International Journal of Research
Available at https://edupediapublications.org/journals

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 22
November 2018

Privacy Policy Inference of User-Uploaded Images On Content Sharing Sites

E.Yasoda Rani[1], M.Subba Reddy[2]
P.G. Scholar[1] , M.Tech,(Ph.D.,)[2]
Branch : Computer Science and Engineering
SVR Engineering College
Email: :yasodarani.ediga@gmail.com, subbareddy.meruva@gmail.com

ABSTRACT

With the expanding volume of images clients share through social destinations, keeping up privacy has turned into a noteworthy issue, as shown by an ongoing influx of exposed occurrences where clients incidentally shared individual information. In light of these episodes, the need of instruments to enable clients to control access to their common substance is evident. Toward tending to this need, we propose an Adaptive Privacy Policy Prediction (A3P) framework to enable clients to form privacy settings for their images. We look at the job of social setting, picture substance, and metadata as conceivable pointers of clients' privacy inclinations. We propose a two-level structure which as indicated by the client's accessible history on the site, decides the best accessible privacy policy for the client's images being transferred. Our answer depends on a picture classification structure for picture classes which might be related with comparable arrangements, and on a policy prediction algorithm to naturally produce a policy for each recently transferred picture, likewise as indicated by clients' social highlights. After some time, the produced arrangements will pursue the advancement of clients' privacy state of mind. We give the consequences of our broad assessment more than 5,000 arrangements, which show the viability of our framework, with prediction exactnesses more than 90 percent.

INTRODUCTION

Images are presently one of the key empowering agents of clients' availability. Sharing happens both among recently settled gatherings of known individuals or social circles (e. g., Google+, Flickr or Picasa), and furthermore progressively with individuals outside the client's social circles, for motivations behind social revelation to enable them to distinguish new companions and find out about associate's interests and social environment. Be that as it may, semantically rich images may uncover content touchy information. Think about a photograph of an understudy's 2012 graduation service, for instance. It could be shared inside a Google+ circle or Flickr gathering, yet may superfluously uncover the understudies, relatives and different companions. Sharing images inside online substance sharing destinations, thusly, may rapidly prompt undesirable exposure and privacy infringement. Further, the determined idea of online media makes it workable for different clients to gather rich accumulated information about the proprietor of the distributed substance and the subjects in the distributed substance. The totaled information can result in surprising presentation of one's social condition and prompt maltreatment of one's close to home information. Most substance sharing sites enable clients to enter their privacy inclinations. Tragically, late examinations have demonstrated that clients battle to set up and keep up such privacy settings. One of the primary reasons gave is that given the measure of shared information this procedure can be repetitive and mistake inclined. Thusly, many have recognized the need of policy suggestion frameworks which can help clients to effectively and legitimately arrange privacy settings. Be that as it may, existing recommendations for computerizing privacy settings seem, by all accounts, to be insufficient to address the extraordinary privacy needs of images, because of the measure of information certainly conveyed inside images, and their association with the online condition wherein they are uncovered. In this paper, we propose an Adaptive Privacy Policy Prediction (A3P) framework which intends to give clients a problem free privacy settings encounter via consequently creating customized approaches. The A3P framework handles client transferred images, and factors in the accompanying criteria that impact one's privacy settings of images: The effect of social condition and individual attributes. Social setting of clients, for example, their profile information and associations with others may give helpful information in regards to clients' privacy inclinations. For instance, clients intrigued by photography may get a kick out of the chance to share their photographs with other beginner picture takers. Clients who have a few relatives among their social contacts may impart to them pictures identified with family occasions. Be that as it may, utilizing normal arrangements over all clients or crosswise over clients with comparable characteristics might be excessively oversimplified and not fulfill singular inclinations. Clients may have definitely extraordinary feelings even on a similar kind of images.

For instance, a privacy unfriendly individual might will share all his own images while a more moderate individual may simply need to impart individual images to his relatives.

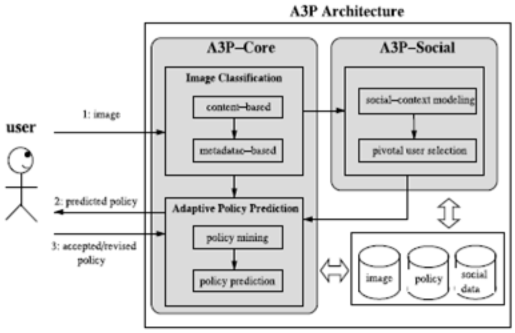


Figure 1: A3P Architecture

In light of these contemplations, it is critical to discover the adjusting point between the effect of social condition and clients' individual qualities with the end goal to foresee the arrangements that coordinate every individual's needs. In addition, people may change their general mentality toward privacy over the long haul. With the end goal to build up a customized policy suggestion framework, such changes on privacy feelings ought to be painstakingly considered. The job of picture's substance and metadata. All in all, comparable images frequently cause comparable privacy inclinations, particularly when individuals show up in the images. For instance, one may transfer a few photographs of his children and determine that just his relatives are permitted to see these photographs. He may transfer some different photographs of scenes which he took as a side interest and for these photographs, he may set privacy inclination enabling anybody to view and remark the photographs. Investigating the visual substance may not be adequate to catch clients' privacy inclinations. Labels and other metadata are demonstrative of the social setting of the picture, including where it was taken and why [4], and furthermore give an engineered portrayal of images, supplementing the information acquired from visual substance investigation. Relating to the previously mentioned two criteria, the proposed A3P framework is contained two principle building hinders (as appeared in Fig. 1): A3P-Social and A3P-Core. The

