International Engineering Journal For Research & Development
Vol.4
Issue 5

E-ISSN NO:-2349-0721

Impact factor : 6.03

SECURED PHOTO SHARING IN WEB TECHNOLOGY

Narendra. M. Jathe
Department of Computer Science, Arts Commerce and Science College
Kiran Nagar Amravati, India
njathe@gmail.com

Abstract-

Sharing photos online is a common activity on social networks and photo hosting platforms, such as Facebook, Pinterest, Instagram, or Flickr. However, after reports of citizens surveillance by governmental agencies and the scandalous leakage of celebrities private photos online, people have become concerned about their online privacy and are looking for ways to protect it. Popular social networks typically offer privacy protection solutions only in response to the public demand and therefore are often rudimental, complex to use, and provide limited degree of control and protection. Most solutions either allow users to control who can access the shared photos or for how long they can be accessed. In contrast, in this paper, we take a structured privacy by design approach to the problem of online photo privacy protection. We propose a privacy-preserving photo sharing architecture that takes into account content and context of a photo with privacy protection integrated inside the JPEG file itself in a secure way. We demonstrate the proposed architecture with a prototype mobile iOS application called ProShare that offers scrambling as the privacy protection tool for a selected region in a photo, secure access to the protected images, and secure photo sharing on Instagram.

Keywords- Facebook, Pinterest, Instagram, Flickr, ProShare

I. INTRODUCTION

Photograph sharing is an alluring component which promotes Online Social Networks (OSNs). Shockingly, it might release clients' protection in the event that they are permitted to post, remark, and tag a photograph uninhibitedly. In this paper, we endeavor to address this issue and study the situation when a client shares a photograph containing people other than himself/herself. Be that as it may, additionally requesting protection setting may confine the quantity of the photographs openly accessible to prepare the FR framework. To manage this quandary, our component endeavor to use clients' private photographs to outline a customized FR framework particularly prepared to separate conceivable photograph co-proprietors without releasing their security. We additionally build up a dispersed consensus based technique to decrease the computational many sided quality and secure the private preparing set.

We demonstrate that our framework is better than other conceivable methodologies as far as acknowledgment proportion and effectiveness. Our system is actualized as a proof of an idea Android application on Facebook's stage. Are urging clients to post co-photographs and tag their companions with a specific end goal to get more individuals included. Be that as it may, imagine a scenario in which the co-proprietors of a photograph are not willing to share. This photograph? Is it a protection infringement to share this co photo without consent of the co-proprietors? Ought to the co-proprietors have some control over the co-photographs? To answer these inquiries, we have to expound on the protection issues over OSNs. Generally, protection is viewed as a condition of social withdrawal. As indicated by Altman's protection direction hypothesis, security is a persuasion and dynamic limit direction handle where security is not static but rather "a specific control of get to the self or to ones gathering". In this hypothesis, "rationalization" alludes to the openness and closeness of self to others furthermore, "dynamic" means the coveted protection level changes with time as indicated by condition.

Amid the procedure of security control, we endeavor to coordinate the accomplished security level to the coveted one. At the ideal protection level, we can encounter the coveted certainty when we need to cover up or appreciate the coveted consideration when we need to appear. In any case, if the genuine level of security is more prominent than the coveted one, we will feel desolate or separated; then again, if the genuine level of security is littler than the coveted one, we will feel over-uncovered what's more, defenceless. Tragically, on most current OSNs, clients have no control over the data showing up outside their profile page. In Thomas, Grier and Nicol inspect how the absence of joint protection control can incidentally uncover touchy data about a client.

II. OBJECTIVE OF THE PAPER

Photo sharing refers to the transfer or publishing of a user's digital photos online and the website which provides such acquaintances over services such as hosting, uploading, sharing and managing of photos through online system. This function provides the upload and display of images through both websites and applications. The photo sharing term can be set up and managed by individual users for the usage of online photo galleries including photo blogs. It means that other users can view but not essentially download the photos, users being able to select different copy-right options for their photos. Unfortunately, it may reveal users privacy if they are permitted to post, comment, and tag a photo liberally. To address this problem, this paper proposes an efficient facial recognition system that can recognize everyone in the photo. Online photo sharing applications have become popular as it provides users various new and innovative alternatives to share photos with a range of people. The photo sharing feature is incorporated in many social networking sites which allow users to post photo for their loving ones, families and friends. For users of social networking sites such as Instagram, this system focuses on the privacy concerns and needs of the users, at the same time explores ideas for privacy protection mechanisms. By considering users current concerns and behaviors, the tool can be designed as per the user's desire which they can adopt and then can be motivated to use.

