BOOSTING CONFIDENTIALITY ON DIGITAL IMAGE SHARING USING TRUST BASED APPROACH

[1] Ms.K.Spandana, [2]K.Hrithik,[3] K.Jeevika,[4] K.Nikhil Kumar,[5] K.Vasu
[1] Assistant Professor,[2345]B.Tech Students
Department Of Computer Science & Engineering
Sri Indu College Of Engineering & Technology,Sheriguda, Ibrahimpatnam

ABSTRACT

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. However, The Rich Information Contained In A Photo Makes It Easier For A Malicious Viewer To Infer Sensitive Information About Those Who Appear In The Photo. How To Deal With The Privacy Disclosure Problem Incurred By Photo Sharing Has Attracted Much Attention In Recent Years. When Sharing A Photo That Involves Multiple Users, The Publisher Of The Photo Should Take Into All Related Users' Privacy Into Account. In This Paper, We Propose A Trust- Based Privacy Preserving Mechanism For Sharing Such Co-Owned Photos. The Basic Idea Is To Anonymize The Original Photo So That Users Who May Suffer A High Privacy Loss From The Sharing Of The Photo Cannot Be Identified From The Anonymized Photo. The Privacy Loss To A User Depends On How Much He Trusts The Receiver Of The Photo. And The User's Trust In The Publisher Is Affected By The Privacy Loss. The Anonymization Result Of A Photo Is Controlled By A Threshold Specified By The Publisher. We Propose A Greedy Method For The Publisher To Tune The Threshold, In The Purpose Of Balancing Between The Privacy Preserved By Anonymization And The Information Shared With Others. Simulation Results Demonstrate That The Trust-Based Photo Sharing Mechanism Is Helpful To Reduce The Privacy Loss, And The Proposed Threshold Tuning Method Can Bring A Good Payoff To The User.

