ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

Secure User Data and Images on Content Sharing Sites Using Virtual Password and APP Scheme

Priyanka M. Lokhande

Post Graduate Student, Dept. of Information Technology, RMDSSOE Warje, Savitribai Phule Pune University, Pune, India

ABSTRACT: Data especially images sharing on social networking sites like Facebook, Instragram, etc. becoming very much popular now days. Social networking users will upload various images including personal images on social networking sites with some captions and related messages. Such upload images needs accessing privacy policy set to secure image access by other social networking users. The developed application will take care of uploaded image for sharing on social networking site by recommending different accessing policies which are defined as per image classification. An image classification framework for image categories which is correlated with similar policies to automatically produce a policy for each newly updated image, also according to users social features. The policy formation is also considered caption and any message related with image. The policy recommendation system implemented is named as APP. For security of shared image, application will implement one to one encryption policy such that only the user to whom image is shared is able to view it. The auto-vanish technique is also implemented in developed application which auto-deleted shared image after expiration of set period time. Also to secure users access to social networking site, virtual password mechanism is implemented which gives user to set a secure password by set of random clicks on user selected images which improves security.

KEYWORDS: Privacy, social networks, affiliation networks, personalization, protection mechanisms, privacy risk.

I. INTRODUCTION

Mobile Access Privacy Policy Scheme provide technique to a comprehensive review of various privacy policy approaches for sharing image in the social media sites. When user uploaded an image, for access policy recommendation such that share policy generation factors considered such as Meta data information of image, User behavior, Image Content and profile based. One to one encryption of shared image improves the security as no one other able to view shared image. A virtual password mechanism in which a user can get freedom to select a virtual password scheme which is ranging from weak security to strong security.

User's passwords from being stolen by adversaries in online environments and automated teller machines. With the increasing volume of images users share through social sites, maintaining privacy has become a major problem. As demonstrated by a recent wave of publicized incidents where users inadvertently shared personal information. In light of these incidents, the need of tools to help users control access to their shared content is apparent. Toward addressing this need, proposed system to help users compose privacy settings for their images.

The purpose of implemented application is to provide a strong authentication security which is been implemented using virtual password mechanism. Also the application is implemented to provide access and sharing security for sharing contents like images and documents on social networks.

In this proposed system evidence are created like virtual password and access privacy policy. Application is to provide a strong authentication security which is been implemented using virtual password mechanism. Also the application is implemented to provide access and sharing security for sharing contents like images on social networks. How this evidence work and on the basis of this how their policies are changes on the images on content sharing sites, this technique motivate me to done this project.

DOI: 10.15680/IJIRCCE.2017. 0506059

II. RELATED WORK

Vanitha.A, Magentharan.N. uses a differentiated virtual password mechanisms [1], in which a user has the freedom to choose a virtual password scheme ranging from weak security to strong security, where a virtual password requires a small amount of human computing to secure users passwords. A system using color Scheme authentication which aims to provide users a hassle free privacy settings experience by automatically generating personalized policies. Anna Cinzia Squicciarini developed an Adaptive Privacy Policy Prediction (A3P) system [2], a free privacy settings system by automatically generating personalized policies. The A3P system handles user uploaded images based on the person's personal characteristics and images content and metadata. The A3P system consists of two components: A3P Core and A3P Social. When a user uploads an image, the image will be first sent to the A3P-core. The A3P-core classifies the image and determines whether there is a need to invoke the A3P-social. Klemperer et al.[3] studied whether the keywords and captions with which users tag their photos can be used to help users more intuitively create and maintain access control policies. Their findings are in line with our approach: tags created for organizational purposes can be repurposed to help create reasonably accurate access-control rules. Peter F. Klemperer developed a tag based access control of data shared in the social media sites. A system that creates access-control policies from photo management tags. Every photo is incorporated with an access grid for mapping the photo with the participant's friends. The participants can select a suitable preference and access the information. Photo tags can be categorized as organizational or communicative based on the user needs. There are several important limitations to our study design. First, our results are limited by the participants we recruited and the photos they provided. A second set of limitations concerns our use of machine generated access-control rules. The algorithm has no access to the context and meaning of tags and no insight into the policy the participant intended when tagging for access control. As a result, some rules appeared strange or arbitrary to the participants, potentially driving them toward explicit policy-based tags like private and public. Sergej Zerr uses a technique Privacy-Aware Image Classification and Search [4] to automatically detect private images, and to enable privacy-oriented image search. It combines textual Meta data images with variety of visual features to provide security policies. In this the selected image features (edges, faces, color histograms) which can help discriminate between natural and man-made objects/scenes (the EDCV feature) that can indicate the presence or absence of particular objects(SIFT). It uses various classification models trained on a large scale dataset with privacy assignments obtained through a social annotation game. Alessandra Mazzia introduced PViz Comprehension Tool [5], an interface and system that corresponds more directly with how users model groups and privacy policies applied to their networks. Such groupings are not always explicit and existing policy comprehension tools which allow the user to understand the visibility of her profile according to automatically constructed, natural sub- groupings of friends, and at different levels of granularity. Because the user must be able to identify and distinguish automatically-constructed groups, also address the important sub-problem of producing effective group labels. PViz is better than other current policy comprehension tools Facebooks Audience View and Custom Settings page.