A3P-center spotlights on examining every individual client's very own images and metadata, while the A3P-Social offers a network point of view of privacy setting suggestions for a client's potential privacy enhancement. We plan the connection streams between the two building squares to adjust the advantages from meeting individual attributes and getting network exhortation.

To survey the handy estimation of our methodology, we assembled a framework model and played out a broad exploratory assessment. We gathered and tried more than 5,500 genuine arrangements created by in excess of 160 clients. Our exploratory outcomes exhibit both productivity and high prediction precision of our framework. A primer talk of the A3P-center was exhibited in [32]. In this work, we present an updated adaptation of A3P, which incorporates an all-inclusive policy prediction algorithm in A3P-center (that is currently parameterized dependent on client gatherings and furthermore factors in conceivable anomalies), and another A3P-social module that builds up the thought of social setting to refine and broaden the prediction intensity of our framework. We likewise direct extra tries different things with another informational collection gathering more than 1,400 images and relating arrangements, and we expand our examination of the exact outcomes to reveal more bits of knowledge of our framework's execution. Whatever remains of the paper is sorted out as pursues.

SYSTEM ARCHITECTURE

Architecture Flow:

Underneath design outline speaks to chiefly stream of demand from the clients to database through servers. In this situation in general framework is planned in three levels independently utilizing three layers called introduction layer, business layer, information interface layer. This venture was produced utilizing 3-level design.

3-Tier Architecture:

The three-level programming architecture (a three-layer architecture) developed during the 1990s to beat the confinements of the two-level architecture. The third level (center level server) is between the UI (customer) and the information administration (server) segments. This center level gives process administration where business rationale and principles are executed and can oblige many clients (when contrasted with just 100 clients with the two level architecture) by giving capacities, for example, lining, application execution, and database organizing.

The three level architecture is utilized when a powerful circulated customer/server configuration is required that gives (when contrasted with the two level) expanded execution, adaptability, practicality, reusability, and versatility, while concealing the unpredictability of disseminated handling from the client. These qualities have made three layer architectures a famous decision for Internet applications and net-driven information frameworks

Advantages of Three-Tier:

- Separates usefulness from introduction
- Clear partition - better understanding
- Changes constrained to well characterize segments
- Can be running on WWW
- Effective system execution

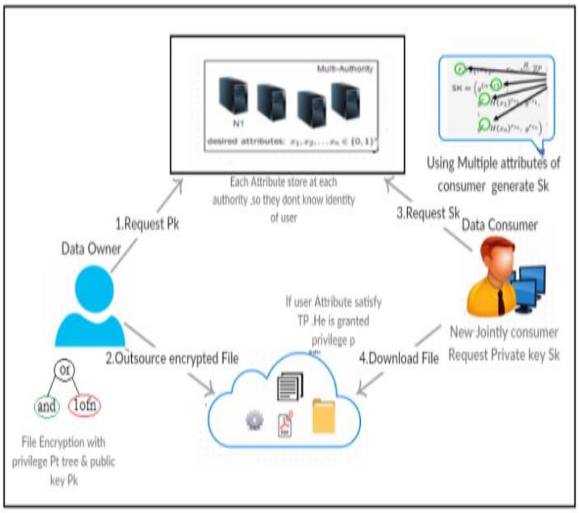

Multi-Authority
N1
desired attributes: $x_1, x_2, \ldots, x_n \in \{0,1\}^*$
SK =
Using Multiple attributes of consumer generate Sk
Each Attribute store at each authority ,so they dont know identity of user
1.Request Pk
3.Request Sk
Data Consumer
Data Owner
If user Attribute satisfy TP .He is granted privilege p
New Jointly consumer Request Private key Sk
2.Outsource encrypted File
4.Download File
or
and
1ofn
File Encryption with privilege Pt tree & public key Pk

