

PAPER • OPEN ACCESS

## Security policy speculation of user uploaded images on content sharing sites

To cite this article: M Iyapparaja and Maneesh Tiwari 2017 *IOP Conf. Ser.: Mater. Sci. Eng.* **263** 042019

View the [article online](#) for updates and enhancements.

### Related content

- [Quo Vadis Quantum Mechanics?](#)  
W G Unruh
- [Some speculations on the critical exponents and fractal dimensionalities relevant to realistic spin glasses](#)  
A Mookerjee
- [Lifshitz-point critical behaviour to  \$O\(2\)\$](#)   
H W Diehl and M Shpot

### Recent citations

- [Effective Feature Selection Using Hybrid GA-EHO for Classifying Big Data SIoT](#)  
Iyapparaja M and Deva Arul S
- [M. Iyapparaja et al](#)
- [Active contour with modified Otsu method for automatic detection of polycystic ovary syndrome from ultrasound image of ovary](#)  
C. Gopalakrishnan and M. Iyapparaja



**ECS** **240th ECS Meeting**  
Oct 10-14, 2021, Orlando, Florida

**Register early and save up to 20% on registration costs**

Early registration deadline Sep 13

**REGISTER NOW**

# Security policy speculation of user uploaded images on content sharing sites

**Iyapparaja M and Maneesh Tiwari**

School of Information Technology and Engineering, VIT University, Vellore-632014, Tamil Nadu, India.

E-mail: iyapparaja85@gmail.com

**Abstract.** Innovation is developing step by step tremendously. As there are numerous social locales where information likes pictures, sound, video and so forth are shared by the client to each other. In concentrate to all exercises on social locales, there is need of protection to pictures. Because of this reason, I utilized Adaptive protection strategy forecast instrument to give security to the pictures. Issue identified with pictures is the huge issue in social locales like Facebook, twitter and so on. So here the part of a social thought, security to pictures, metadata and so on is produced. To conquer this issue we produced an answer which is 2 systems which understanding to a background marked by the pictures gives appropriated answer for them. Here we give an arrangement to the specific sort of pictures by characterizing them and in addition giving protection to pictures which are transferred agreement to a calculation that we utilized. Consequently as indicated by this arrangement expectation pictures take after a similar approach on up and coming pictures and give successful security to them.

## 1. Introduction

As we probably am aware web is two route correspondences in which separate and customer associate for correspondence. Here there are loads of social locales which give office to impart each other and offer their data, for example, pictures, sound, information and some more. Be that as it may, in the greater part of this security is the measure concern. So it is critical to give security to data that is shared by the clients on the web. For example on the off chance that somebody needs to share his/her children pictures on social locales then he/she need to set security as observed by just relatives as it were. Other than this on the off chance that he/she need to share his/her own day by day interest or typical routine pictures then protection can be situate as ordinary. So understanding to need one can fluctuate his/her security status. So contemplating on comparable conduct of picture is insufficient. Other than the greater part of this one tag on pictures might be of various areas require likewise protection, that why one can't decide security agreement to the specific conduct. So propel security inclinations are required. Greater part of this client who utilizing social substance sharing sites having some association with specific clients that additionally demonstrate their security need and as indicated by that need everything is revamped. Let's take a case a man clicked a few pictures in parties where the two his/her family, companions and office companions are additionally there. So there on



the off chance that he sharing photographs by labeling them from which some photographs are identified with various gatherings. So to defeat this one can set his/her security need and can send photographs to various gatherings person. In this condition one can share substance understanding to ones intrigue and security alternative gave in that specific social substance sites. In our framework we proposed a framework through which one can utilize his/her propel rendition of picking security for various sorts of gatherings or diverse sorts of photographs. There are different innovation utilized as a part of my venture to give security to the clients in which while sending and acknowledge one can choose their arrangement, connection and gathering so that can give security to the clients of the specific substance sharing site. If there should arise an occurrence of Facebook, twitter and numerous more substance sharing social sites concern is of security of information when it is shared between various clients. So to deal with this circumstance or conquer this circumstance we gave a secured approach to share substance to each other on greater security premise.

It is work on the algorithm called Adaptive privacy policy predication(APPP) which provides security to the user content on the basis of some algorithm like pattern matching of similar type of action performed by the user and different types of policy selected by the users. Here this APPP algorithm works on 2 framework policy names as follows:

### *1.1. APPP-Core*

APPP-core works on the users individual information like images, data and many more and study their behavior and provide privacy accordance to that. This is works on content and metadata based of the particular images.