III. LITREATURE REVIEW

In 2006, Barbara Carminati, Elena Ferrari, and Andrea Perego, presents a sys-tem that consists of policies in the form of constraints on the type, depth and trust level of the relationship that are existing on the access control model for Web-based social networks (WBSNs). The authenticity to the relationships are presented in the form of certificates and rule based approach is used on the client side enforcement to provide access control where the user requesting for access has the entire rights to it. The system doesn't use the relationship among users to provide access as the relationship might not be a strong point of consideration. Instead the trust factor and the depth of relationship among users are very important and based on that the access is provided. A rule-based access control model is proposed for WBSNs, which allows the requirement of access rules for online resources where the relationship between authorized users in the network is denoted in terms of the relationship type, depth, and trust level. In this system, the certificates which are specified by the users are stored and managed by the central node of the network, whereas storing of access control and performing access control is done by a set of peripheral nodes.

In 2009, Jonathan Anderson proposed a paradigm called Privacy Suites which allows users to easily choose suites of privacy settings that can be created by an expert using privacy programming or can be created through exporting them to the abstract format or through existing configuration UIs. A Privacy suite can be verified by a good practice, a high level language and motivated users which then can be then distributed to the members of the social sites through existing distribution channels.

In 2011, Barbara Carminati, Elena Ferrari , Raymond Heatherly, Murat Kantar-cioglub, Bhavani Thuraisingham, address that security and privacy concerns need to be addressed for creating applications of online social networks that include person specific information. So a prime concern is given towards improving social network access control systems. But the current OSNs provide very basic access control system to the users such as marking a particular item as public, private or accessible by their direct contacts but they lack exibility as they do not specify the access control requirements. So a ne-grained OSN access control model based on semantic web technologies is proposed in which encode social network-related information by means of ontology. Semantic Web Rule Language (SWRL) can be used to set the security policies in the form of rules which are expressed in ontology and this can be enforced by simply querying the authorizations.

In 2013, Kambiz Ghazinour proposed a recommender system known as Your Privacy Protector that assists by understanding the behavior of privacy setting and recommends reasonable privacy options. The personal pro le of the user is constructed based on the parameters such as users interests, users privacy settings and users personal pro le on photo albums and based on this pro le of users it assigns the privacy options. The user is granted permission to see their current privacy settings which will be monitored by the system and if any risk is detected it adopts the necessary privacy settings.

In 2015, Anna Cinzia Squicciarini developed an Adaptive Privacy Policy Pre-diction (A3P) system that automatically generates personalized policies as it is a free privacy settings system. Based on the images content, persons personal characteristics and metadata, the user uploaded image can be handled by A3P system. It consists of two components: A3P Core and A3P Social. The A3P core receives the image uploaded by the user, which it classifies and decides whether there is a need to call upon the A3Psocial. If the metadata is unavailable or if it is created manually then it may cause inaccurate classification, violation policy and even may cause inaccurate privacy policy generation.

IV. REQUIREMENT ANALYSIS

Requirement Analysis and Input Output Specification

Requirement analysis is a software engineering task that bridges the gap between system level requirement engineering and software analysis design. The job of requirement analysis is to understand the specific

requirement that must be achieved to build high quality software. The customer is too told at the same time what is technically possible and what plans he had to left under this software. Software requirement analysis is divided into five areas of efforts. These are the problem recognition, synthesis, modeling, specification, review. It is also important to review the 'software scope' in order to estimate the planning estimates.