I. INTRODUCTION

Social media, which enable people to interact with each other by creating and sharing information, has now become an important part of our daily life. Users of social media services create a huge amount of information in forms of text posts, digital photos or videos. Such user generated content is the lifeblood of social media. However, user-generated content usually involves the creator's sensitive information, which means the sharing of such content may compromise the creator's privacy. How to deal with the privacy issues caused by information sharing is a long active topic in the study of social media. A major form of the content sharing activities in social media websites is the sharing of digital photos. Some popular online social networking services, such as Instagram1 , Flicker2 , and Pinterest3 , are mainly designed for photo sharing. Compared to textual data, photos can deliver more detailed information to the viewer, which is detrimental to individual's privacy. Moreover, the background information contains in a photo may be utilized by a malicious viewer to infer one's sensitive information. On the good side, it is more convenient for a user to hide his sensitive information, without too much damage to insensitive information, by image processing (e.g. blurring) than by text editing. In this paper we study the privacy issue raised by photo sharing in online social networks (OSNs). Privacy policies in current OSNs are mainly about how a user's information will be explored by the service provider, and through which methods a user can control the scope of information sharing. Most OSNs offer a privacy setting function to their users. 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. If the sharing of such photos is fully controlled by one user, then the privacy of other related users may be compromised. This privacy issue can be further explained via the following example. Suppose that Alice takes a photo of herself and her friend Bob, and then shares the photo to her colleague Charlie without telling Bob. If Bob does not know Charlie well, then the sharing of the photo will become a privacy invasion to Bob. In the above example, the photo is actually co-owned by Alice and Bob. When Alice wants to share the photo with others, she should solicit Bob's opinion, or at least, she should take some measures to reduce the possible privacy loss to Bob. For example, Alice can use a photo editing tool to make Bob's face blurred, so that Bob can hardly be identified by Charlie. Given a photo, or more generally, a data item, related users usually have different opinions on whether a user is allowed to access it. Researchers have proposed different approaches to resolve the conflicts among users' access control policies. In most studies, an aggregated policy, which is essentially a set of users who are authorized to access the data item, will be generated by a mediator (e.g. the service provider). In our previous work, a trust- based mechanism is proposed for collaborative privacy management in OSNs. The proposed mechanism requires a user to solicit related users' opinions before sharing a data item with others. The trust values between users are utilized to generate an aggregated option. By comparing the aggregated option with a threshold, the user decides whether to share the data item. Previous studies usually consider the data item to be shared as a whole. That is to say, a user can either obtain all the information contained in the data item or get nothing. However, the aggregated access control policy cannot always make every related user satisfied. In the above example, suppose there is another user David in the photo taken by Alice. If both Alice and David want Charlie to have this photo and Bob does not, then the aggregated policy generated by a majority voting scheme will authorize Charlie to view this photo. As a result, Bob's privacy is still compromised. While in fact, in the case of photo sharing, it is possible to completely resolve the conflicts among users' privacy requirements, though it is hard to realize in the case of textual data sharing. The rationale is that a photo can be divided into multiple disjoint areas. Each area can be correlated to a specific user. If we delete this area or make the area blurred, then the corresponding user's privacy can be preserved when the photo is accessible to an undesired user. In this paper, we consider a photo-sharing scenario where the user who publishes the photo, referred to as publisher, decides how to process the photo so as to protect privacy of related users. A trust-based mechanism is proposed to help the publisher make a proper decision. Different from our previous work [10], the publisher does not communicate with other related users before he posts the photo. Instead, the publisher predicts the privacy loss to each related user in case that the photo is shared with a certain user. We explore the trust between users to measure the privacy loss. The basic idea is that whether a user allows another user to learn his sensitive information depends on how much the former trusts the latter. Also, whether a user is willing to protect another user's privacy depends on how much the former trusts the latter. Basically, if the publisher predicts a high privacy loss to a related user who is also highly trusted by the publisher, then the publisher will "delete" the user from the photo by processing the corresponding area of the photo. Those related users are not directly involved in the decision-making process of the publisher. After the photo is processed and sent to the user designated by the publisher, each related user can evaluate whether his privacy is disclosed. If the user suffers a privacy loss, he will lose trust in the publisher. And if the user finds that his privacy is protected by the publisher, he may have more trust in the publisher. Due to the correlation between privacy and trust, the publisher will not ignore other users' privacy when sharing photos. Intuitively, if the publisher deletes all users from the photo, then no one will suffer a privacy loss, and the publisher will gain more trust from others. As a result, the publisher's privacy will be more valued by other users. However, with all user related information being deleted, the sharing of the photo becomes meaningless. In the proposed mechanism, a threshold is introduced to control the number of users deleted from a photo. To find a balance between privacy preserving and photo sharing, we propose a method to make the threshold adaptive to the trust relationship between users.

II. LITERATURE SURVEY

TITLE: - Privacy-Protected Photo Sharing in Social Media Platform

AUTHORS: - Regin Rajan, D Vincy Jaslin

ABSTRACT: - The advancement of the social communication platform, sharing snapshots, videos, and much more information has become a prominent way of retaining connections with multiple users. Despite the sensitive data the photo holds, it will be an effortless way for the evil-minded user to steal the data of those who appear in the picture. Dealing with the privacy exposure provoked by sharing snapshots that contain the faces of various end-users attracted the minds of many social media users. Sharing a picture that contains multiple clients, the person who uploads the images should consider the interconnected client's privacy. This paper proposes a privacy-protected mechanism based on the level of assurance the interconnected client gives to the person who uploads the picture. The thought process of this mechanism is while uploading an image of a co-owned photo, and a request is sent to the related user based on the reply the related user gives; the photo is displayed to the followers of the uploader. With the help of this privacy, the related user will not be compromising.

TITLE:- Trust-Based Privacy-Preserving Photo Sharing In Online Social Networks

AUTHORS Lt. M. Krishna Kishore, A. Supriya

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.

