International Journal of Current Research and Modern Education (IJCRME)
ISSN (Online): 2455 - 5428
(www.rdmodernresearch.com) Volume I, Issue I, 2016

PROTOCOL TO CHECKPHOTO SHARING IN A FOOLPROOF WAY

R. Arthi* & M. Rajakumar**
* PG Scholar, Department of Master of Computer Applications, Dhanalakshmi Srinivasan Engineering College, Perambalur, Tamilnadu
** Associate Professor & Head, Department of Master of Computer Applications, Dhanalakshmi Srinivasan Engineering College, Perambalur, Tamilnadu

Abstract:
Photo sharing is an attractive feature which popularizes Online Social Networks (OSNs). Unfortunately, it may leak users' privacy if they are allowed to post, comment, and tag a photo freely. To attempt the address this issue and study the scenario when a user shares a photo containing individuals other than himself/herself (termed co-photo for short). To prevent possible privacy leakage of a photo, the project design a mechanism named classifier to enable each individual in a photo be aware of the posting activity and participate in the decision making on the photo posting. Photos are uploaded in social networks. Sharing such photos is an important feature & most users do that. But this sharing is subjected to be limited to a particular group. However photos are leaked by some malicious users. The focus here is to prevent such photo leaks to unauthorized users. To deal with this dilemma and to prevent privacy leakage of photos of a particular member in a computationally cost effective manner and to devise a mechanism which provides a proper permission granting model before posting the photo. The mechanism attempts to utilize users' private photos to design a personalized system specifically trained to differentiate possible photo co-owners without leaking their privacy. The projects also develop a distributed consensus based method to reduce the computational complexity and protect the private training set. The system is superior to other possible approaches in terms of recognition ratio and efficiency.

Key Words: Social Network, Photo Privacy & Secure Sharing

1. Introduction:

SNS have become integral part of our daily life with each other, fulfilling our social needs–the needs for social interactions, information sharing, appreciation and respect. It is also this very nature of social media that makes people put more content, including photos over OSNs without too much thought on the content. However, once something, such as a photo, is posted online, it becomes a permanent record, which may be used for purposes we never expect. For example, a posted photo in a party may reveal a connection of a celebrity to a mafia world. Because OSN users may be careless in posting content while the effect is so far-reaching, privacy protection over OSNs becomes an important issue. When more functions such as photo sharing and tagging are added, the situation becomes more complicated. For instance, nowadays we can share any photo as we like on OSNs, regardless of whether this photo contains other people (is a co-photo) or not.

Currently there is no restriction with sharing of co-photos, on the contrary, social network service providers like Face book are encouraging users to post co-photos and tag their friends in order to get more people involved. However, what if the co-owners of a photo are not willing to share this photo? Is it a privacy violation to share this co-photo without permission of the co-owners? Should the co-owners have some control over the co-photos? To answer these questions, we need to elaborate on the privacy issues over OSNs. Traditionally, privacy is regarded as a state of social withdrawal Privacy is a dialectic and dynamic boundary regulation process where privacy is not

static but "a selective control of access to the self or to one's group". In this theory, "dialectic" refers to the openness and closeness of self to others and "dynamic" means the desired privacy level changes with time according to environment. During the process of privacy regulation, we strive to match the achieved privacy level to the desired one.

At the optimum privacy level, we can experience the desired confidence when we want to hide or enjoy the desired attention when we want to show. However, if the actual level of privacy is greater than the desired one, we will feel lonely or isolated; on the other hand, if the actual level of privacy is smaller than the desired one, we will feel over-exposed and vulnerable. Unfortunately, on most current OSNs, users have no control over the information appearing outside their profile page.

