www.ijecs.in
*International Journal Of Engineering And Computer Science ISSN: 2319-7242*
*Volume 5 Issue 5 May 2016, Page No. 16492-16503*

# My Privacy My Decision: Control Communication media on Online Social Networks

**Arpitha B, Mrs. Deepika**
Post Graduate
Department of Computer Science & Engineering
PES College of Engineering
Mandya, Karnataka, India
Arpithab92@gmail.com
Asst Professor, BE, Mtech
Department of Computer Science & Engineering
PES College of Engineering
Mandya, Karnataka, India
deepu_daya@yahoo.com

**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. 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 Facebook's platform.**

Index Terms—Social network, photo privacy, secure multi-party computation, support vector machine, collaborative learning

!

## INTRODUCTION

Social sites have become important part of our daily life .Online social networks (OSNs) such as face book, Google and sound of birds are inherently designed to make able people to part personal and public information and make social connections with friends, coworkers, persons having like-position, family, and even with strangers. To keep safe (out of danger) user facts, way in control has become a chief thing point of OSNs. However it becomes everlasting record once some photo/image is posted/uploaded. Late consequences can be dangerous, people may use it for different unexpected purposes. For example a posted may reveal the mafia relationship of any celebrity. A user profile usually includes information with respect to the users work history birthday, sex, residence, interests, education, and, travel information and be in touch information. Moreover, users upload the picture and tag other people even though they are willing or not willing to be part of uploaded image/content. When other people are tagged the situation becomes more complicated. The user uploading the image is totally unaware of the consequences that arise for the person which is involved in tagging or image. Currently nobody can stop such unavoidable situation. We need to have a control over such actions to minimize the risks of photos being tagged or uploaded. Instead of imposing restrictions over such incidents or increasing security, sites like FB and Instagram are encouraging people to get into such things more. Most of the times user is unwilling to get tagged or being exposed without his permission. Is it violation if we share picture without taking a permission from all the people involved in picture? To answer this we need to explain the privacy and security issues over the social sites. Whenever a photograph is shared it includes everybody's security, which can be put on risk if the proper permissions are not sought. We need to enforce maximum level of privacy and security of the content being uploaded on social sites. So while using the online social networks one can feel desired level of confidence and security. He/she can confidently make use of social sites without worrying or photos being shared in insecure and unauthorized way. Desired level of privacy and security is a first important thing for a user using online social sites. With respect to current architecture and implementations of social sites, either user will alone because highly imposed security constraints else will be impacted by several security threats because of low security mechanisms. Few authors studied about the security challenges because of lack of joint or collaborative control over the images being shared across the online social sites. To minimize this or to completely avoid this they have suggested social sites like Facebook, Instagram to

DOI: 10.18535/ijecs/v5i5.27

make use of multi-party privacy model to increase privacy. There should be mutual acceptable policy to grant access for a photo when multiple user are involved. For security user might need to create a group where they can grant access for their uploaded images. Exposure policy can be defined as the group of users where an image can be accessed when particular user is involved and the privacy policy can be stated as the group of users/friends who can have a direct access of the uploaded images. These two policies are used to define the overall audience or group of users/friends who can be given access to uploaded image. But before establishing this there should be a proper process of defining these groups. For this the facial recognitions are used. Most of the times the people found in the co-photo are close friends. So face recognitions engines are trained for identifying the friends in social circle. FR engines with more accuracy rates require large number of test data/samples specific to a person but most of the times it is not possible. Users who care about the privacy and security mostly restrict themselves from uploading the photos but if these people are provided with proper privacy preserving techniques then they can post photos without any reluctance. We are designing a privacy enhancing system of photo sharing which makes use of collaborative training system. We are enabling the users of social site to have own personal FR engine based on social relations which will make use of images stored in their personal system. It will help to build a social relationship tree, which can be used for policies for sharing of data. We make use of cryptographic techniques are well to build such training data. We need to propose a secure approach to gain efficiency and privacy both. The user is trained first from his local training set, means set of photos in her gallery. Exposure policies are defined to have access on photo. And then by global knowledge of relationships the photo sharing can be initiated. Finally data will be distributed to the right people who have access. Efficiency and privacy can be achieved by simultaneously comparing the current and previous experiments.

1. The users in a shared photo are automatically detected without being tagged by somebody.

2. We propose a secure sharing of private photos by making use of social context to have personal FR Engines. 3. We can achieve privacy, security and efficiency.