### *1.2. APPP-Social*

APPP-social completely works on the mechanism of social context. In social context all the information related to social is analyzed accordance to some pattern.

## **2. Literature Review**

In 2014, Acquisti and Gross are said that, there are various social websites like Facebook. Flickr, twitter and many more gain publicity in short period of time and very popular in this current era. But other than all of this there is problem that they are not effective and efficient in providing security and privacy to the images that are shared or uploaded on this type of social sites. In this paper they done survey in a college of Us where they encountered a problem that social websites which are available on the web is not so privacy effective and if there is privacy that is more complex.

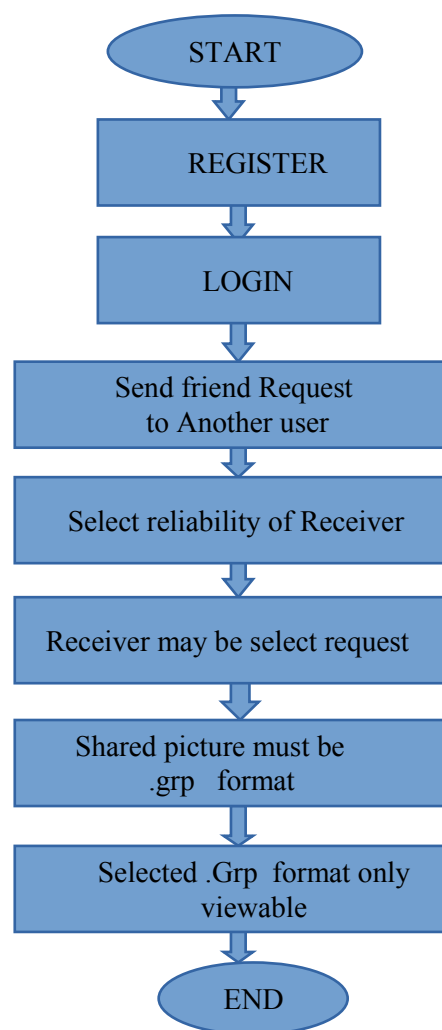
If there is large data then that time we required large database to efficient and effective storage of whatever data on that we are working on. Like Agrawal and Srikant are modified algorithm in the year 2015 and which is not effective for that purpose managing large file storage. And we are having one more algorithm with some effective properties. So in this paper it is discussed that if you have two ideas of algorithm then you can combine both of these algorithms.

In why we tag: Motivations for annotation in mobile and online media paper of year 2014, it is focusing on topic that why people tag others people on their camera photo or on their posts. As this is the way through which image privacy concern is going to arise. As Zone tag is technology that is used by various content based social sites like facebook and many more. As in this paper authors completed study by conducting survey about various types of behaviour of peoples while tagging like some are friends, some tag non friends also who are new and are in the photos. So when this type of situation arises this lead to concern of image privacy.

In 2015, A. Besmer and H. Lipford fully discussed on the concerns and possible protection related to privacy of images. Here in this paper concerns like someone who can viewing images, sharing images, downloading and many more are the main reason so need of all privacy or security to images are arise. To overcome this situation in this paper various suggestion and ways are discussed through which one can tackle or handle that situation.

