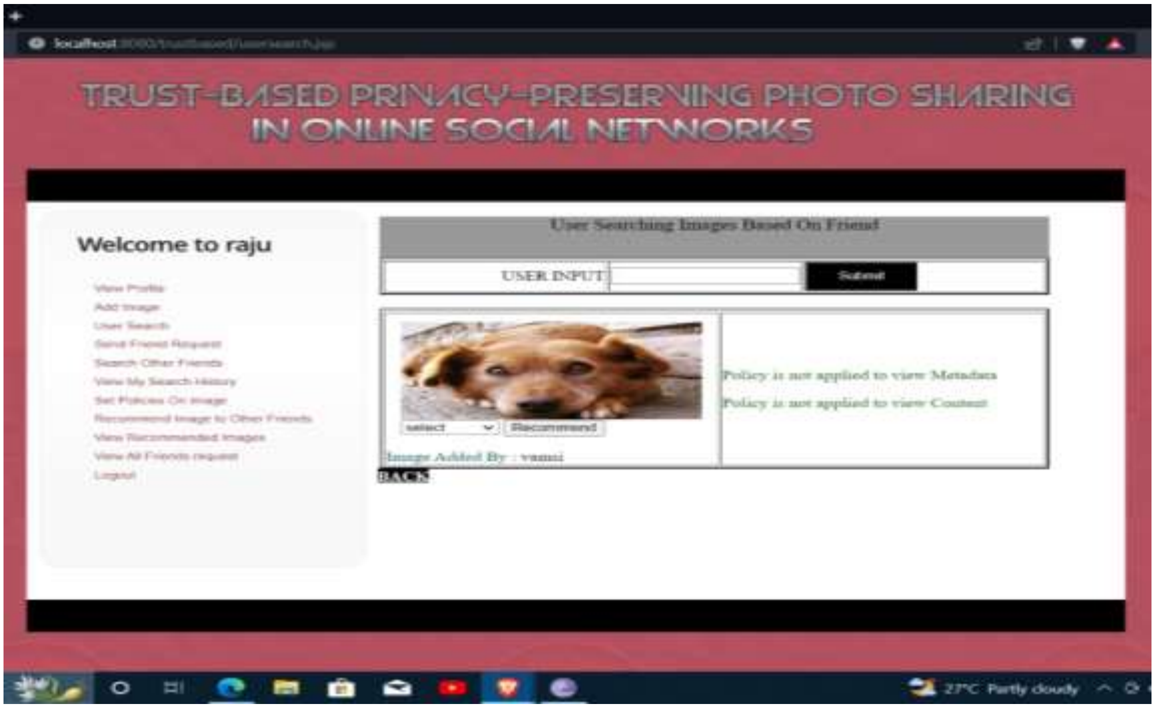


TRUST-BASED PRIVACY-PRESERVING PHOTO SHARING IN ONLINE SOCIAL NETWORKS

Welcome to vamsi

List Of Users !!!