Figure 4.3 :System Architecture

ARCHITECTURE DIAGRAM

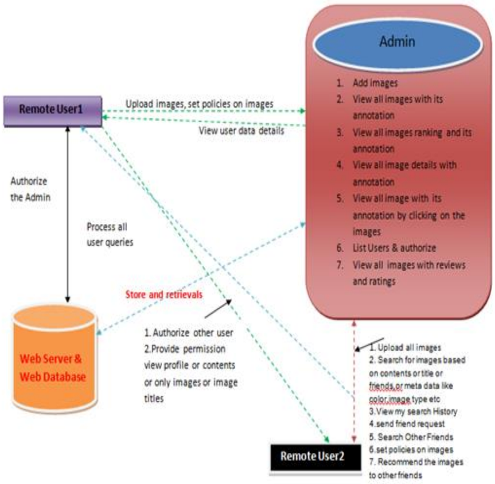

Admin
1. Add images
2. View all images with its annotation
3. View all images ranking and its annotation
4. View all image details with annotation
5. View all image with its annotation by clicking on the images
6. List Users & authorize
7. View all images with reviews and ratings
Remote User1
Upload 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

Figure 4.4: System Design

RELATED WORKS

According to Banupriya(2016) Social Network is a rising E-benefit for substance sharing destinations (CSS). It is rising administration which gives a dependable correspondence, through this correspondence another assault ground for information programmers; they can without much of a stretch abuses the information through these media. A few clients over CSS influences clients privacy on their own substance, where a few clients continue sending undesirable remarks and messages by exploiting the clients' characteristic trust in their relationship organize. By this privacy of the client information might be misfortune for this issue this paper handles the most predominant issues and dangers focusing on various CSS as of late. This proposes a privacy policy prediction and access limitations alongside blocking plan for social locales utilizing information mining systems. To play out this, the framework uses APP (Access Policy Prediction) and

Access control system by applying BIC algorithm (Bayesian Information Criterion).

According to Anna Cinzia(2011) An ever increasing number of individuals go online today and offer their own images utilizing well known web administrations like Picasa. While getting a charge out of the accommodation brought by cutting edge innovation, individuals likewise turned out to be mindful of the privacy issues of information being shared. Ongoing investigations have featured that individuals anticipate that more devices will enable them to recapture authority over their privacy. In this work, we propose an Adaptive Privacy Policy Prediction (A3P) framework to enable clients to form privacy settings for their images. Specifically, we analyze the job of picture substance and metadata as conceivable pointers of clients' privacy inclinations. We propose a two-level picture classification system to get picture classes which might be related with comparable arrangements. At that point, we build up a policy prediction algorithm to consequently produce a policy for each recently transferred picture. In particular, the created policy will pursue the pattern of the client's privacy concerns advanced with time. We have directed a broad client consider and the outcomes show adequacy of our framework with the prediction exactness around 90%.

We have led the primary exhaustive investigation of the market for privacy practices and strategies in online social systems. From an assessment of 45 social systems administration locales utilizing 260 criteria we locate that numerous prominent suppositions with respect to privacy and social systems administration should be returned to while considering the whole biological system rather than just a bunch of surely understood destinations. In spite of the basic impression of an oligopolistic advertise, we discover proof of enthusiastic rivalry for new clients. In spite of watching numerous poor security rehearses, there is proof that social system suppliers are trying endeavors to actualize privacy improving advances with considerable assorted variety in the measure of privacy control advertised. Be that as it may, privacy is once in a while utilized as an offering point, and, after its all said and done just as helper, nondecisive element. Locales additionally neglected to advance their current privacy controls inside the site. We comparatively discovered incredible assorted variety in the length and substance of formal privacy strategies, however found an inverse special pattern: however all approaches are not available to conventional clients because of jumbling lawful language, they prominently vaunt the destinations' privacy rehearses. We infer that the market for privacy in social systems is useless in that there is huge variety in destinations' privacy controls, information accumulation necessities, and lawful privacy approaches, however this isn't successfully passed on to clients. Our experimental discoveries inspire us to present the novel model of a privacy correspondence diversion, where the monetarily discerning decision for a site administrator is to make privacy control accessible to sidestep feedback from privacy fundamentalists, while concealing the privacy control interface and privacy policy to expand join numbers and energize information sharing from the practical dominant part of clients.

A Survey on **"Fuzzy identity-based encryption"**

Abstract

As sharing individual media online ends up simpler and generally spread, new privacy concerns develop particularly when the steady idea of the media and related setting uncovers insights about the physical and social setting in which the media things were made. In a first-of-its-kind examination, we utilize setting mindful camera telephone gadgets to inspect privacy choices in portable and online photograph sharing. Through information investigation on a corpus of privacy choices and related setting information from a certifiable framework, we recognize connections between area of photograph catch and photograph privacy settings. Our information examination prompts additionally questions which we explore through an arrangement of meetings with 15 clients. The meetings uncover regular topics in privacy contemplations: security, social exposure, character and comfort. At long last, we feature a few ramifications and open doors for plan of media sharing applications, including utilizing past privacy examples to forestall oversights and mistakes.

Issues of online privacy have for some time been of worry in the HCI people group, and are of developing worry for the overall population as an expanding measure of individual substance is getting to be accessible on the web. They have directed a subjective and quantitative investigation of privacy in a genuine photograph sharing versatile and online application. Utilizing setting mindful camera telephones as catch gadgets enabled us to investigate examples of privacy in a way that was already inaccessible. Our discoveries, and structure suggestions, are significant to scientists and originators of substance sharing frameworks and additionally versatile catch gadgets. Are clients over-uncovered? For the present, it involves taste; however while the potential for fiasco exists, a few clients stay unconcerned. We are planning to continue examining the theme to get a more definite take a gander at examples over a more extended era, and maybe in various societies.