2. Related Works:

- ✓ **Kaihe Xu,Yuanxiong Guo, Linke Guo, Yuguang Fang & Xiaolin Li, "My Privacy My Decision:** Control of Photo Sharing on Online Social Networks": Photo sharing is an attractive feature which popularizes Online Social Networks (OSNs). Unfortunately, it may leak user's privacy if they are allowed to post, comment, and tag a photo freely. In this paper, we attempt to address this issue and study the scenario when a user shares a photo containing individuals other than himself/herself (termed co-photo for short). To prevent possible privacy leakage of a photo, we design a mechanism to enable each individual in a photo be aware of the posting activity and participate in the decision making on the photo posting. For this purpose, we need an efficient facial recognition (FR) system that can recognize everyone in the photo. However, more demanding privacy setting may limit the number of the photos publicly available to train the FR system. To deal with this dilemma, our mechanism attempts to utilize users' private photos to design a personalized FR system specifically trained to differentiate possible photo co-owners without leaking their privacy. We also develop a distributed consensus based method to reduce the computational complexity and protect the private training set. We show that our system is superior to other possible approaches in terms of recognition ratio and efficiency. Our mechanism is implemented as a proof of concept Android application on Face book's platform.
- ✓ **Kurt Thomas, Chris Grier & David M. Nicol, "Unfriendly: Multi-Party Privacy Risks in Social Networks":** As the popularity of social networks expands, the information users expose to the public has potentially dangerous implications for individual privacy. While social networks allow users to restrict access to their personal data, there is currently no mechanism to enforce privacy concerns over content uploaded by other users. As group photos and stories are shared by friends and family, personal privacy goes beyond the discretion of what a user uploads about himself and becomes an issue of what every network participant reveals. In this paper, we examine how the lack of joint privacy controls over content can inadvertently reveal sensitive information about a user including preferences, relationships, conversations, and photos. Specially, we analyze Face book to identify scenarios where conflicting privacy settings between friends will reveal information that at least one user intended remain private. By aggregating the information exposed in this manner, we demonstrate how a user's private attributes can be inferred from simply being listed as a friend or mentioned in a story. To mitigate this threat, we show how Face book's privacy model can be adapted to enforce multi-party privacy. We present a proof of concept

application built into Face book that automatically ensures mutually acceptable privacy restrictions are enforced on group content in their relationship network. This paper will illustrate and discuss the most prevalent issues and threats targeting different social networks today.

- ✓ **Candid Wuest, "The Risks of Social Networking":** Social networks are an inherent part of today's Internet and used by more than a billion people worldwide. They allow people to share ideas and interact with other people, from old friends to strangers. This interaction reveals a lot of information, often including personal information visible to anyone who wants to view it. Hence privacy is often a key concern by the users. Since millions of people are willing to interact with others, it is also a new attack ground for malware authors. They are spreading malicious code and sending spam messages by taking advantage of the users' inherent trust.
- ✓ **Matthew Turk & Alex Pentland, "Eigen faces for Recognition":** We have developed a near-real-time computer system that can locate and track a subject's head and then recognize the person by comparing characteristics of the face to those of known individuals. The computational approach taken in this system is motivated by both physiology and information theory, as well as by the practical requirements of near-real-time performance and accuracy. Our approach treats the face recognition problem rather than requiring recovery of three dimensional geometry, taking advantage of the fact that faces are normally upright and thus may be described by a small set of 2-D characteristics views. The system functions by projecting face images on to a feature space that spans the significant variations among known face images. The significant features are known as "eigen faces," because they are the eigenvectors (principal components) of the set of faces; they do not necessarily correspond to the features. The projection operation characterizes an individual face by a weighted sum of the eigen face feature and so to recognize a particular face it is necessary only to compare these weights to those of known individuals. Some particular advantages of our approach are that it provides for the ability to learn and later recognize new faces in an unsupervised manner, and that it is easy to implement using neural network architecture.