TITLE:- Social media privacy concerns, security concerns, trust, and awareness: Empirical validation of an instrument

AUTHORS:- Alex Koohang, Kevin Floyd, Johnathan Yerby, Joanna Paliszkiewicz

ABSTRACT:- This paper endeavours to empirically validate an instrument that measures users' privacy concerns, security concerns, trust, and risk awareness on social media. Four constructs (privacy concerns, security concerns, trust, and risk awareness) were used, each included specific items that explained the construct. Data were collected from 154 undergraduate students from a mid-sized university in the Southeast USA and analyzed via exploratory factor analysis. All subjects were using one or more social media platforms regularly. The results showed that all four constructs of the instrument were reliable to measure measures users' privacy concerns, security concerns, trust, and risk awareness on social media

TITLE: - Privacy-Protected Photo Sharing in Social Media Platform

AUTHORS: - Regin Rajan, D Vincy Jaslin

ABSTRACT: - The advancement of the social communication platform, sharing snapshots, videos, and much more information has become a prominent way of retaining connections with multiple users. Despite the sensitive data the photo holds, it will be an effortless way for the evil-minded user to steal the data of those who appear in the picture. Dealing with the privacy exposure provoked by sharing snapshots that contain the faces of various end-users attracted the minds of many social media users. Sharing a picture that contains multiple clients, the person who uploads the images should consider the interconnected client's privacy. This paper proposes a privacy-protected mechanism based on the level of assurance the interconnected client gives to the person who uploads the picture. The thought process of this mechanism is while uploading an image of a co-owned photo, and a request is sent to the related user based on the reply the related user gives; the photo is displayed to the followers of the uploader. With the help of this privacy, the related user will not be compromising.

TITLE:- Trust-Based Privacy-Preserving Photo Sharing In Online Social Networks

AUTHORS Lt. M. Krishna Kishore, A. Supriya

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.

TITLE:- Social media privacy concerns, security concerns, trust, and awareness: Empirical validation of an instrument

AUTHORS:- Alex Koohang, Kevin Floyd, Johnathan Yerby, Joanna Paliszkiewicz

ABSTRACT:- This paper endeavours to empirically validate an instrument that measures users' privacy concerns, security concerns, trust, and risk awareness on social media. Four constructs (privacy concerns, security concerns, trust, and risk awareness) were used, each included specific items that explained the construct. Data were collected from 154 undergraduate students from a mid-sized university in the Southeast USA and analyzed via exploratory factor analysis. All subjects were using one or more social media platforms regularly. The results showed that all four constructs of the instrument were reliable to measure measures users' privacy concerns, security concerns, trust, and risk awareness on social mediaTITLE: - Privacy-Protected Photo Sharing in Social Media Platform

AUTHORS: - Regin Rajan, D Vincy Jaslin

ABSTRACT: - The advancement of the social communication platform, sharing snapshots, videos, and much more information has become a prominent way of retaining connections with multiple users. Despite the sensitive data the photo holds, it will be an effortless way for the evil-minded user to steal the data of those who appear in the picture. Dealing with the privacy exposure provoked by sharing snapshots that contain the faces of various end-users attracted the minds of many social media users. Sharing a picture that contains multiple clients, the person who uploads the images should consider the interconnected client's privacy. This paper proposes a privacy-protected mechanism based on the level of assurance the interconnected client gives to the person who uploads the picture. The thought process of this mechanism is while uploading an image of a co-owned photo, and a request is sent to the related user based on the reply the related user gives; the photo is displayed to the followers of the uploader. With the help of this privacy, the related user will not be compromising.

TITLE:- Trust-Based Privacy-Preserving Photo Sharing In Online Social Networks

AUTHORS Lt. M. Krishna Kishore, A. Supriya

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.