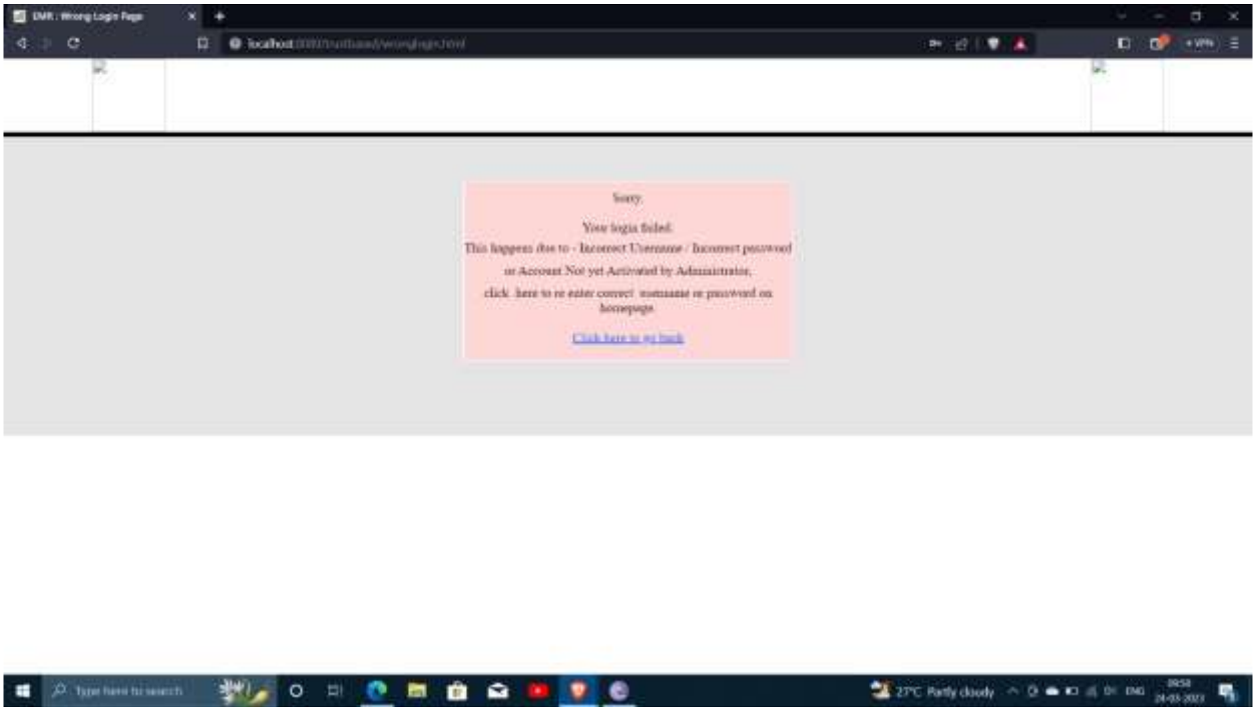
Username	Mobile	Email	Send Request
Rakesh	8956412344	rakesh@gmail.com	sent
Raju	9955662233	raju@gmail.com	Already Friend
supriya	1234567890	supriya@gmail.com	request



Policy is not applied to view Metadata

Policy is not applied to view Content

Image Added By : vamsi



Sorry.

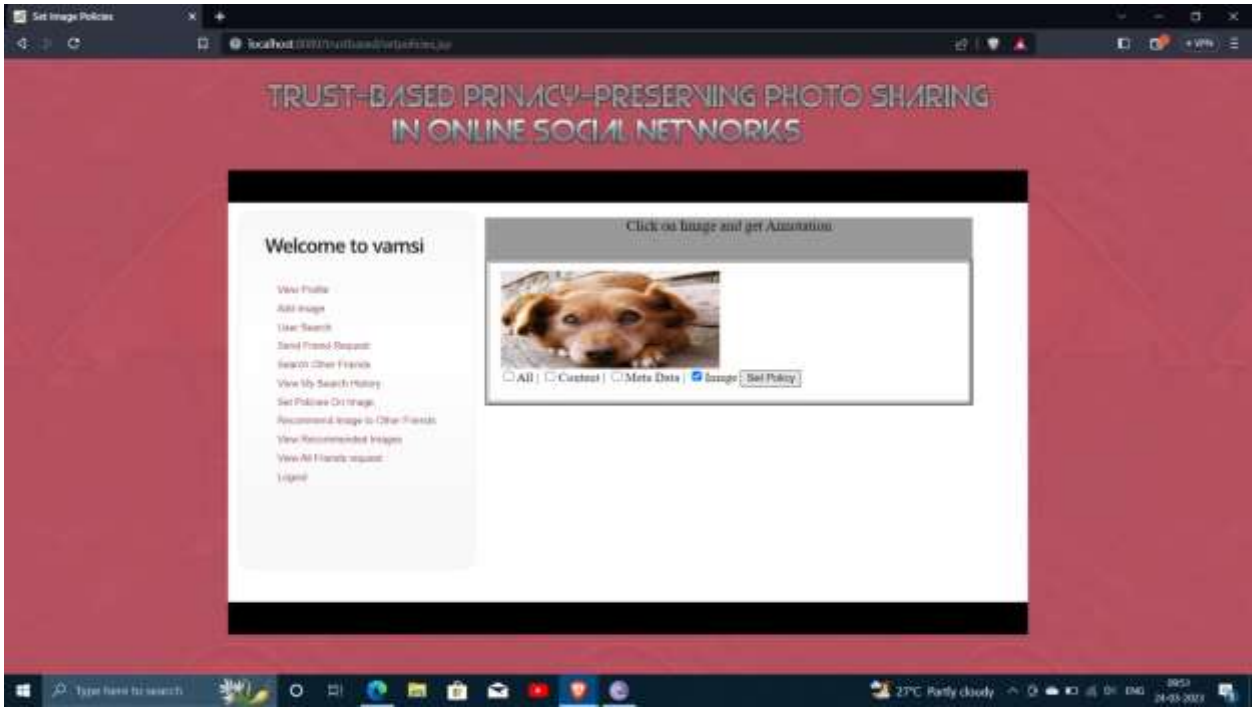
Your login failed.