3. Existing System:

Mostly Shared photos are misused by unauthorized users. Basic methodology used in existing systems is to un-tag photos. So shared photos are not being able to be used. But this results in lot of manual work. Leads to Unsatisfactory countermeasures. The lack of joint privacy control can inadvertently reveal sensitive information about a user. To mitigate this threat, they suggest Face book's privacy model to be adapted to achieve multi-party privacy. Specifically, there should be a mutually acceptable privacy policy. While determining which information should be posted and shared. To achieve this, OSN users are asked to specify a privacy policy and a exposure policy. Privacy policy is used to define group of users that are able to access a photo when being the owner, while exposure policy is used to define group of users that are able to access when being a co-owner. These two policies will together mutually specify how a co-photo could be accessed. However, before examining these policies, finding identities in co-photos is the first and probably the most import step. In the rest of this paper we will focus on a RF engine to find identities on a co-photo. FR problems over OSNs are easier than a regular FR problem because the contextual information of OSN could be utilized for FR. For example, people showing up together on a co-photo are very likely to be

friends on OSNs, and thus, the FR engine could be trained to recognize social friends (people in social circle) specifically. Training techniques could be adapted from the off-the-shelf FR training algorithms, but how to get enough training samples is tricky. FR engine with higher recognition ratio demands more training samples (photos of each specific person), but online photo resources are often insufficient. User's cares about privacy are unlikely to put photos online. Perhaps it is exactly those people who really want to have a photo privacy protection scheme. To break this dilemma, we propose a privacy-preserving distributed collaborative training system as our FR engine.

4. Proposed System:

Users are classified as friends. So essentially a friend is a friend of a friend theory is established. A user needs to coordinate all friends to build classifiers in a OSN. This classifier acts as a bridge between them. A Self friend and friend known to the two. This ensured that friends only communicate with each other. So any unknown person will not be able to misuse shared data. Thus privacy is preserved. With the training data (private photo sets) distributed among users, this problem could be formulated as a typical secure multi-party computation problem. Intuitively, we may apply cryptographic technique to protect the private photos, but the computational and communication cost may pose a serious problem for a large OSN. In this paper, we propose a novel consensus based approach to achieve efficiency and privacy at the same time. The idea is to let each user only deal with his/her private photo set as the local train data and use it to learn out the local training result. After this, local training results are exchanged among users to form a global knowledge. In the next round, each user learns over his/hers local data again by taking the global knowledge as a reference. Finally the information will be spread over users and consensus could be reached. We show later that by performing local learning in parallel, efficiency and privacy could be achieved at the same time.

Advantages:

- ✓ The model is very fast and accurate.
- ✓ Privacy is effectively preserved.
- ✓ No computational overheads.
- ✓ Secret sharing is only between the users.
- ✓ So any unknown Person cannot Access the Photos and Any Data
- ✓ It's Access Permission only.

Module:

- ✓ OSN Configuration
- ✓ Unique Identity
- ✓ Key Generation
- ✓ Classify
- ✓ Identify
- ✓ Share and Revoke

Module Description:

OSN Configuration: The online social media information filtering techniques are used to remove unwanted contents by using customizable content based filtering rules, Machine learning approach; according to user's interest and recommends an item. A user post (a truncation of the expression weblog post) is a discussion or informational site published on the World Wide Web and consisting of discrete entries ("posts") typically displayed in reverse chronological order (the most recent post appears first). All the blog posts were usually the work of a single individual, occasionally of a small group, and often covered a single subject. More recently "multi-author blog posts"

(MABs) have developed, with posts written by large numbers of authors and professionally edited. Majorities are interactive, allowing visitors to upload photos each other via GUI widgets on the blogs, and it is this interactivity that distinguishes them from other static websites.

New User Registration Module:

Unique Identity: First the new user who wants to access is given a unique identity. The unique identity provided to each and every user is the problem provided by the new user module. This enables to take the new user to the next step that is key generation. First the users who want to post register in this module. The users give their data like name, address, city, pincode, contact and email id to the form. All the details are stored in the SQL Database Server. So only after the registration is complete a message is delivered to the user that he has been successfully accommodated into the system as a user. The users then may be redirected to the posting module, where they may post contents with title and category. Thus the registration phase is an important part of the user for logging into the system.

Key Generation: A unique secret key for this user is generated and sent to the cloud. The other component we will have to worry about is the actual key that is used to encrypt and decrypt. The key must be such that it is not easily guessed, and since no one is expected to remember it, it may not be a string of human comprehensible characters. It can be just any arbitrary string of characters. The best option to generate a key is using the new code segment DES3GetKey in the package toolkit. As in all other codes in this package, the DES3GetKey code is also implemented as both a procedure and a function and overloaded with both VARCHAR2 and RAW data types. The parameter to the procedure version in the RAW format is then processed.