### 3. Methodology

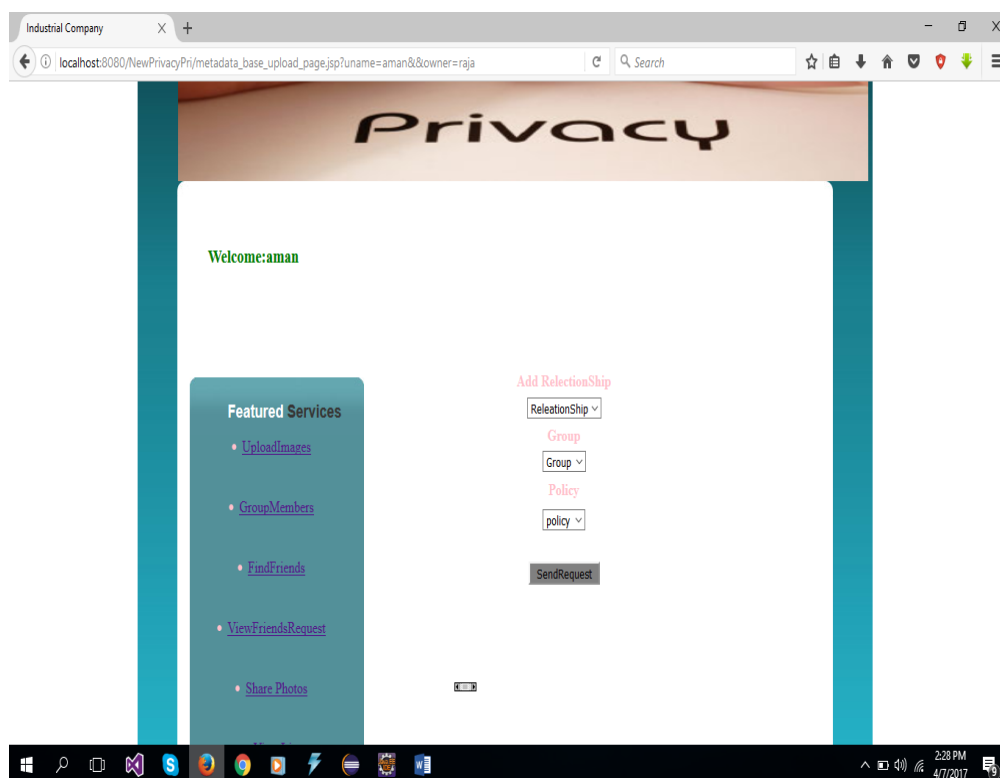
#### 3.1 Schematic of proposed System



**Figure 1. System flow**

In the above figure 1 shows, how flow of this procedure goes on. It starts with sending request till only selected group can only view the images.

In this paper, we applied algorithm known as Adaptive privacy policy predication algorithm (APPP). As we seen now there is bunches of social destinations which is not ready to give quality security to the substance like pictures, sound and video and some more. So to deal with this circumstance we can a more secure and powerful application in required that defeat all the disadvantage of others social substance sites like Facebook and some more. For instance: on the off chance that we need to share photographs identified with family and in the event that we need that other won't see that photograph then we require a viable strategy identified with it. In our framework we took after two sorts of arrangement as social and center. This word on 2 system versatile strategy predication calculation. Here while sending demand from one to other sender need to pick arrangement, relationship to the accompanying individual like family, companion, office and others. Different this one need to pick aggregate too. In the wake of doing the majority of this one need to pick primary concern strategy like we are sending to the specific individual as a center or social. And keeping in mind that tolerant to whom we are sending likewise need to pick like individual who is sending demand is our companion or relative, since as indicated by our decision just security strategy on pictures works. Time of transferring or sending pictures it is seen understanding to the security that we give to the specific client.



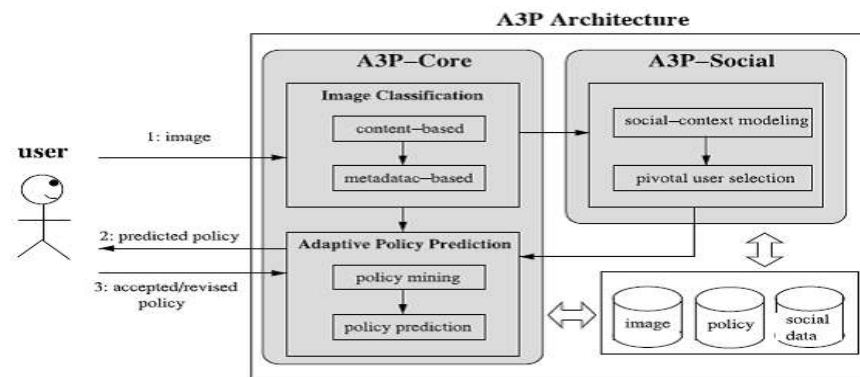
**Figure 2. Privacy system**

In Figure 2 shows some that how while sending or accepting request user have to set their preference and according to that preference and pattern in future image privacy works.

### 3.2 APPP System

In APPP System when user going to sends a request user have to mention relation and privacy policy as a core or social. If it is core then image is classified accordance to the content and metadata that is connected to particular content. And according to this process when image uploaded it provides security. After this it is stored in database which follows mining mechanism which takes some pattern

for images that going to upload and provide privacy to the images. Social works on context based modeling like it not focus on particular images it going to treat all social images as same. Here pattern is not created and this is less privacy efficient compare to core policy.



**Figure 3. APPP Architecture**

### 3.3 Image classification

Image classification plays a vital role to provide security to the user. It is because according to the image pattern, content based or metadata based some pattern is going to set. And after that privacy to images is provided efficiently and effectively. So image classification is the important part of the architecture. All the process is depend on this also for providing security and accessing the data on content sharing sites.