III. PROPOSED SYSTEM ARCHITECTURE

The objective of Virtual Password and APP Scheme is generate a password using some images as a source of virtual password to quickly and efficiently provide users a hassle free privacy settings experience by automatically generating personalized policies. The project will be implemented using web based application. Project contains mainly two modules:

A. *Virtual Password in registration and login*

Virtual passwords are an authentication mechanism for computer systems. The difference between a Virtual passwords and the currently dominant alphanumeric password is that with a Virtual passwords, a user's password is represented by where that user clicks on an image. Thus, an application using Virtual passwords for authentication would show a picture to the user. The user would then click in a number of places on the picture, and the coordinates of the clicks would be stored by an application. During authentication, the user has to click on the established points. Another benefit of graphical passwords is the cued-recall, which helps users to remember a password based on the picture displayed, and not just on memory alone. In application, virtual password authentication system is used in registration and then in login. Application shows a grid of images to user and then user have to generate password from clicks on an images. User can able to click any times and randomly on images. Password generated is hidden from user and hence he/she must have to memorize the click sequence of clicks on images.

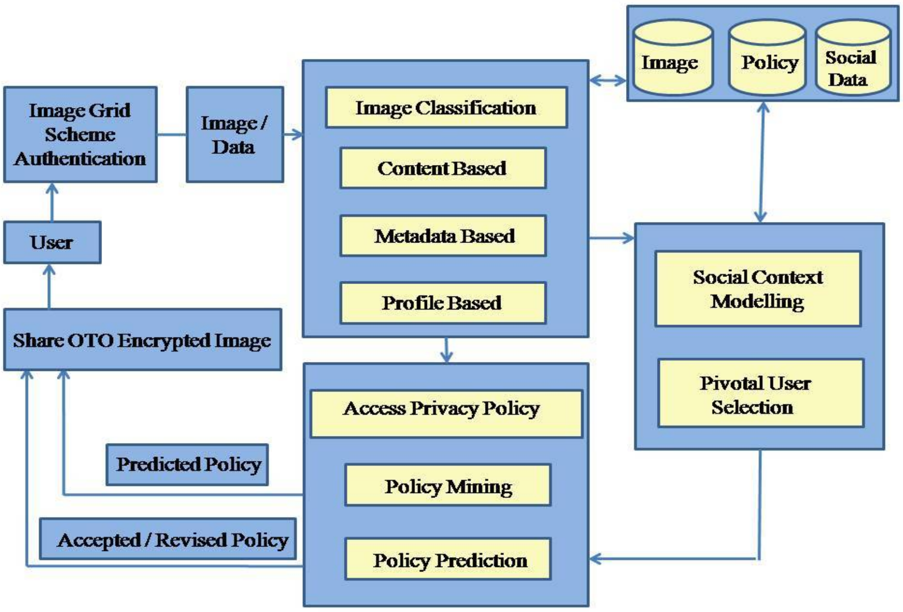

Fig. Proposed System Architecture

B. ***Access Privacy Policy(APP)Scheme***

For access policy recommendation such that share policy generation, following factors will be considered. These factors are;

- **Image uploads for sharing**

The application is act at social networking site where user can upload images for sharing with friends. User can able to add tag line and message with an image for sharing. The uploaded image will go through image pre-processing and according to image class, contents and metadata information; image sharing access policies are generated. The access policies are generated by processing image under different modules and then at final, policy mining is executed and generated policies are suggested to user. User will accept required policies and share image with friend.