Requirement analysis consists of two parts:

1. User Requirements
2. System Requirements
   a. Functional Requirements
   b. Non-functional Requirements

V. HARDWARE AND SOFTWARE SPECIFICATION

Hardware Tool

- Minimum 4GB RAM
- Microsoft Windows 7/8/10
- 1280*800 minimum screen resolution

Software Tool

- JAVA (Jdk 1.8)
- Maria DB Database
- Apache Tomcat
- HTML and CSS
- JavaScript

VI. TECHNOLOGY USED

Tomcat

ExerTran uses Apache Tomcat to dynamically generate web pages. The current system uses Tomcat 5. In a standard, or original, Tomcat installation, a web application, or webapp would be stored in the webapps directory of the Tomcat installation in a directory whose name defines the application's name. Instead of this the application directory is kept within the ExerTran directory structure and this directory is linked to Tomcat via an entry in the context file that is created for each coursework application: the context file tells Tomcat all about the application and this file is created and installed when a build of the coursework is performed.

WEB-INF

Tomcat hides the contents of this directory from users, and is the location where Java class files are stored as well as the Tomcat "web.xml" file which defines a number of parameters for the application in particular security information and the mapping of user requests, i.e. URIs, to servlets.

Java Development Kit (JDK)

The Java Development Kit (JDK) provides the foundation upon which all applications that are targeted toward the Java platform are built. The JDK includes a variety of tools and utilities that perform a variety of tasks, which include compiling source code into bytecode, packaging applications, spinning up Java virtual machines (JVMs) and managing the runtime environment of Java applications.

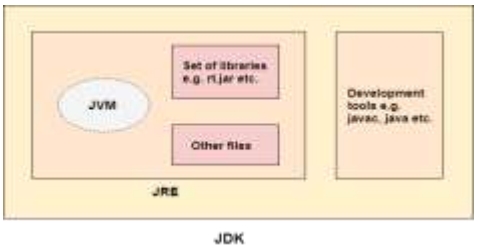


Figure 4.1. JDK

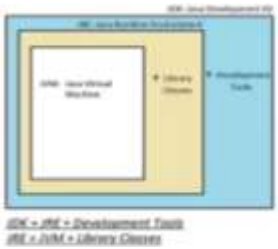


Figure 4.2

MySQL

MySQL is an Oracle-backed open source relational database management system (RDBMS) based on Structured Query Language (SQL). MySQL runs on virtually all platforms, including Linux, UNIX and Windows. Although it can be used in a wide range of applications, MySQL is most often associated with web applications and online publishing.

MySQL is an important component of an open source enterprise stack called LAMP. LAMP is a web development platform that uses Linux as the operating system, Apache as the web server, MySQL as the

relational database management system and PHP as the object-oriented scripting language. (Sometimes Perl or Python is used instead of PHP.)

Originally conceived by the Swedish company MySQL AB, MySQL was acquired by Sun Microsystems in 2008 and then by Oracle when it bought Sun in 2010. Developers can use MySQL under the GNU General Public License (GPL), but enterprises must obtain a commercial license from Oracle.

Today, MySQL is the RDBMS behind many of the top websites in the world and countless corporate and consumer-facing web-based applications, including Facebook, Twitter and YouTube.

VII. SYSTEM DESIGN

Propsed system

Secured Photo Sharing in Web Technology is a web based application which is uses to share photograph with friends and relatives .User own communication to friends.

List of modular description

There are 2 Modules are used in this paper like,

- **User**
- **Admin**

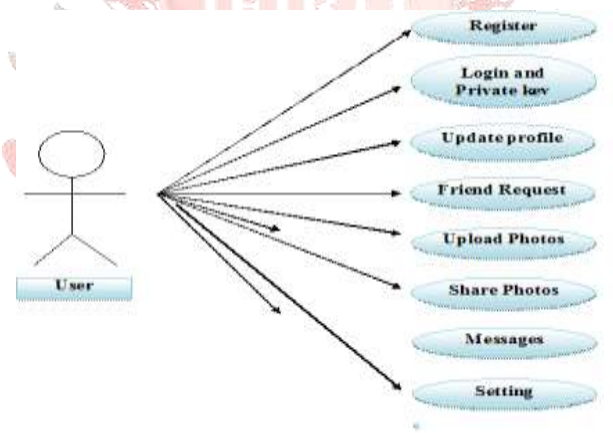
User

- **New Registration:** Create registration for new user.
- **Update Login Details: U**pdate all personal details and upload profile picture.
- **Photos Sharing:** Upload, View photos.
- **Messaging:** Write message to friends.
- **Change Password:** User can change the password.