EXISTING SYSTEM

Most substance sharing sites enable clients to enter their privacy inclinations. Lamentably, late investigations have demonstrated that clients battle to set up and keep up such privacy settings.

One of the primary reasons gave is that given the measure of shared information this procedure can be dreary and blunder inclined. In this manner, many have recognized the need of policy suggestion frameworks which can help clients to effortlessly and legitimately arrange privacy settings.

PROPOSED SYSTEM

In this paper, we propose an Adaptive Privacy Policy Prediction (A3P) framework which expects to give clients a problem free privacy settings encounter via naturally creating customized strategies. The A3P framework handles client transferred images, and factors in the accompanying criteria that impact one's privacy settings of images.

The effect of social condition and individual attributes. Social setting of clients, for example, their profile information and associations with others may give helpful information in regards to clients' privacy inclinations. For instance, clients inspired by photography may get a kick out of the chance to share their photographs with other novice picture takers.

The job of picture's substance and metadata. By and large, comparable images frequently bring about comparative privacy inclinations, particularly when individuals show up in the images. For instance, one may transfer a few photographs of his children and indicate that just his relatives are permitted to see these photographs.

Useful Requirements:
Information Owner:

A Data Owner is the substance who wishes to redistribute scrambled information record to the Cloud Servers.

Cloud Server:

The Cloud Server, who is expected to have sufficient capacity limit, does only store them.

Information Consumers:

All Data Consumers can download any of the scrambled information records, however just those whose private keys fulfill the benefit tree Tp can execute the task related with benefit p. The server is appointed to execute a task p if and just if the client's accreditations are confirmed through the benefit tree Tp. Recently joined Data Consumers ask for private keys from the majority of the experts, and they don't realize which properties are controlled by which specialists. At the point when the Data Consumers ask for their private keys from the specialists, experts mutually make relating private key and send it to them.

NON-FUNCTIONAL REQUIREMENTS

Expanded administrator security: The PC ought to be exceedingly anchored and available just by the manager to evade the abuse of the application.

Compactness: The GUIs of this application is easy to understand so it is simple for the client to comprehend and react to the equivalent.

Unwavering quality: This framework has high likelihood to convey us the required questions and the functionalities accessible in the application.

Reaction time: The time taken by the framework to finish an undertaking given by the client is observed to be less.

Adaptability: The framework can be reached out to coordinate the adjustments done in the present application to enhance the nature of the item. This is intended for the future works that will be done on the application.

Strength: The application is blame tolerant as for unlawful client/collector inputs. Mistake checking has been worked in the framework to avoid framework disappointment.
Document Uploading Protocol:

This convention goes for enabling customers to transfer records by means of the evaluator. In particular, the record transferring convention incorporates three stages:

• Phase 1 (cloud customer → cloud server): customer plays out the copy check with the cloud server to affirm if such a document is put away in distributed storage or not before transferring a record. On the off chance that there is a copy, another convention called Proof of Ownership will be kept running between the customer and the distributed storage server. Something else, the accompanying conventions (counting stage 2 and stage 3) are kept running between these two substances.

• Phase 2 (cloud customer → examiner): customer transfers records to the inspector, and gets a receipt from reviewer.

• Phase 3 (examiner → cloud server): inspector produces an arrangement of labels for the transferring document, and send them alongside this record to cloud server.

Modules

System Construction Module

The A3P structure contains two principal parts: A3P-focus and A3P-social. The general information stream is the going with. Exactly when a customer exchanges an image, the image will be first sent to the A3P-focus. The A3P-focus arranges the image and chooses if there is a need to gather the A3P-social. Generally speaking, the A3P-focus predicts approaches for the customers clearly subject to their chronicled lead.
In case one of the going with two cases is affirmed legitimate, A3P-focus will summon A3Psocial: (I) The customer does not have enough information for the kind of the exchanged picture to lead policy prediction; (ii) The A3P-focus recognizes the continuous critical changes among the customer's district about their privacy practices close by customer's extension of social frameworks organization works out (development of new partners, new posts on one's profile et cetera).

Content-Based Classification

To get social occasions of images that may be connected with practically identical privacy tendencies, we propose a dynamic picture classification which organizes images initially subject to their substance and after that refine each class into subcategories reliant on their metadata. Images that don't have metadata will be amassed just by substance. Such a dynamic classification gives a higher need to picture substance and limits the effect of missing marks. Note that it is possible that a couple of images are fused into different classifications as long as they contain the average substance features or metadata of those classifications.