The sharing data including image, tag line and message, are all get one to one such that end to end encrypted. One to one encryption is implemented using AES encryption in which encryption is auto generated and maintained with sharing automatically. User need to enter any encryption key while uploading and sharing images. Also, during viewing of an image, entry of encryption key by use is not required.

- **Access shared image**

The image uploads for sharing module is undergoing processing by different sub modules as enlisted below;

1. Profile - face based policy forming

These module looks for any present of face in an image. If uploaded image contains any face then finding out corresponding profile face match. The application will generate a policy with respect to profile face match found.

2. Image contents - whether image contains vehicles or persons or any else

These module looks for image contents in terms of what exactly image will contains such that presence of any kind of vehicle or human being in an image. Or none of these present in an image. Image is categorized accordingly.

3. Image metadata information

Image metadata information is nothing but soft information available with an image. This information contains, image make, whether these image is pictured or downloaded. Whether these image is owned or copyrighted or not, etc.

The making date of an image which helps in understanding oldness of an image. These help in generate metadata based access policies for an image.

4. Is image contains plain text (ex. document scanned type images) or not?

These modules find out whether image is a textual image or graphical image. Textual image is nothing but an image which contains any textual information or any advertising text in an image. If module didn't find any text, then image is considered as graphical image.

5. Image tags, message related with image

Tags are a tag-line given to shared image while message is nothing but text about an image or message to a friend to whom image is going to share. Both these textual information is used to generate image category depending upon text associated with an image. Depending upon above defined image processing, image category is finalized and corresponding image sharing access policy is generated. Each sub modules will give image category depending upon image processing result.

6. Policy accepted history (User behavior) for similar class images

After generating image sharing access policies, a previous image sharing record is searched for similar class image shared records. The image sharing history is retrieved for similar class images and selected sharing access policies are appended with currently generated sharing access policies.

- **Policy mining from all above steps and present to user**

Policy mining is nothing but finalizing image sharing access policies from all above policies and image categories which are formed after image processing in different modules. These will mine all policies and make them presentable to user. Image sharing policies are normally contains policies like view, like, comment, share and download. These policies are clustered together in different groups depending upon image category which is find out processing image by different modules as mentioned above. Also these sharing policies are clustered with user profile if any match of user profile found in an image.

- **Apply policy to shared image as per user selection**

Policy mining module will present mined policies to user. Then user have to select policies from given generated policies as per his/her choice. The selected policy or policies are applied on an image and then shared with friend. The shared image and corresponding applied policies are stored in a record.

- **Encrypt image and corresponding contents**

The uploaded image and corresponding tag line and message such that textual data undergoes encryption. The AES encryption is implemented to encrypt image and other textual data. The encryption is implemented to achieve one to one such that ends to end encryption. This is done by using system generated keyword which is maintained by an application. User need to worry about any kind of encryption key.

IV. Mathematical Module

Mathematical description of modules Virtual Password, APP Scheme and One to One Encryption is explain as follows,

A. *Mathematical module for Virtual Password*

The image in virtual password contains Data grid of image, DG[I] (I = Image for virtual password) Where each data grid will contains eight columns and eight rows having random characters or digits in each cell,

$$DG\{x, y\} = \{[x_0,y_0],[x_0,y_1],[x0,y_2],\ldots,[x_1,y_0],[x_1,y_1],[x1,y_2],\ldots.,[x_7,y_7]\} \qquad (1)$$

This data grid will be different for each image in a virtual password which will be given as; DG[I1], DG[I2], DG[I3] and DG[I4] (I1 to I4 = four images for virtual password) The click on random cells in virtual password images will generate password

$$PASSWORD = \{DG[I1] + DG[I2] + DG[I3] + DG[I4]\} \qquad (2)$$

From equation [1] and [2],

PASSWORD = $\sum_{I=0}^{7}(DG)x^{0-7}y^{0-7}$ (3)

Equation three will give generated equation which will be sent to server to save in database.