### *Literature survey*

Literature survey is the most important step in software development process. Before developing the tool it is necessary to determine the time factor, economy and company strength. Once these things are satisfied, ten next steps are to determine which operating system and language can be used for developing the tool. Once the programmers start building the tool the programmers need lot of external support. This support can be obtained from senior programmers, from book or from websites. Before building the system the above consideration are taken into account for developing the proposed system.

Privacy concerns with social networking services have been raised growing concerns amongst users on the dangers of giving out too much personal information and the threat of sexual predators. Users of these services also need to be aware of data theft or viruses. However, large services, such as Myspace and Netlog, often work with law enforcement to try to prevent such incidents.

In addition, there is a perceived privacy threat in relation to placing too much personal information in the hands of large corporations or governmental bodies, allowing a profile to be produced on an individual's behavior on which decisions, detrimental to an individual, may be taken.

Companies are able to improve their sales and profitability. With this data, companies create customer profiles that contain customer demographics and online behavior. A recent strategy has been the purchase and production of "network analysis software". This software is able to sort out through the influx of social networking data for any specific company. Facebook has been especially important to marketing strategists. Facebook's controversial "Social Ads" program gives companies access to the millions of profiles in order to tailor their ads to a Facebook user's own interests and hobbies. However, rather than sell actual user information, Facebook sells tracked "social actions". That is, they track the websites a user uses outside of Facebook through a program called Facebook. Access control to online resources forms element of the broader concept of policy (Bonatti et al. 2006) [1] on the Web. A variety of access control mechanisms to private resources on the Web have been discussed by different authors in the literature.

For example, PeerTrust (Gavriloaie et al. 2004) [2] has proposed to provide an access control mechanism based on semantic annotation, policies and automated trust negotiation. Users are involved in an iterative process of exchanging credentials to establish trust between them. While the system provides a reliable mechanism to establish trust between two parties, the process and the need of providing certain private information involve substantial overhead which may not be necessary in common online activities such as photo sharing.

Lalanaetal. (2006) [3] propose a Web-based policy management framework called Rein which makes use on Semantic Web technologies. The framework provides an ontology which can be used to describe what access control policies are attached to a user’s resources and in what languages the policies are written.

Tootoonchian et al. (2008) [4] introduce an access control scheme called Lockers. It allows a user to send to other users something called social attestations which they use to prove their social relationship with the user to any Web sites storing personal contents. Lockr also allows policies based on different kinds of social relationship to be created by allowing a user to construct a social access control list. The authors propose that information about a social network should be separated from content delivery. However, the possibility of using linked data on the Web is not considered.

In addition, Yag¨ue et al. (2003) [5] describes a layered access control scheme based on Semantic Web technologies and gives

**access to users based on their as well as the resources semantic properties. Working in the context of Semantic Web services, Agarwal and Sprick (2004) [6] studies how access control policies to a composite Web service can be determined based on those of its components. While these studies focus on the utilizing Semantic Web technologies, they do not discuss how the potentiality of linked data can be exploited to help create expressive policies.**

**Some of the systems proposed for privacy preserving on an online social network includes:**

- **Rule Based Access Control**
  **It presents a system that consists of policies in the form of constraints on the type, depth and the trust level of the relationship that are existing on the access control model for Web-based social networks (WBSNs). The authenticity of 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 [7], 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.**

- **Face Annotation using Collaborative Face Recognition**
  **Face annotation (or tagging) method aimed towards improving the accuracy of face annotation by making use of multiple and distributed databases and FR (Face Recognition) engine which are distributed on an online social network. The FR recognition method was done using the standard MPEG-7VCE-3 dataset and a set of real-world personal photos from the web. The system devise a collaborative FR method [8] aiming to improve the face annotation accuracy by combining annotation results obtained from individual FR engines. A social relationship among community members and social context in personal photographs are used to form FR databases and engines to annotate faces in a collaborative way rather than considering individual FR in which fusion techniques are applied to combine results from the multiple FR engine and give a single result.**

- **Semantic Web based**
  **Security and privacy concerns need to be addressed in 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 (Online Social Networks) 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 flexibility as they do not specify the access control requirements. So a fine-grained OSN access control model based on semantic web technologies is proposed in [9] 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 the ontology and this can be enforced by simply querying the authorizations.**