### 3.4 Modules

#### 3.4.1 User Registration Login

User will register their profile into our system. Then admin provides login access. when user will log in their social media. And user conjointly desires to send friend request to the opposite existing user. That friend request has that person what's the link to send requester. that details requester should mention into that request. And another user will access or decline the request rely on the respondent would like.

#### 3.4.2 Image Classification

Here to get images with similar pattern we used a way which is hierarchical way of image classification. In which first image is going to classify accordance to the content of the images. After that image subcategory is taken as preference in which it is classify accordance to the content of the images. And if images metadata are not there then it is also possible to group it by its only content basis. So after that hierarchical classification of image it is classified. Other than all of this there is one possibility that images can also included in both content based and metadata based. So to overcome this we can store both of images in content or metadata category. We can tackle this problem by two ways one by classifying images according to their content.



### 4. Experiment and results

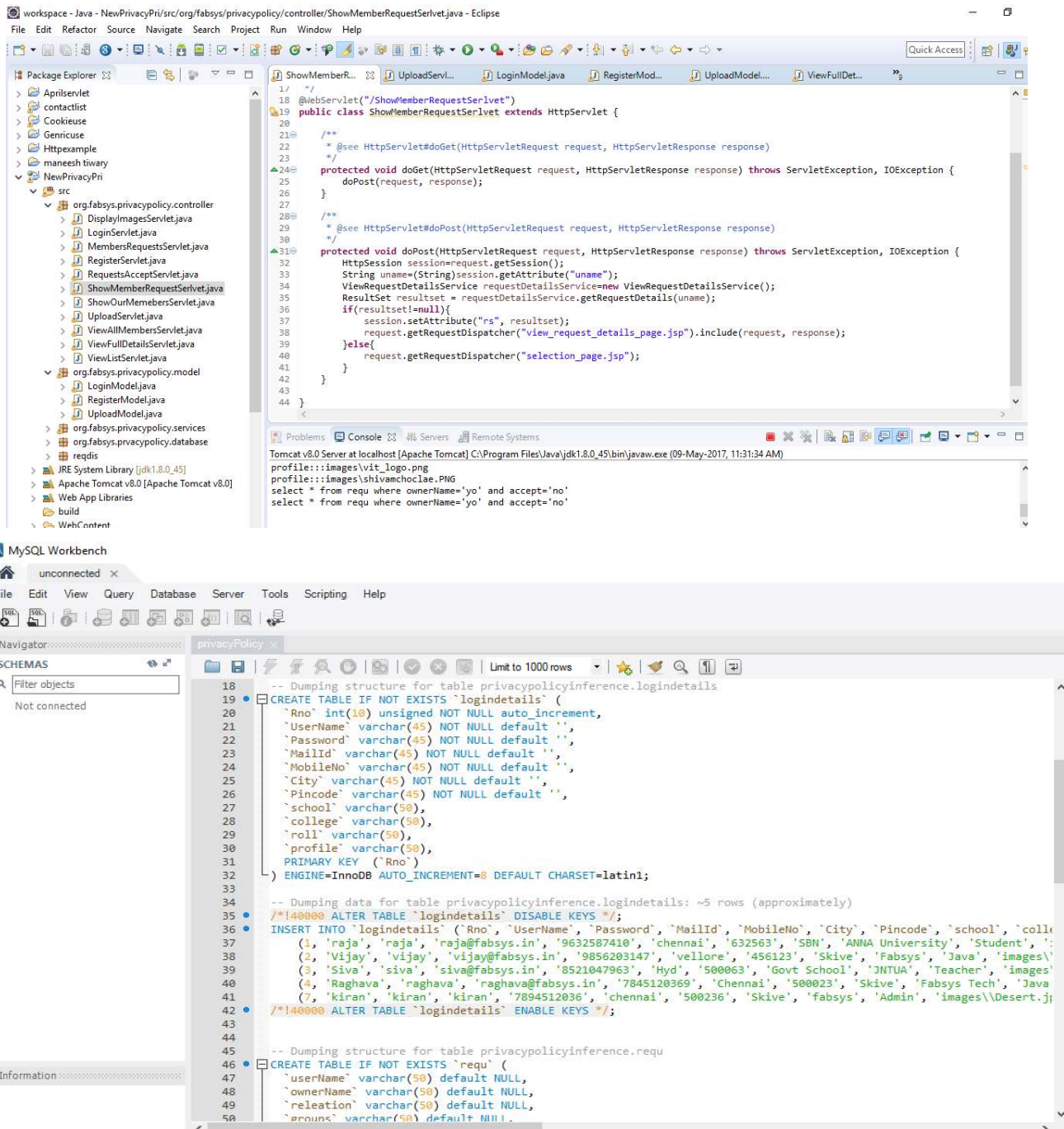


Figure 4. Program index page execution

After successful execution of program index page is project is open. In this page it contains the option like register, about our project, login. This project is works on the basis Adaptive privacy policy predication. In which we everything is implemented on the basis of giving privacy to the images. If a user is new he or she has to first register into the account by filling necessary detail regarding them. Username and password that he or she given in the project have to login into the project. Then profile