Our approach to manage substance built classification is arranged in light of a powerful yet correct picture likeness approach. Specifically, our classification algorithm sees picture marks portrayed subject to estimated and disinfected type of Haar wavelet change. For each image, the wavelet change encodes repeat and spatial information related to picture shading, measure, invariant change, shape, surface, symmetry, et cetera. By then, couple of coefficients are molded the sign of the image. The substance similarity among images is then controlled by the division among their image marks.

Metadata-Based Classification

The metadata-based classification packs images into subcategories under recently specified standard classes. The technique includes three key advances. The underlying advance is to expel watchwords from the metadata related with an image. The metadata considered in our work are marks, engravings, and comments. The second step is to deduce an operator hypernym (demonstrated as h) from each metadata vector. The third step is to find a subcategory that an image has a place with. This is an incremental technique. At the beginning, the essential picture shapes a subcategory as itself and the specialist hypernyms of the image transforms into the subcategory's agent hypernyms.

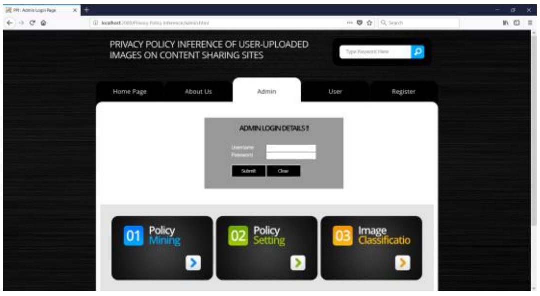
Adaptive Policy Prediction

The policy prediction algorithm gives a foreseen policy of an as of late exchanged picture to the customer for his/her reference. Even more significantly, the foreseen policy will reflect the possible changes of a customer's privacy concerns. The prediction methodology includes three essential stages: (I) policy institutionalization; (ii) policy mining; and (iii) policy prediction.

SCREEN SHOTS

Experimental result analysis is a procedure of analyzing the output of experiments carried on the system.

Admin Login Page

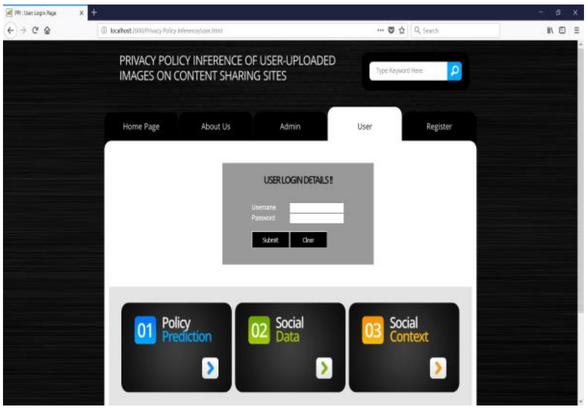


PRIVACY POLICY INFERENCE OF USER-UPLOADED IMAGES ON CONTENT SHARING SITES

ADMIN LOGIN DETAILS !!

Username
Password

User Login Page

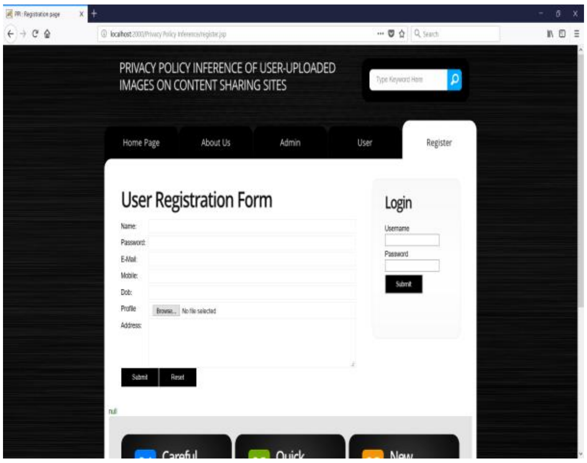


PRIVACY POLICY INFERENCE OF USER-UPLOADED IMAGES ON CONTENT SHARING SITES

USER LOGIN DETAILS !!

Username
Password

User Registration Page



PRIVACY POLICY INFERENCE OF USER-UPLOADED IMAGES ON CONTENT SHARING SITES

User Registration Form

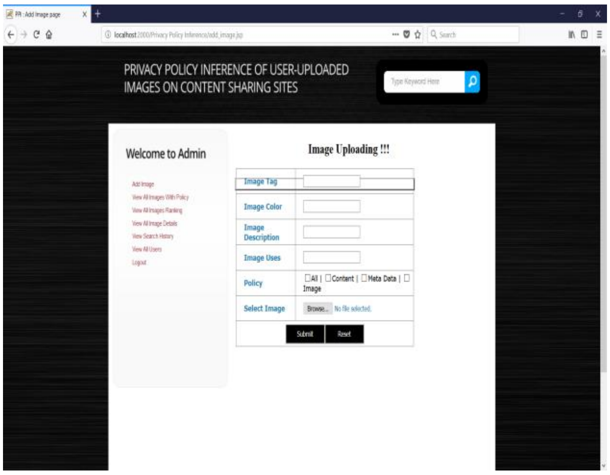
Name:
Password:
E-Mail:
Mobile:
Dob:
Profile: Browse... No file selected
Address:

null

Login

Username
Password

Administrator: Add Image Page



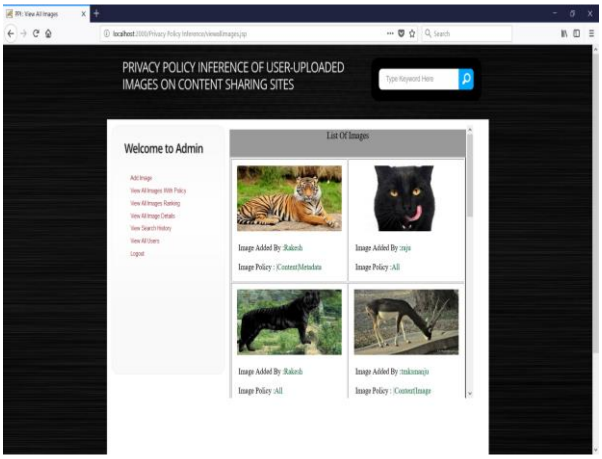
PRIVACY POLICY INFERENCE OF USER-UPLOADED IMAGES ON CONTENT SHARING SITES

Welcome to Admin

Image Uploading !!!

Image Tag
Image Color
Image Description
Image Uses
Policy □All | □Content | □Meta Data | □ Image
Select Image Browse... No file selected.

Administrator: View All Images with Policy



PRIVACY POLICY INFERENCE OF USER-UPLOADED IMAGES ON CONTENT SHARING SITES

Welcome to Admin

List Of Images

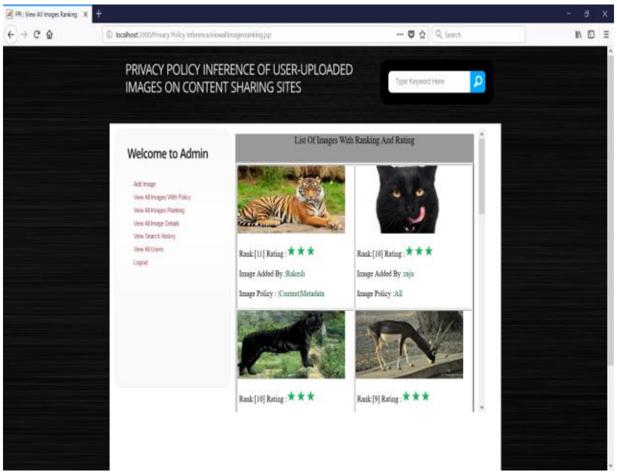
Image Added By :Rakesh
Image Policy : ContentMetadata

Image Added By :raju
Image Policy :All

Image Added By :Rakesh
Image Policy :All

Image Added By :tmkumaraju
Image Policy : ContentImage

Administrator: View All Images Ranking



PRIVACY POLICY INFERENCE OF USER-UPLOADED IMAGES ON CONTENT SHARING SITES

Welcome to Admin

List Of Images With Ranking And Rating

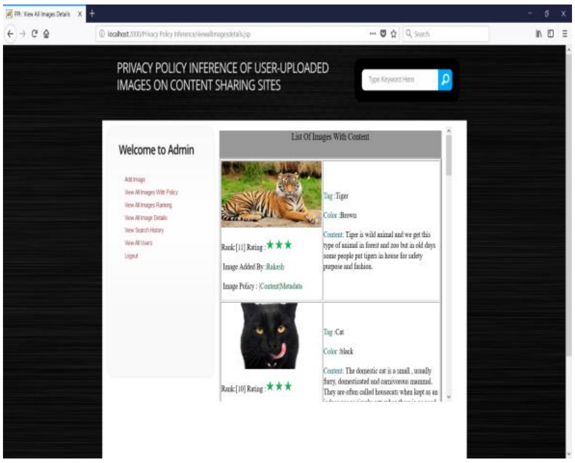
Rank:[11] Rating :★★★
Image Added By :Rakesh
Image Policy : ContentMetadata

Rank:[10] Rating :★★★
Image Added By :raju
Image Policy :All

Rank:[10] Rating :★★★

Rank:[9] Rating :★★★

Administrator: View All Image Details


PPI : View All Images Details
localhost:2000/Privacy Policy Inference/viewallimagesdetails.jsp
Search
Type Keyword Here
Add Image
View All Images With Policy
View All Images Ranking
View All Image Details
View Search History
View All Users
Logout

PRIVACY POLICY INFERENCE OF USER-UPLOADED IMAGES ON CONTENT SHARING SITES

Welcome to Admin

List Of Images With Content

Rank:[11] Rating : ★★★

Image Added By :Rakesh

Image Policy : |Content|Metadata

Tag :Tiger

Color :Brown

Content: Tiger is wild animal and we get this type of animal in forest and zoo but in old days some people put tigers in house for safety purpose and fashion.