- **Photo Tagging**
  **The sensitive and private user attributes can be revealed by the act of tagging pictures on the social-networking site of Facebook. Through Facebook lots of data is being shared which may even be private and very sensitive so a prime concern is given to user privacy. Even it is being revealed that even the date and place of birth of a profile can be used to predict the Social Security Number (SSN) of a Facebook user and additional to that much more can be revealed through the user's friends list.**
  **People may be identified on the photo through sensitive information which may be embedded in the photo as metadata by accompanying much more information that could be exploited like comments, captions marked regions and photo tags. Even if through the photo tags [10], if the individual is not identified, it is possible to infer someone's identity through the combination of face recognition software and publicly available data. So it is preferred that the users should be able to hide their tags, rather than deleting it and thus keep a high degree of interaction by keeping track of the photos they have online with the album owner but the photos shouldn't be linked directly to their profiles.**

- **PViz Comprehension Tool**
  **It is a tool that explains how user model groups and privacy policies applied to their networks. PViz [11] is an interface and system that allows the user to understand its profile based on various factors such as natural subgroups of friends that is constructed at different levels of granularity. The group labels are provided so that the user can identify and distinguish automatically constructed groups. This tool is better than other tools like Facebook's Audience View and Custom Settings page.**

- **Privacy Suites**
  **Privacy Suites [12] 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 (User Interfaces). 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.**

- Social Circles
  **Privacy settings based on the concept of social circles [13] which protects personal information through a web based solution was developed. The friend's lists are automatically generated through Social Circles Finder that identifies the intensities of the relation by analyzing the social circle of the person which in turn helps in categorizing of friends for privacy policy setting. The social circle of the subject will be identified by the application, but won't be revealed to the subject. The subject's interest of sharing the information will be considered by interrogating the subject and based on that the piece of personal information will be shared in the form of visual graphs.**

- Privacy-Aware Image Classification and Search
  **In 2012, Sergej Zerr developed a technique [14] which enables privacy-oriented image search for automatically detecting private images. The security policies are provided by a combination of textual metadata images with a variety of visual features. In this the selected image features (edges, faces, color histograms) which can help to distinguish between natural and man-made objects/scenes can be done through image features like edges, faces or color histogram through which the presence or absence of an object can be determined. It uses various classification models trained on a large scale dataset with privacy assignments obtained through a social annotation game.**

- Decentralized authentication protocol
  **An access control system based on a [15], descriptive tags and linked data of social networks on the Semantic Web. It allows users to create expressive policies for their photos stored in one or more photo sharing sites, and users can specify access control rules based on open linked data provided by other parties.**

- Adaptive Privacy Policy Prediction (A3P)
  **A3P system [16] automatically generates personalized policies as it is a free privacy setting system. Based on the image content, person's 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 A3P-social. 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.**

- Conditional Random Field (CRF)
  **The conditional random field is a pair wise model which based on the conditional density finds the optimal joint labeling. In CRF, the accuracy of the face annotation is improved by considering the existing labeled photos as the training sample along with the FR score. The system combine face recognition scores with social context in a conditional random field (CRF) model and apply this model to label faces in photos from the popular online social network Facebook, which is now the top photo-sharing site on the Web with billions of photos in total. Existing metadata from online social networks can improve automatic photo annotation. But it will be impossible for the system to label some individuals in newly posted photos.**

- Facial recognition (FR) System

**A privacy-preserving FR system is used to identify individuals in a co-photo. The owners of shared photos can be automatically identified with or without user-generated tags. The FR engine is derived from the private photos and social contexts. The privacy is protected by providing user facility to restrict others from seeing their photos. Each user is able to define his/her policy which is the privacy policy and exposure policy. Computation cost is very low. FR system provides privacy by notifying the subject about the posting activity and thus leading the other subjects to take active part in it.**

**We can find a scheme of game-theoretic suggested by Squicciarini et al in [17]. In this scheme privacy policies are mutually enforced over the shared data. It is possible for every user to define his/her privacy policy and exposure policy. When a photo is processed with owner's privacy policy and co-owners exposure policy only then it could be posted. But it is difficult to find co-owner of the co-photo automatically. Tagging feature on present OSNs must be used to find a potential co-owner in this case.**

**A mechanism has been designed to make users aware of the posting activity and make them actively take part in the photo posting and decision making paradigm for which a facial recognition (FR) system is recommended which can recognize everyone present in the photo. If more privacy setting is done, then it may limit the number of photos which will be utilized as the training set for FR system. In order to overcome this problem and for the training set for FR system we would utilize the private photos of users, which would differentiate the photo co-owners without affecting their privacy. A distributed consensus based method is developed which would protect the private training set and even reduce the computational complexity.**