Classify: In content based filtering to check the user's interest and previous activity as well as item uses by users best match is found. For example OSNs such as Face book, Orkut used content based filtering policy. In that by checking users profile attributes like education, work area, hobbies etc. suggested friend request may send. The main purpose of content based filtering, the system is able to learn from user's actions related to a particular content source and use them for other content types. In collaborative filtering information will be selected on the basis of user's preferences, actions, predicts, likes, and dislikes. Match all this information with other users to find out similar items. Large dataset is required for collaborative filtering system. According to user's likes and dislikes. In policy based filtering system users filtering ability is represented to filter wall messages according to filtering criteria of the user. Twitter is the best example for policy based filtering. In that communication policy can be defines between two communicating parties. It is in this module that the abusive posts and words are entered and the system is trained to filter the posts in the social media using these words as rules. The Filtering Rules are customizable by the user. User can have authority to decide what contents should be blocked or displayed on his wall by using Filtering rules. For specify a Filtering rules user profile as well as user social relationship will be considered. Author is a person who defines the rules. User Spec denotes the set of OSN user. Content Spec is a Boolean expression defined on content.

Identify: If the photos content is not found to be shared by the owner then they are not shown. A message by is sent to the user of the post. The list is maintained for the words which have been trained by the users to get hold of the abusive and explicitly destructive content which should not be seen and may cause damage to other users. It may also lead to unnecessary altercations and erupt into full-fledged clashes. Thus blacklisting helps in reducing such notoriety from spreading its wings.

Share and Revoke: Such photos will be deleted by the admin of the social network system. Further continuance by the users to be abusive will be dealt with severely by terminating all their posts. The post and its contents along with the title will be removed permanently from the system and other users will not be able to see it. The users will further be scrutinized so that they do not cause any damage to the system. The posts thus revoked will be deleted from the SQL Server table also so that it may not crop up in the future. Cloud Servers store all the secret key components of SK except for the one corresponding to the dummy attribute AttD. Such a design allows Cloud Servers to update these secret key components during user revocation as we will describe soon. As there still exists one undisclosed secret key component (the one for AttD), Cloud Servers cannot use these known ones to correctly decrypt cipher texts. Actually, these disclosed secret key components, if given to any unauthorized user, do not give him any extra advantage in decryption as we will show in our security analysis. Here the key is verified for the user. It is in this module that the absolute verification is done to ensure the secure transmission of the data. If verification fails than the transmission is stopped and further processing is aborted.

5. System Architecture:

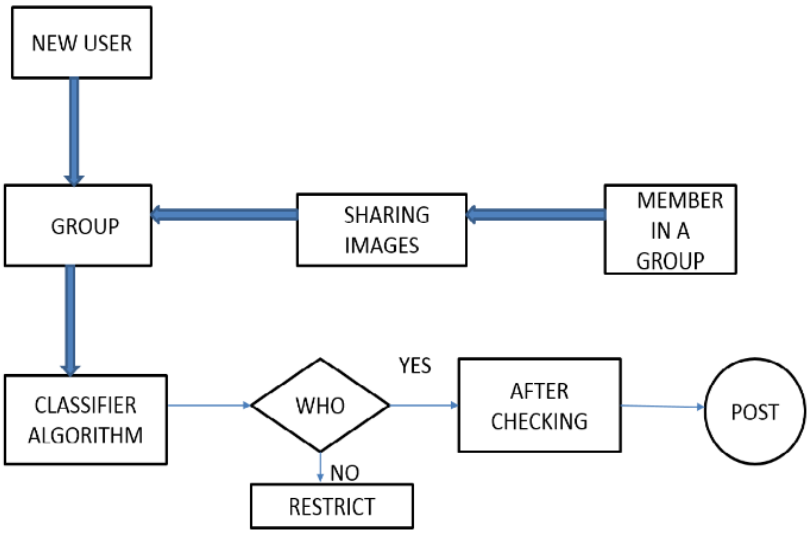

Figure 1: System Architecture

Functions of System Design:

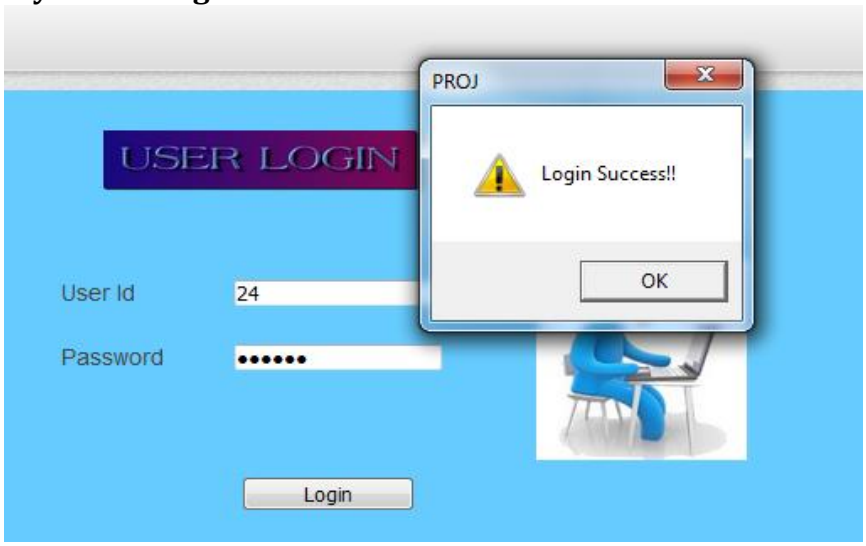

Figure 2: Login Success

Figure 3: User Menu

Figure 4: Login Failed

Used Mechanisms:

- ✓ Classifier Algorithm
- ✓ RSA Algorithm

Classifier Algorithm:

- ✓ Users are classified as friends. So essentially a friend is a friend of a friend theory is established.
- ✓ A user needs to coordinate all friends to build classifiers in a OSN.
- ✓ This classifier acts as a bridge between them. Self-friend and friend known to the two.
- ✓ This ensured that friends only communicate with each other.
- ✓ So any unknown person will not be able to misuse shared data.
- ✓ Thus privacy is preserved.

RSA Algorithm:

In cryptography, RSA (which stands for Rivest, Shamir and Adleman who first publicly described it) is an algorithm for public-key cryptography. It is the first algorithm known to be suitable for signing as well as encryption, and was one of the first great advances in public key cryptography. RSA is widely used in electronic commerce protocols, and is believed to be secure given sufficiently long keys and the use of up-to-date implementations.

Key Generation:

RSA involves a public key and a private key. The public key can be known to everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted using the private key. The keys for the RSA algorithm are generated the following way:

Step 1: Choose two distinct prime numbers p and q.

Step 2: For security purposes, the integer's p and q should be chosen at random, and should be of similar bit-length.

Step 3: Prime integers can be efficiently found using a primality test.

Step 4: Compute n = pq.

Step 5: n is used as the modulus for both the public and private keys

Step 6: Compute $\varphi(n) = (p - 1)(q - 1)$, where φ is Euler's totient function.

Step 7: Choose an integer e such that $1 < e < \varphi(n)$ and $\gcd(e,\varphi(n)) = 1$, i.e. e and $\varphi(n)$ are coprime.

Step 8: e is released as the public key exponent.

Step 9: e having a short bit-length and small Hamming weight results in more efficient encryption - most commonly 0x10001 = 65537. However, small values of e (such as 3) have been shown to be less secure in some settings.

Step10: Determine $d = e^{-1} \bmod \varphi(n)$; i.e. d is the multiplicative inverse of e mod $\varphi(n)$.

Step 11: This is often computed using the extended Euclidean algorithm.

Step 12: d is kept as the private key exponent.

Step 13: The public key consists of the modulus n and the public (or encryption) exponent e.

Step 14: The private key consists of the private (or decryption) exponent d which must be kept secret.