TITLE:- Social media privacy concerns, security concerns, trust, and awareness: Empirical validation of an instrument

AUTHORS:- Alex Koohang, Kevin Floyd, Johnathan Yerby, Joanna Paliszkiewicz

ABSTRACT:- This paper endeavours to empirically validate an instrument that measures users' privacy concerns, security concerns, trust, and risk awareness on social media. Four constructs (privacy concerns, security concerns, trust, and risk awareness) were used, each included specific items that explained the construct. Data were collected from 154 undergraduate students from a mid-sized university in the Southeast USA and analyzed via exploratory factor analysis. All subjects were using one or more social media platforms regularly. The results showed that all four constructs of the instrument were reliable to measure measures users' privacy concerns, security concerns, trust, and risk awareness on social media

III. SYSTEM ANALYSIS & DESIGN

EXISTING SYSTEM

The growing amount of online personal content exposes users to a new set of privacy concerns. Digital cameras, and lately, a new class of camera phoneapplications that can upload photos or video content directly to the web, make publishing of personal content increasingly easy. Privacy concerns are especially acute in the case of these multimedia collections, as they could revealmuch of the user's personal and social environment. The persistent nature of such online media could expose rich aggregate information about the owner, andsubjects, of the content. Rather than simply searching for, and passively consuming, information, users are collaboratively creating, evaluating, and distributing information. In the near future, new information-processing applications enabled by social media will include tools for personalized information discovery, applications that exploit the “wisdom of crowds” (e.g., emergent semantics and collaborative in Copyright c 2008, American Association for Artificial Intelligence (www.aaai.org). All rights reserved. formation evaluation), deeper analysis of community structure to identify trendsand experts, and many others still difficult to imagine

PROPOSED SYSTEM

The photo sharing site Flickr is one of the earliest and more popular examples of the new generation of Web sites, labelled social media, whose content is primarily user-driven. Other examples of social media include: blogs (personal online journals that allow users to share thoughts and receive feedback on them), Wikipedia (a collectively written and edited online encyclopedia), and Del.icio.us and Digg (Web sites that allow users to share, discuss, and rank Web pages, and news stories respectively). The rise of social media underscores a transformation of the Web as fundamental as its birth. In this work, we examine how users of Flickr [8], a popular photo-sharing web site, manage their privacy policies for photographic content. The users we studied upload photos to the Flickr web site using Zone Tag, a mobile application running on high-resolution, location-aware camera phones. Concentrating on these users and the existence of contextual data that is associated with their actions puts us in a unique position to explore critical aspects of privacy, including

ADVANTAGES:

- Rich Data Source: Smartphones generate a wealth of data due to their constant connectivity and numerous sensors. This data can provide insightsinto user behaviour, preferences, and routines, making it a valuable resource for understanding privacy concerns.
- Real-Time Context: Contextual data from smartphones includes location, time, device usage, app interactions, and more. Analysing this data can reveal how users' privacy is impacted in real-time scenarios, shedding lighton the vulnerabilities they face.

SYSTEM ARCHITECTURE

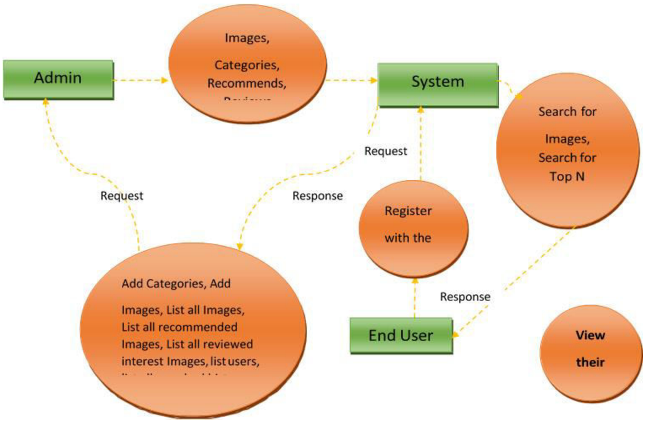


Fig. SYSTEM ARCHITECTURE

IV. IMPLEMENTATION

MODULES

- System Construction Module
- Content-Based Classification
- Metadata-Based Classification
- Adaptive Policy Prediction

MODULE DESCRIPTION

DATA OWNER

In this module, the data provider uploads their encrypted data in the Cloud server. For the security purpose the data owner encrypts the data file and then store in the server. The Data owner can have capable of manipulating the encrypted data file and performs the following operations Register and Login, Attackers, Upload File, View Files ,Verify data (Verifiability), View and Delete Files, View All Transactions.