**The contributions of this work when compared with previous work are mentioned below:-**

- **The potential owners of shared items (photos) can be automatically identified.**

- **Orthogonal to the traditional cryptographic solution, this work proposes a consensus-based method to achieve privacy and efficiency.**
- **Achieve efficiency and privacy at the same time.**

## RELATED WORK

**In [12], Mavridis et al. study the statistics of photo sharing on social networks and propose a three realms model: "a social realm, in which identities are entities, and friendship a relation; second, a visual sensory realm, of which faces are entities, and co-occurrence in images a relation; and third, a physical realm, in which bodies belong, with physical proximity being a relation." They show that any two realms are highly correlated. Given information in one realm, we can give a good estimation of the relationship of the other realm. In [19], [20], Stone et al., for the first time, propose to use the contextual information in the social realm and co-photo relationship to do automatic FR. They define a pairwise conditional random field (CRF) model to find the optimal joint labeling by maximizing the conditional density. Specifically, they use the existing labeled photos as the training samples and combine the photo co- occurrence statistics and baseline FR score to improve the accuracy of face annotation. In [6], Choir et al. discuss the difference between the traditional FR system and the FR system that is designed specifically for OSNs. They point out that a customized FR system for each user is expected to be much more accurate in his/her own photo collections. A similar work is done in [5], in which Choi et al. propose to use multiple personal FR engines to work collaboratively to improve the recognition ratio. Specifically, they use the social context to select the suit- able FR engines that contain the identity of the queried face image with high probability.**

## Existing System:

**A survey was conducted in to study the effectiveness of the existing countermeasure of un tagging and shows that this countermeasure is far from satisfactory users are worrying about offending their friends when un tagging. As a result, they provide a tool to enable users to restrict others from seeing their photos when posted as a complementary strategy to protect privacy. However, this method will introduce a large number of manual tasks for end users. In , Squicciarini et al. propose a game-theoretic scheme in which the privacy policies are collaboratively enforced over the shared data. This happens when the appearance of user i has changed, or the photos in the training set are modified adding new images or deleting existing images. The friendship graph may change over time.**

## PROPOSED SYSTEM

**While intensive research interests lie in FR engines refined by social connections, the security and privacy issues in OSNs also emerge as important and crucial research topics. In [17], the privacy leakage caused by the poor access control of shared data in Web 2.0 is well studied. To deal with this issue, access control schemes are proposed in [13] and [4]. In these works, flexible access control schemes based on social contexts are investigated. However, in current OSNs, when posting a photo, a user is not required to ask for permissions of other users appearing in the photo. In [2],Besmer and Lipford study the privacy concerns on photo sharing and tagging features on Facebook. A survey was conducted in [2] to study the effectiveness of the existing countermeasure of un tagging and shows that this countermeasure is far from satisfactory: users are worrying about offending their friends when un tagging.As a result, they provide a tool to enable users to restrict others from seeing their photos when posted asa complementary strategy to protect privacy. However, this method will introduce a large number of manual tasks for end users. In [18], Squicciarini et al. propose agame-theoretic scheme in which the privacy policies are collaboratively enforced over the shared data. Each user is able to define his/her privacy policy and exposure policy. Only when a photo is processed with owner's privacy policy and co-owner's exposure policy could it be posted. However, the co-owners of a co-photo cannot be determined automatically, instead, potential co-owners could only be identified by using the tagging features on the current OSNs.**

**During the process of privacy regulation, we strive to match the achieved privacy level to the desired one. Unfortunately, on most current OSNs, users have no control over the information appearing outside their profile page. In , Thomas, Grier and Nicol examine how the lack of joint privacy control can inadvertently reveal sensitive information about a user. To mitigate this threat, they suggest Facebook's privacy model to be adapted to achieve multi-party privacy. In these works, flexible access control schemes based on social contexts are investigated. However, in current OSNs, when posting a photo, a user is not required to ask for permissions of other users appearing in the photo. In , Besmer and Lipford study the privacy concerns on photo sharing and tagging features on Facebook. A survey was conducted in to study the effectiveness of the existing countermeasure of un tagging and shows that this countermeasure is far from satisfactory: users are worrying about offending their friends when un tagging. As a result, they provide a tool to enable users to restrict others from seeing their photos when posted as a complementary strategy to protect privacy. However, this method will introduce a large number of manual tasks for end users. In Squicciarini et al.**