of that account is display. Here we can send request to the friend and accept it. But for this while accepting or sending request we have to set privacy. It works on privacy policy like core and social that option for the option that we have to choose. At end we can share any images keeping view of privacy of images. This is why everything is shared is more secured.

SENDING REQUEST			
USER	IMAGE PRIVACY GROUP	IMAGE PRIVACY POLICY	PRIVACY
1	FRIEND	CORE	STRONG
2	FAMILY	CORE	STRONG
3	OFFICE	SOCIAL	WEAK
4	OTHERS	SOCIAL	WEAK
ACCEPTING REQUEST			
USER	IMAGE PRIVACY GROUP	IMAGE PRIVACY POLICY	PRIVACY
1	FRIEND	SOCIAL	WEAK
2	FAMILY	CORE	STRONG
3	OFFICE	SOCIAL	STRONG
4	OTHERS	CORE	WEAK

**Figure 5. Sending and Accepting Request**

Here after selecting a relationship and group one should select privacy policy very careful. It is because according to that policy only privacy to the images and data in particular profile is provided. In figure 5, as we can see after selecting relation one can send and accept request. If privacy policy of sending request is core and accepted as core then it is very secure. In this condition, user image is shared then it only seen by the allowable user. If it is accepted as social then other person is not able to access and see images. This mechanism completely provides a effective security to the image that are uploaded. Either privacy policy is core and core or social and social other than this will not going to accept.

## 5. Conclusion

Here in our project we used a concept which provides more security to the user uploaded images. So to do so we used Adaptive privacy predication algorithm (APPP) which efficiently deals with images and provide them security? It is work on the concept of social and core. Here core is used to access each information and social is related to access information accordance to some particular privacy. Here other than this we use a particular patter which is used to differentiate particular images accordance to the algorithm. So by this privacy of images can be provided with an ease. So accordance



to all of whatever is shared is more securable and can give confidence to user. It is very simple and effective way of security.

## References

- [1] Agrawal R and Srikant R 2012 Fast algorithms for mining association rules in large databases *in Proc. 20th Int. Conf. Very Large Data Bases* 487–499
- [2] Bonneau J, Anderson J and Church L 2015 Privacy suites: Shared privacy for social networks *in Proc. Symp. Usable Privacy Security*
- [3] Ames M and Naaman M 2014 Why we tag: Motivations for annotation in mobile and online media *in Proc. Conf. Human Factors Comput. Syst.* 971–980
- [4] Acquisti A and Gross R 2006 Imagined communities: Awareness, information sharing, and privacy on the facebook *in Proc. 6th Int. Conf. Privacy Enhancing Technol. Workshop* 36–58.
- [5] Besmer A and Lipford H 2009 Tagged photos: Concerns, perceptions, and protections *in Proc. 27th Int. Conf. Extended AbstRisubcats Human Factors Comput. Syst.* 4585–4590
- [6] Altman D G and Bland J M 1995 Multiple significance tests: The bonferroni method *Brit. Med. J.* **310** 6973.
- [7] Iyapparaja M et.al 2012 Coupling and Cohesion Metrics in Java for Adaptive Reusability Risk Reduction *IET Chennai 3rd International Conference on Sustainable Energy and Intelligent Systems (SEISCON 2012) (624 CP)* 52-57
- [8] Bonneau J, Anderson J and Church L 2015 Privacy suites: Shared privacy for social networks *in Proc. Symp. Usable Privacy Security*
- [9] Bonneau J, Anderson J and Danezis G 2009 Prying data out of a social network *in Proc. Int. Conf. Adv. Soc. Netw. Anal. Mining* 249–254
- [10] Chen H M, Chang M H, Chang P C, Tien M C, Hsu W H and Wu J L 2008 Sheepdog: Group and tag recommendation for flickr photos by automatic search-based learning *in Proc. 16<sup>th</sup> ACM Int. Conf. Multimedia* 737–740