CLOUD SERVICE PROVIDER

The Cloud server manages which is to provide data storage service for the Data Owners. The server will generate the aggregate key if the end user requests for file authorization to access and performs the following operations such as Login, View and Authorize Users, View and Authorize Owners, View Files, View All Search Transactions, View All File Transactions, View All Top Searched, View Attackers, Search Requests, View Time Delay, View Throughput.

USER

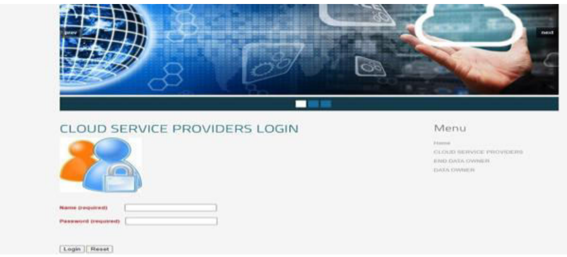
In this module, the user can only access the data file with the secret key. The user can search the file for a specified keyword. The data which matches for a particular keyword will be indexed in the cloud server and then response to the end user and performing the following operations Register and Login, My Profile, View Files, Search Files,

Search Ratio, Top K Search, Req Search Control.

PKG
responsible for viewing Files and Generate Key.

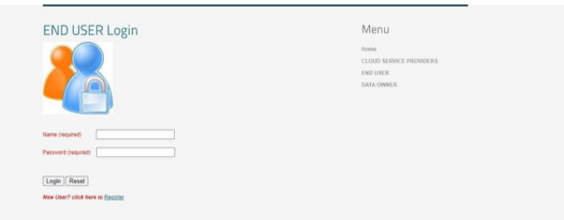
V. SCREENSHOTS:

Cloud Service Provider Login



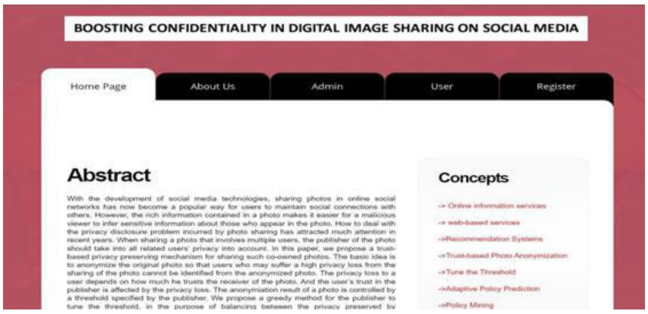
End Data Owner Register

End User Login



New User? click here to Register

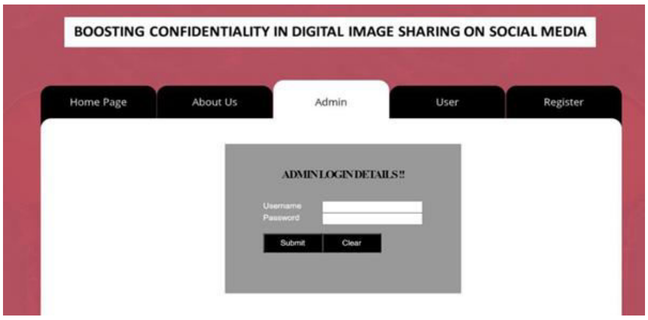
Home Screen


BOOSTING CONFIDENTIALITY IN DIGITAL IMAGE SHARING ON SOCIAL MEDIA
Home Page
About Us
Admin
User
Register
Concepts
-> Online information services
-> web-based services
->Recommendation Systems
->Trust-based Photo Anonymization
->Tune the Threshold
->Adaptive Policy Prediction
->Policy Mining