propose a game-theoretic scheme in which the privacy policies are collaboratively enforced over the shared data. Basically, in our proposed one-against-one strategy a user needs to establish classifiers between self, friend and friend, friend also known as the two loops in Algorithm. 2. During the first loop, there is no privacy concerns of Alice's friend list because friendship graph is undirected. However, in the second loop, Alice need to coordinate all her friends to build classifiers between them. According to our protocol, her friends only communicate with her and they have no idea of what they are computing for .

```
Algorithm 1: Iterative Method to Compute uij
Input: Positive samples Xi, Negative samples Xj
Output: The classifier uij(_)
Initial _; u0i; u0j; _0i ; _0j as vectors of all zeros;
A = 2Xi(_ + 4_I)□1XTi ;
for t = 0, 1, 2... do
B = 1 + 2Xi(_ + 4_I)□1(_ti □ _tj□ 2_utj)
;u_t+1 = qd(A;B);
ut+1i = 2(_ + 4_I)□1[XTi _t+1 □ (_ti □ _tj) + 2_utj ];
if jut+1i □ utij <threshold then
break;
else
a_t+1i = _ti + _(ut+1i □ ut+1j );
send ut+1i and _t+1i to user j;
request ut+1j and _t+1j from user j;
end
end
return ut+1i ;
```

```
Algorithm: Classifier Computation Algorithm
Initial as Ci = ;; 8i 2 N ;
for i 2 N do
for j 2 Bi do
if uij * Ci then
uij = F(Xi;Xj);
uji = 肾uij ;
Ci = fuij ; Cig; Cj = fuji; Cjg;
end
end
end
for i 2 N do
for k; j 2 Bi jj k 6= j do
if ukj * Ck then
ukj = F(Xk;Xj);
else
Request ujk from user j;
end
Ci = fujk; Cig;
end
end
```

## ADVANTAGES

- Secret Sharing Photo Unknown Person cannot Access The Photos And Any Data Its Access Permission only .

## PROPOSED SYSTEM ALGORITHMS

According to algorithms: there are two steps to build classifiers for each neighborhood: firstly find classifiers of fself, friendg for each node, then find classifiers of ffriend, friendg. Notice that the second step is tricky, because the friend list of the neighborhood owner could be revealed to all his/her friends. On the other hand, friends may not know how to communicate with each other.

## Homomorphic Encryption Algorithm:

Homomorphic encryption is a form of encryption that allows computations to be carried out on ciphertext, thus generating an encrypted result which, when decrypted, matches the result of operations performed on the plaintext. Homomorphic encryption would allow the chaining together of different services without exposing the data to each of those services.

```
public class EncryptionDecryptionAES {

	static Cipher cipher;

	public static void main(String[] args) throws Exception {

		KeyGenerator keyGenerator = KeyGenerator.getInstance("AES");

		keyGenerator.init(128);

		SecretKey secretKey = keyGenerator.generateKey();

		cipher = Cipher.getInstance("AES");

		String plainText = "AES Symmetric Encryption Decryption";

		System.out.println("Plain Text Before Encryption: " + plainText);

		String encryptedText = encrypt(plainText, secretKey);

		System.out.println("Encrypted Text After Encryption: " + encryptedText);
```

```
                        String decryptedText =
decrypt(encryptedText, secretKey);

                        System.out.println("Decrypted Text
After Decryption: " + decryptedText);

            }



            public static String encrypt(String plainText,
SecretKey secretKey)

                                    throws Exception {

                        byte[] plainTextByte =
plainText.getBytes();

                        cipher.init(Cipher.ENCRYPT_MODE,
secretKey);

                        byte[] encryptedByte =
cipher.doFinal(plainTextByte);

                        Base64.Encoder encoder =
Base64.getEncoder();

                        String encryptedText =
encoder.encodeToString(encryptedByte);

                        return encryptedText;

            }



            public static String decrypt(String encryptedText,
SecretKey secretKey)

                                    throws Exception {

                        Base64.Decoder decoder =
Base64.getDecoder();

                        byte[] encryptedTextByte =
decoder.decode(encryptedText);

                        cipher.init(Cipher.DECRYPT_MODE,
secretKey);

                        byte[] decryptedByte =
cipher.doFinal(encryptedTextByte);

                        String decryptedText = new
String(decryptedByte);

                        return decryptedText;

            }

}
```

**Modules Description:**

**Photo privacy:**

Users care about privacy is 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. In our system, we ask each of our users to establish a private photo set of their own. We use these private photos to build personal FR engines based on the specific social context and promise that during FR training, only the discriminating rules are revealed but nothing else 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.