B. *Mathematical module for APP*

The policy will be defined as per image metadata, user behaviour and image content. Metadata information of User Image (UI) will contains Tags and Captions MD(UI) = T +C. Nouns from metadata will be extracted and collected in a variable MD^{Nouns}

$MD(UI)^{Nouns} = \{T_{Nouns}(t_0, t_1, t_2, \dots, t_n) + C_{Nouns}(C_0, C_1, C_2, \dots, C_n)\}$ (1)

From above equation, share policy based metadata will be generated

$SP_{MD} = ANA(MD(UI)^{Noun}$ (2)

User behaviour means the share log of user generated for previous shared images UB = $\sum_{I=0}^{n}(SL)$ for images shared 0 to n. From this user behaviour share logs, the share policy based user behaviour for user uploaded image will be analysed,

$SP_{UB} = ANA(UB)$ (3)

Image content will be include the image properties, description and actual image contents data including profile face present in image if any.

Image properties are given by equation

PROP(UI) = RGB(UI) + BRIT(UI) + CONT(UI) (4)

RGB give colour information of user image, BRIT give brightness information and CONT contrast information of image. Image description will be given by equation

DESC(UI) = SIZE(UI) + TIMESTAMP(UI) + OWNER(UI) (5)

Image data will be given by equation

DATA(UI) = FACE(UI) + VECH(UI) + OTHR(UI) (6)

Where,

FACE(UI) = Find any face if present and match it with profile face of other users. If (FACE(UI)=PROFILE(User)) Then,

DATA(UI) = DATA (UI) + PROFILE(User)

This will gives faces and/or vehicles and/or other detectable information in a user image.

From above equations (a), (b) and (c), image contents will be formed as

CONT(UI) = PROP(UI) + DESC(UI) + DATA(UI)

From above equation, share policy based image contents will be generated;

$SP_{CONT} = ANA(CONT)$ (7)

From equations (2), (3) and (7)

$SP(APP) = SP_{MD} + SP_{UB} + SP_{CONT}$

Above equation will give APP share policy.

C. *Mathematical module for One to One encryption*

One to one encryption uses the user id of a user as an encryption key,

Encryption key Ek = ID(User)

Data_To_Encrypt=Bytes(Data_to_Share)

Where, Data_To_Encrypt = Data to be share by user which includes image, and any tags, message with an image. Each of these is compared as individual for an encryption

Encrypted_Bytes=Data_To_Encrypt + Ek

Where,

Encrypted_Bytes = Encrypted data.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

V. Simulation Results

In this, compare the APP core with two variants of itself, in order to evaluate the contribution of each component in the APP made for privacy prediction. The first variant uses only content-based image classification followed by our policy mining algorithm, denoted as "Content+Mining". The second variant uses only tag classification followed by the policy mining, denoted as "Tag+Mining".

Table.1. Policy Performance Analysis

Match	APP	Content+Mining	Tag+Mining	Mining Only	Classification Only
Exact Match 2-	92	84	62	50	39
Component Match 1-	13	19	23	36	41
Component Match	6	13	17	26	30
No Match	0	5	9	15	20

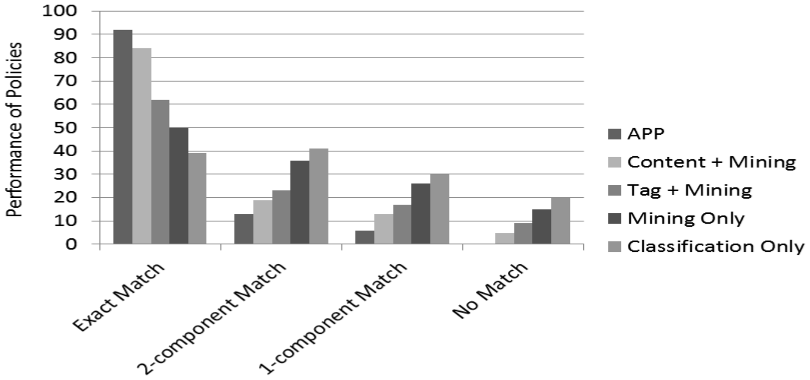

Fig. 2. Policy Performance Analysis Graph

The percentage of predicted policies in four groups: "Exact Match" means a predicted policy is exactly the same for the same image; "x-component Match" means a predicted policy and its corresponding real policy have x-components (i.e., subject, action, condition) fully matched; "No match" simply means that the predicted policy is wrong for all components. As shown in the figure, each component of the APP singularly contributes toward policy prediction, however, none of them individually equalizes the accuracy achieved by the APP in its entirety.