This happens due to - Incorrect Username / Incorrect password

or Account Not yet Activated by Administrator,

click here to re enter correct username or password on homepage

Click here to go back



TRUST-BASED PRIVACY-PRESERVING PHOTO SHARING IN ONLINE SOCIAL NETWORKS

Welcome to vamsi

Click on Image and get Annotation

□ All | □ Content | □ Meta Data | ☑ Image | Set Policy

Conclusion

Sharing single co-owned photos on social media sites may complicate the security for multiple users. To fix such a safety concern, in this research, we suggest an image-sharing method that protects privacy that users rely on to determine how an image must be uploaded. The user's desired image is temporarily held by the user. The amount of privacy damage caused by sharing the photo is estimated provided by the service provider cause participant based on the users' trust. The provider of services then decides whether or not to remove a stakeholder from the picture by contrasting the loss of privacy to a limit set by the publisher. The photograph is now decided to share, each stakeholder looks at the loss of privacy he has experienced and changes how much he trusts the publication. This mechanism of trust encourages the publisher for privacy reasons of the stakeholders. However, the process of anonymity results in a shortfall of shared knowledge. Considering that the publisher's limit governs the exchange between sharing information and protecting privacy, we suggest a service service-assisted approach to assisting the publisher in setting the limit. We run a series of simulations utilizing real-world network data and synthetic network data information to validate the threshold tuning approach and proposed mechanism for sharing photos. The simulation results show that the publisher must adjust the threshold in order to strike a balance between photo sharing and privacy preservation in order to reduce user privacy loss by integrating trust level into the image privacy - preserving method.

References

1. Lei Xu, Ting Bao, Yan Zhang. Trust-Based Privacy-Preserving Photo Sharing in Online Social Networks. March 2019.DOI: 10.1109/TMM.2018.2887019.
2. Lin Yuan, Pavel Korshunov, T. Ebrahimi. Privacy-preserving photo sharing based on a secure JPEG. August 2015. DOI: 10.1109/INFCOMW.2015.7179382.
3. K Xu, Y Guo, Linke Guo Privacy My Decision: Control of Photo Sharing on Online Social Networks. March 2017. DOI: 10.1109/TDSC.2015.2443795.
4. C. Ma, Z. Yan, and C. W. Chen. Scalable access control for privacy-aware media sharing. Jan 2019. DOI: 10.1109/TMM.2018.2851446.
5. A. M. Kaplan and M. Haenlein. Users of the world, unite! The challenges and opportunities of social media.2010. DOI: 10.1016/bushor.2009.09.003.
6. N. Senthil Kumar, K. Saravanakumar, and K. Deepa. On privacy and security in social media a comprehensive study.2016. DOI: 10.1016/j.procs.2016.02.019.
7. Dr. K. Sridharan, Siva Ragavan, Ranjith Kumar R. Trust-based Collaborative Privacy Management in Online Social Networks. March 2019. DOI: 10.17148/IJARCCE.2019.8304.
8. Ryan Wishart, Domenico Corapi, Srdjan Marinovic. Collaborative Privacy Policy Authoring in a Social Networking Context. August 2010. DOI: 10.1109/POLICY.2010.13.
9. Pingshui Wang, Qinjuan Ma. Issues of Privacy Conflict in mobile social network. March 2020. DOI: 10.1177/1550147720912939.
10. Changji Wang, Wentao LI, Xilei Xu, Yuan Li. A Ciphertext-Policy Attribute-Based Encryption Scheme Supporting Keyword Search Function. January 2013. DOI: 10.1007/978-3-319-03584-0 28
11. W. Sherchan, S. Nepal. A survey of trust in social networks. August 2013. DOI:10.1145/2501654.2501661
12. Joseph Bonneau, Jonathan Anderson, Luke Church. Privacy Suites: Shared Privacy for Social Networks. July 2009. DOI: 10.1145/1572532.1572569.
13. Kristina Lerman, Anon Plangprasopchok, Chio Wong. Personalizing Image Search Results on Flickr. Apr 2007. DOI: 10.48550/arXiv.0704.1676