Experimental Results:

The proposed classifier algorithm is implemented with social network. This is used to prevent the group from hackers. (i.e.) without getting proper permission the unauthorized person cannot get in to the group. In a day-to-day life so many persons are affected by this kind of misusing of images. This algorithm generates a key to the new person who is entering into the group. Therefore, the new person is entering with the knowledge of users. So there may not be any stealing process or any kind of misusing of images. So no need to worry about the safety of the group.

6. Future Enhancement:

The scope of this Protocol is widening and today it offers a strong support to secure images from unauthorized persons. Future of this model brings exiting promises as expected from the experience of limited users. It may also help Improving the ways of dealing with organizations. The bright future prospect of this model is also proven with the fact that the technology is integrated in the mobile phones as well. So, this model gives great prospects in future.

7. Conclusion:

Thus the proposed model is very effective for OSN users. Helps in data privacy of the individual. The decision to share the photo or data rests with the user. Provides a mechanism for effective control over what is to be shared and between whom using classifiers. Photo sharing is one of the most popular features in online social networks such as Face book. Unfortunately, careless photo posting may reveal privacy of individuals in a posted photo. To curb the privacy leakage, proposed to enable individuals potentially in a photo to give the permissions before posting a co-photo. The proposed system is featured with low computation cost and confidentiality of the

training set. Theoretical analysis and experiments were conducted to show effectiveness and efficiency of the proposed scheme. The proposed scheme is very useful in protecting users' privacy in photo/image sharing over online social networks. However, there always exist trade-off between privacy and utility. Latency introduced in this process will greatly impact user experience of OSNs.

8. References:

1. B. Carminati, E. Ferrari, and A. Perego. Rule-based access control for social networks. In R. Meersman, Z. Tari, and P. Herrero, editors, On the Move to Meaningful Internet Systems 2006: OTM 2006 Workshops, volume 4278 of Lecture Notes in Computer Science,pages 1734–1744. Springer Berlin Heidelberg, 2006.
2. J. Y. Choi, W. De Neve, K. Plataniotis, and Y.-M. Ro. Collaborative face recognition for improved face annotation in personal photo collections shared on online social networks. Multimedia, IEEE Transactions on, 13(1):14–28, 2011.
3. K. Choi, H. Byun, and K.-A. Toh. A collaborative face recognition framework on a social network platform. In Automatic Face Gesture Recognition, 2008. FG '08. 8th IEEE International Conference on, pages 1–6, 2008.
4. K.-B.Duan and S.S.Keerthi. Which is the best multiclass svm method? an empirical study. In Proceedings of the 6th international conference on Multiple Classifier Systems, MCS'05, pages 278–285, Berlin, Heidelberg, 2005. Springer-Verlag.
5. P.A.Forero, A.Cano, and G.B.Giannakis. Consensus-based distributed support vector machines. J. Mach. Learn. Res., 99:1663–1707, August 2010.
6. B.Goethals, S.Laur, H.Lipmaa, and T.Mielikinen. On private scalar product computation for privacy-preserving data mining. In In Proceedings of the 7th Annual International Conference in Information Security and Cryptology, pages 104–120. Springer-Verlag, 2004.
7. L. Kissner and D. Song. Privacy-preserving set operations. In IN ADVANCES IN CRYPTOLOGY - CRYPTO 2005, LNCS, pages 241–257. Springer, 2005.
8. L. Kissner and D. X. Song. Privacy-preserving set operations.In V. Shoup, editor, CRYPTO, volume 3621 of Lecture Notes in Computer Science, pages 241–257. Springer, 2005.
9. N. Mavridis, W. Kazmi, and P. Toulis. Friends with faces: How social networks can enhance face recognition and vice versa. In Computational Social Network Analysis, Computer Communications and Networks, pages 453–482, Springer, London, 2010.
10. R. J. Michael Hart and A. Stent. More content - less control: Access control in the web 2.0. In Proceedings of the Workshop on Web 2.0 Security and Privacy at the IEEE Symposium on Security and Privacy, 2007.