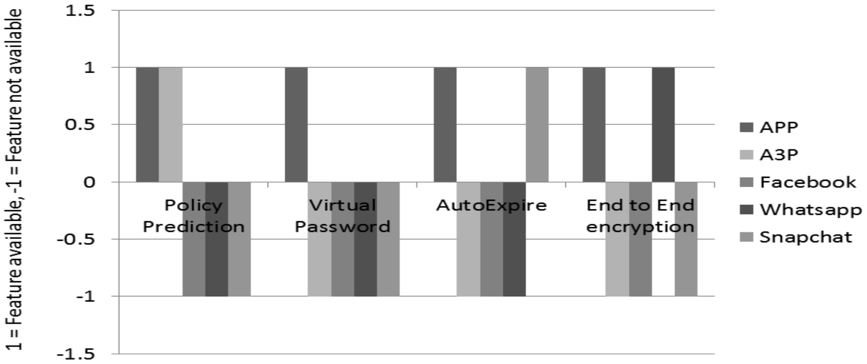

Fig. 3. Features Comparison Graph

Features comparison graph compares different features of an application with existing image sharing application websites. The graph indicates +1 unit for availability of a feature and -1 unit if feature is not available with an application. The application developed has most features under one application which are not collectively available in any other application. The policy prediction is a feature which gives better result as compared to A3P application. Virtual password system is not available with any other of image sharing website applications. Also auto expose is a functional feature which was unique feature of developed application. All these concluded that the developed application is most secure and advanced image sharing website application.

VI. CONCLUSION

This project is undertaken to design privacy policy techniques for user uploaded data images in various content sharing sites and evaluate a virtual password mechanism in which a user can get freedom to select a virtual password scheme which is ranging from weak security to strong security. Also, this work introduces one to one encryption scheme which ensures sharing of images and other contents with authorized person only. The auto-expire mechanism applied by image owner on image gives security to image by auto-vanishing the image and related texts in a time period set by user.

This study has found that generally a system having a new perspective on content sharing in social sites to improve the security of information shared in the social media sites with one to one encryption.

VII. ACKNOWLEDGMENT

I would like to express my gratitude towards Miss. Pratibha Chavan for their persistence guidance throughout the project. I would like to thank Mr. D. A. Meshram for their constructive criticism and Mrs.Sweta Kale for their valuable support.

REFERENCES

1. Vanitha.A, Magentharan.N. , "An Improved Privacy Policy Inference Over The Socially Shared Images In Social Websites," IRJAET , Vol. 2, Issue 1, 2016.
2. Anna Cinzia Squicciarini, Dan Lin, Smitha Sundareswaran, and Joshua Wede, "Privacy Policy Inference of User-Uploaded Images on Content Sharing Sites", IEEE Transactions on Knowledge and Data Engineering, Vol. 27, January 2015.
3. P. Klemperer, Y. Liang, M. Mazurek, M. Sleeper, B. Ur, L. Bauer, L. F. Cranor, N. Gupta, And M. Reiter, "Tag, You Can See It!: Using Tags For Access Control In Photo Sharing", In Proc. ACM Annu.Conf. Human Factors Comput. Syst., 2012.
4. S. Zerr, S. Siersdorfer, J. Hare, And E. Demidova, "Privacy-aware Image Classification And Search", In Proc. 35th Int. ACM SIGIR Conf. Res. Develop. Inform. Retrieval, Pp. 3544, 2012.
5. A. Mazzia, K. LeFevre, and A. E., "The PViz comprehension tool for social network privacy settings", in Proc. Symp. Usable Privacy Security, 2012.
6. J. Bonneau, J. Anderson, and L. Church, "Privacy suites: Shared privacy for social networks", in Proc. Symp. Usable Privacy Security, 2009.
7. J. Yu, D. Joshi, and J. Luo, "Connecting people in photo-sharing sites by photo content and user annotations", in Proc. IEEE Int.Conf. Multimedia Expo, pp.14641467, 2009.
8. 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.
9. K. Lerman, A. Plangprasopchok, and C. Wong, "Personalizing image search results on flicker", CoRR, vol. abs/0704.1676, 2007.