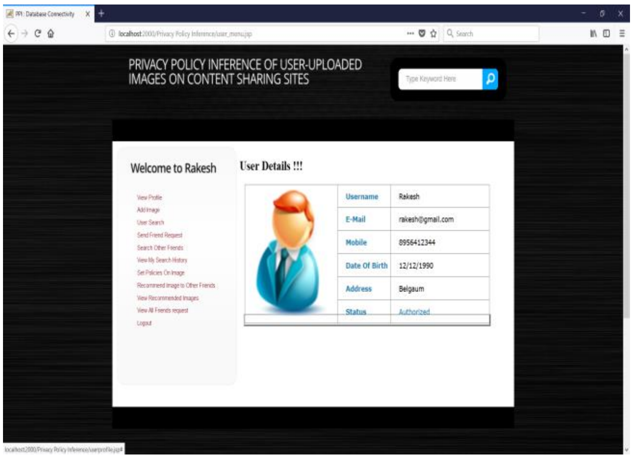
Rank:[10] Rating : ★★★

Tag :Cat

Color :black

Content: The domestic cat is a small , usually furry, domesticated and carnivorous mammal. They are often called housecats when kept as an

1. User: View Profile



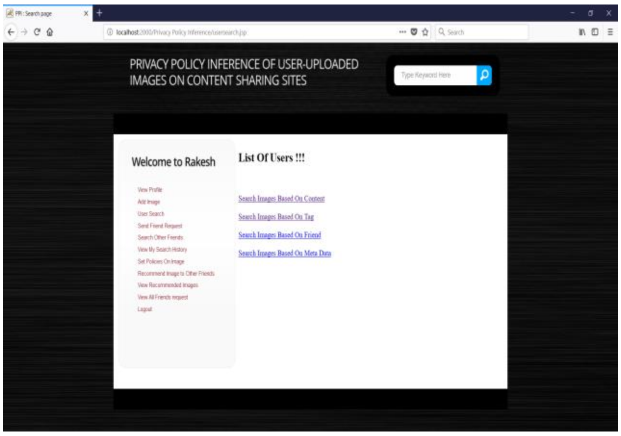
PRIVACY POLICY INFERENCE OF USER-UPLOADED IMAGES ON CONTENT SHARING SITES

Welcome to Rakesh

User Details !!!

Username	Rakesh
E-Mail	rakesh@gmail.com
Mobile	8956412344
Date Of Birth	12/12/1990
Address	Belgaum
Status	Authorized

2. User: Search Images based on Content / Tag / Friend / Meta Data



PRIVACY POLICY INFERENCE OF USER-UPLOADED IMAGES ON CONTENT SHARING SITES

Welcome to Rakesh

List Of Users !!!

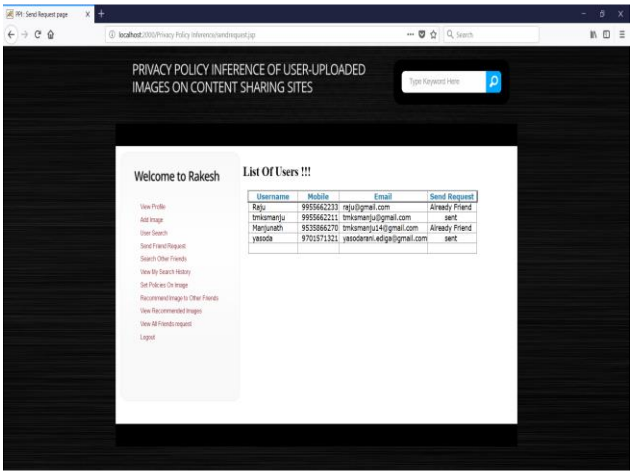
Search Images Based On Content

Search Images Based On Tag

Search Images Based On Friend

Search Images Based On Meta Data

3. User: Send friend request



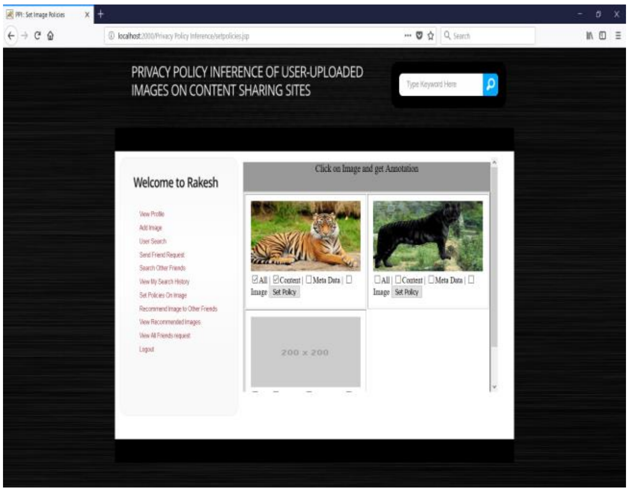
PRIVACY POLICY INFERENCE OF USER-UPLOADED IMAGES ON CONTENT SHARING SITES

Welcome to Rakesh

List Of Users !!!