Admin

The admin helps the admin to do work on database and handle the database of all the users also maintain the security of the database and files of the users.

CASE DIAGRAM



VIII. TEST SPECIFICATION

Testing is a process of executing a program with the interest of finding an error. A good test is one that has high probability of finding the yet undiscovered error. Testing should systematically uncover different classes of errors in a minimum amount of time with a minimum amount of efforts.

Two classes of inputs are provided to test the process

1. A software configuration that includes a software requirement specification, a design specification and source code.

2. A software configuration that includes a test plan and procedure, any testing tool and test cases and their expected results.

Testing is divided into several distinct operations.

Strategic approach of software testing

- Unit Testing
- Integration Testing
- Validation Testing

- Recovery Testing
- Security Testing
- Stress Testing
- Black Box Testing
- Test Data Output

IX. RESULT


Figure 1: Sign Up


Figure 2: Login


Figure 3: User home page


Figure 4: User profile page

Figure 5: After update profile


Figure 6: Message page


Figure 7: User messages page


Figure 8: friend


Figure 9: Search friends


Figure 10: My files

Figure 11 User can share the photos

Figure 12:User can view photos

Figure 13:Password setting

Figure 14: After password setting

X. CONCLUSION

Photo sharing is the process of publishing or transfer of a user's digital photos on-line. Individuals in a co-photo are identified by the proposed FR system. The system reveals the detailed description of our system. Generally speaking, the consensus result could be achieved by iteratively refining the local training result. Various websites o er services such as uploading, hosting, and managing for photo-sharing (publicly or privately). These functions provided by websites and applications facilitate the upload and display of images. The term may even be useful for online photo galleries that are positioned up and managed by individual users, including photo blogs. The system used a toy system with two users to demonstrate the principle of the design. The system that is built has proven that how to build a general personal FR with more than two users.

REFERENCES

1. Kaihe Xu, Yuanxiong Guo, Linke Guo, Yuguang Fang, Xiaolin Li, "My Privacy My Decision: Control of Photo Sharing on Online Social Networks", IEEE Transaction on Dependable and Secure Computing, Volume: PP , Issue: 99, pp-1-1, 2015
2. Z. Stone, T. Zickler, and T. Darrell, "Autotagging facebook: Social network context improves photo annotation", IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops, pp. 1-8, 2008.
3. Kapadia, F. Adu-Oppong, C. K. Gardiner, and P. P. Tsang, "Social circles: Tackling privacy in social networks", in Proc. Sympsable Privacy Security, 2008.
4. J. Bonneau, J. Anderson, and L. Church, "Privacy suites: Shared privacy for social networks", in Proc. Symp. Usable Privacy Security, 2009.
5. C. A. Yeung, L. Kagal, N. Gibbins, and N. Shadbolt, "Pro-viding access control to online photo albums based on tags and linked data", pp. 9-14, 2009.
6. Besmer and H. Richter Lipford. Moving beyond untag-ging: photo privacy in a tagged world. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 1563-1572, 2010.
7. Barbara Carminati, Elena Ferrari, Raymond Heatherly, Mu-rat Kantarcioglu, Bhavani Thuraisingham, "Semantic web-based social network access control", pp. 108-115, 2011.
8. Sergej Zerr, Stefan Siersdorfer, Jonathon Hare, Elena Demi-dova , "I Know What You Did Last Summer!:Privacy-Aware Image Classification and Search ", Proceedings of the 35th international ACM SIGIR conference on Research and development in information retrieval, 2012.
9. Kambiz Ghazinour, Stan Matwin and Marina Sokolova, "Yourprivacyprotector: A Recommender System For Pri-vacy Settings In Social Networks", International Journal of Security, Privacy and Trust Management (IJSPTM), Vol 2, No 4, August 2013.
10. Barbara Carminati, Elena Ferrari, Raymond Heatherly, Murat Kantar-cioglu, Bhavani Thuraisingham, Semantic web-based social network access control, 2011.
11. Prashant Abhang, S. B. Rathod, "My Privacy My decision: Control of Photo Sharing on Online Social Networks", July-2017.