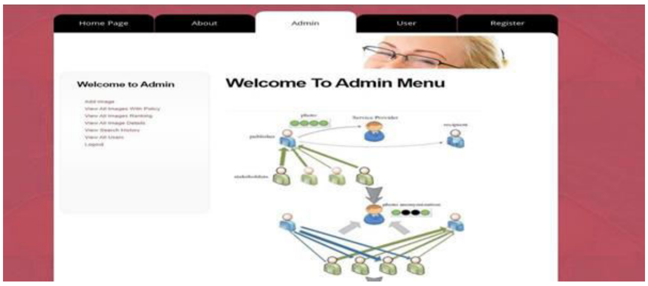
Abstract

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. However, the rich information contained in a photo makes it easier for a malicious viewer to infer sensitive information about those who appear in the photo. How to deal with the privacy disclosure problem incurred by photo sharing has attracted much attention in recent years. When sharing a photo that involves multiple users, the publisher of the photo should take into all related users' privacy into account. In this paper, we propose a trust-based privacy preserving mechanism for sharing such co-owned photos. The basic idea is to anonymize the original photo so that users who may suffer a high privacy loss from the sharing of the photo cannot be identified from the anonymized photo. The privacy loss to a user depends on how much he trusts the receiver of the photo. And the user's trust in the publisher is affected by the privacy loss. The anonymiation result of a photo is controlled by a threshold specified by the publisher. We propose a greedy method for the publisher to tune the threshold, in the purpose of balancing between the privacy preserved by

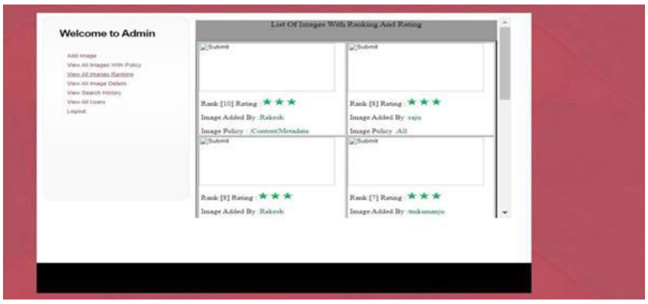
Admin Login



Admin Menu



View All Images Ranking:



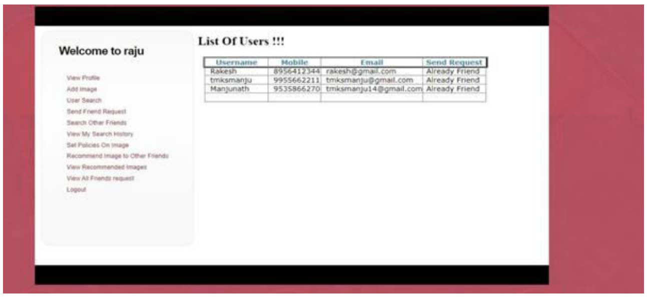
Rank [10] Rating : ★★★
Image Added By :Rakesh
Image Policy : :Content\Metadata

Rank [8] Rating : ★★★
Image Added By :raju
Image Policy :All

Rank [8] Rating : ★★★
Image Added By :Rakesh

Rank [7] Rating : ★★★
Image Added By :tmksmanju

Send Friend request



List Of Users !!!

Username	Mobile	Email	Send Request
Rakesh	8956412344	rakesh@gmail.com	Already Friend
tmksmanju	9955662211	tmksmanju@gmail.com	Already Friend
Manjunath	9535866270	tmksmanju14@gmail.com	Already Friend

Add Image

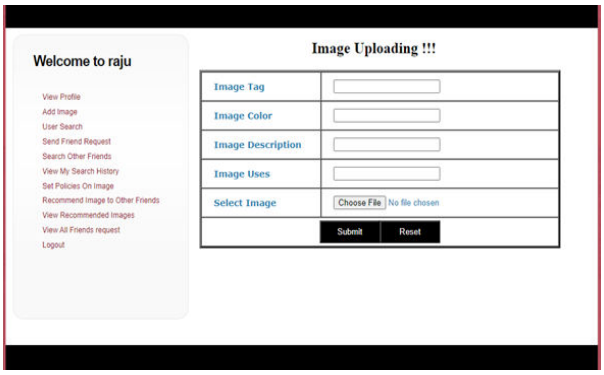
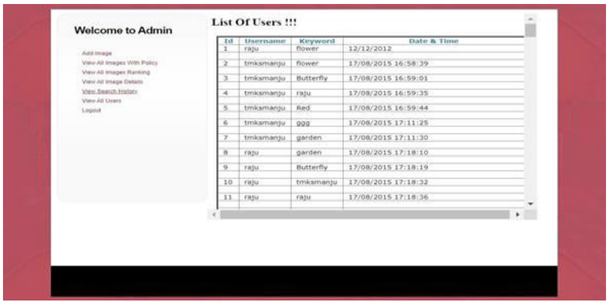


Image Uploading !!!