Username	Mobile	Email	Send Request
Raju	9955662233	raju@gmail.com	Already Friend
tmksmanju	9955662211	tmksmanju@gmail.com	sent
Manjunath	9535866270	tmksmanju14@gmail.com	Already Friend
yasoda	9701571321	yasodarani.ediga@gmail.com	sent

User: Set Policies on Image



PRIVACY POLICY INFERENCE OF USER-UPLOADED IMAGES ON CONTENT SHARING SITES

Welcome to Rakesh

Click on Image and get Annotation

☑All | ☑Content | ☐Meta Data | ☐ Image

☐All | ☐Content | ☐Meta Data | ☐ Image

CONCLUSION

I have proposed an Adaptive Privacy Policy Prediction (A3P) framework that enables clients to robotize the privacy policy settings for their transferred images. The A3P framework gives an exhaustive structure to gather privacy inclinations dependent on the information accessible for a given client. We likewise viably handled the issue of chilly begin, utilizing social setting information. My trial ponder demonstrates that our A3P is a pragmatic instrument that offers noteworthy enhancements over current ways to deal with privacy.

REFERENCES

[1] A. Acquisti and R. Gross, "Imagined communities: Awareness, information sharing, and privacy on the facebook," in Proc. 6th Int. Conf. Privacy Enhancing Technol. Workshop, 2006, pp. 36–58.

[2] R. Agrawal and R. Srikant,"Fast algorithms for mining association rules in large databases," in Proc. 20th Int. Conf. Very Large Data Bases, 1994, pp. 487–499.

[3] S. Ahern, D. Eckles, N. S. Good, S. King, M. Naaman, and R. Nair, "Over-exposed?: Privacy patterns and considerations in online and mobile photo sharing," in Proc. Conf. Human Factors Comput. Syst., 2007, pp. 357–366.

[4] M. Ames and M. Naaman, "Why we tag: Motivations for annotation in mobile and online media," in Proc. Conf. Human Factors Comput. Syst., 2007, pp. 971–980.

[5] A. Besmer and H. Lipford, "Tagged photos: Concerns, perceptions, and protections," in Proc. 27th Int. Conf. Extended Abstracts Human Factors Comput. Syst., 2009, pp. 4585–4590.

[6] D. G. Altman and J. M. Bland ,"Multiple significance tests: The bonferroni method," Brit. Med. J., vol. 310, no. 6973, 1995.

[7] J. Bonneau, J. Anderson, and L. Church, "Privacy suites: Shared privacy for social networks," in Proc. Symp. Usable Privacy Security, 2009.

[8] J. Bonneau, J. Anderson, and G. Danezis, "Prying data out of a social network," in Proc. Int. Conf. Adv. Soc. Netw. Anal. Mining., 2009, pp.249–254.

[9] H.-M. Chen, M.-H. Chang, P.-C. Chang, M.-C. Tien, W. H. Hsu, and J.-L. Wu, "Sheepdog: Group and tag recommendation for flickr photos by automatic search-based learning," in Proc. 16th ACM Int. Conf. Multimedia, 2008, pp. 737–740.

[10] M. D. Choudhury, H. Sundaram, Y.-R. Lin, A. John, and D. D. Seligmann, "Connecting content to community in social media via image content, user tags and user communication," in Proc. IEEE Int. Conf. Multimedia Expo, 2009, pp.1238–1241.

[11] L. Church, J. Anderson, J. Bonneau, and F. Stajano, "Privacy stories: Confidence on privacy behaviors through end user programming," in Proc. 5th Symp. Usable Privacy Security, 2009.

[12] R. da Silva Torres and A. Falc~ao, "Content-based image retrieval: Theory and applications," Revista de Inform_atica Te_orica e Aplicada, vol. 2, no. 13, pp. 161–185, 2006.

[13] R. Datta, D. Joshi, J. Li, and J. Wang, "Image retrieval: Ideas, influences, and trends of the new age," ACM Comput. Surv., vol. 40, no. 2, p. 5, 2008.

[14] J. Deng, A. C. Berg, K. Li, and L. Fei-Fei, "What does classifying more than 10,000 image categories tell us?" in Proc. 11th Eur. Conf. Comput. Vis.: Part V, 2010, pp. 71–84. [Online]. Available: http:// portal.acm.org/citation.cfm?id=1888150.1888157

[15] A. Kapadia, F. Adu-Oppong, C. K. Gardiner, and P. P. Tsang, "Social circles: Tackling privacy in social networks," in Proc. Symp. Usable Privacy Security, 2008

[16] Squicciarini, Anna Cinzia, et al. "A3p: adaptive policy prediction for shared images over popular content sharing sites." Proceedings of the 22nd ACM conference on Hypertext and hypermedia. ACM, 2011.

[17] Bonneau, Joseph, and Sören

Preibusch. "The privacy jungle: On the market for data protection in social networks." Economics of information security and privacy. Springer, Boston, MA, 2010. 121-167.