Image Tag	
Image Color	
Image Description	
Image Uses	
Select Image	Choose File No file chosen

Search History



List Of Users !!!

Id	Username	Keyword	Date & Time
1	raju	flower	12/12/2012
2	tmksmanju	flower	17/08/2015 16:58:39
3	tmksmanju	Butterfly	17/08/2015 16:59:01
4	tmksmanju	raju	17/08/2015 16:59:35
5	tmksmanju	Red	17/08/2015 16:59:44
6	tmksmanju	ggg	17/08/2015 17:11:25
7	tmksmanju	garden	17/08/2015 17:11:30
8	raju	garden	17/08/2015 17:18:10
9	raju	Butterfly	17/08/2015 17:18:19
10	raju	tmksmanju	17/08/2015 17:18:32
11	raju	raju	17/08/2015 17:18:36

VI. CONCLUSION

CONCLUSION

Sharing one co-owned photo in an OSN may compromise multiple users' privacy. To deal with such a privacy issue, in this paper we propose a privacy- preserving photo sharing mechanism which utilizes trust values to decide how a photo should be anonymized. The photo that a user wants to share is temporarily holden by the service provider. Based on the trust relationship between users, the service provider estimates how much privacy loss the sharing of the photo can bring to a stakeholder. Then by comparing the privacy loss with a threshold specified by the publisher, the service provider decides if a stakeholder should be deleted from the photo. After the photo is shared, each stakeholder evaluates the privacy loss he has really suffered, and his trust in the publisher changes accordingly. This trust-based mechanism motivates the publisher to protect the stakeholders' privacy. However, the anonymization operation leads a loss in the shared information. Considering that the threshold specified by the publisher controls the trade-off between privacy preserving and information sharing, we propose a service providerassisted method to help the publisher to tune the threshold. By using synthetic network data and real-world network data, we conduct a series of simulations to verify the proposed photo sharing mechanism and the threshold tuning method. Simulation results demonstrate that incorporating trust values into the photo anonymization process can help to reduce user's privacy loss, and adaptively setting the threshold is necessary for the publisher to balance between privacy preserving and photo sharing. In current study, we mainly focus on the sharing between one publisher and one receiver. Considering that in practice, a user generally shares a photo with multiple users simultaneously, we'd like to investigate such a one- to-many case in future work. The proposed threshold tuning method can be seen as a greedy method, in the sense that the publisher prefers to choose the threshold that brings him the maximal instant payoff. Due to the correlation between privacy loss and trust values, current choice of the threshold will affect the publisher's future payoffs. In future work, we'd like to investigate how to modify the tuning method so as to achieve a better result.

FUTURE SCOPE

In current study, we mainly focus on the sharing between one publisher and one receiver. Considering that in practice, a user generally shares a photo with multiple users simultaneously, we'd like to investigate such a one-to-many case in future work. The proposed threshold tuning method can be seen as a greedy method, in the sense that the publisher prefers to choose the threshold that brings him the maximal instant payoff. Due to the correlation between privacy loss and trust values, current choice of the threshold will affect the publisher's future payoffs. In future work, we'd like to investigate how to modify the tuning method so as to achieve a better result.

REFERENCES

1. W. G. Mangold and D. J. Faulds, "Social media: The new hybrid element of the promotion mix," Business horizons, vol. 52, no. 4, pp. 357–365, 2009.
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. [Online].Available: http://www.sciencedirect.com/science/article/pii/S1877050916000211
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.