**Steps :**

1. Login with valid details
2. Click add post
3. Post title
4. Post user type
5. Add Description
6. Add Location
7. Add Privacy for photo
8. Select Image

**Social network:**

study the statistics of photo sharing on social networks and propose a three realms model: “a social realm, in which identities are entities, and friendship a relation; second, a visual sensory realm, of which faces are entities, and co-occurrence in images a relation; and third, a physical realm, in which bodies belong, with physical proximity being a relation.” They show that any two realms are highly correlated. Given information in one realm, we can give a good estimation of the relationship of the other realm. Stone et al., for the first time, propose to use the contextual information in the social realm and co photo relationship to do automatic FR. They define a pair wise conditional random field (CRF) model to find the optimal joint labeling by maximizing the conditional density. Specifically, they use the existing labeled photos as the training samples and combine the photo co occurrence statistics and baseline FR score to improve the accuracy of face annotation. discuss the difference between the traditional FR system and the FR system that is designed specifically for OSNs. They point out that a customized FR system for each user is expected to be much more accurate in his/her own photo collections. social networks such as Face book. Unfortunately, careless photo posting may reveal privacy of individuals in a posted photo. To curb the privacy leakage, we proposed to enable individuals potentially in a photo to give the permissions before posting a co-photo. We designed a privacy-preserving FR system to identify individuals in a co-photo.

Steps :

1. Register user
2. View Profile
3. Add Post
4. Search post Based on Keyword
5. Search post Based on Content
6. Search Friend
7. Search History
8. View All Request
9. Find the stranger

Friend list:Basically, in our proposed one-against-one strategy a user needs to establish classifiers between self, friend and friend, friend also known as the two loops in Algorithm. 2. During the first loop, there is no privacy concerns of Alice’s friend list because friendship graph is undirected. However, in the second loop, Alice need to coordinate all her friends to build classifiers between them. According to our protocol, her friends only communicate with her and they have no idea of what they are computing for. Friend list could also be revealed during the classifier reuse stage. For example, suppose Alice want to find ubt between Bob and Tom, which has already been computed by Bob. Alice will first query user k to see if ukj has already been computed. If this query is made in plaintext, Bob immediately knows Alice and Bob are friends. To address this problem, Alice will first make a list for desired classifiers use private set operations in [10] to query against her neighbors’ classifiers lists one by one. Classifiers in the intersection part will be reused. Notice that even with this protection, mutual friends between Alice and Bob are still revealed to Bob, this is the trade-off we made for classifiers reuse. Actually, OSNs like Face book shows mutual friends anyway and there is no such privacy setting as “hide mutual friends”

Stets:

1. Login with valid details
2. Search Friend
3. View the friend List
4. Send the friend request
5. Accept the friend request

Collaborative Learning:

To break this dilemma, we propose a privacy-preserving distributed collaborative training system as our FR engine. In our system, we ask each of our users to establish a private photo set of their own. We use these private photos to build personal FR engines based on the specific social context and promise that during FR training, only the discriminating rules are revealed but nothing else. propose to use multiple personal FR engines to work collaboratively to improve the recognition ratio. Specifically, they use the social context to select the suitable FR engines that contain the identity of the queried face image with high probability This data isolation property is the essence of our secure collaborative learning model and the detailed security analysis.

Steps

1. Login

2. View your friend list
3. check the rank of mutual friends
4. check the circle of friendlist
5. select the friend list
6. accept the request
7. reject the request

## 2. SYSTEM STUDY

### 2.1 FEASIBILITY STUDY

The feasibility of the project is analyzed in this phase and business proposal is put forth with a very general plan for the project and some cost estimates. During system analysis the feasibility study of the proposed system is to be carried out. This is to ensure that the proposed system is not a burden to the company. For feasibility analysis, some understanding of the major requirements for the system is essential.

Three key considerations involved in the feasibility analysis are

- ♦ ECONOMICAL FEASIBILITY
- ♦ TECHNICAL FEASIBILITY
- ♦ SOCIAL FEASIBILITY

### ECONOMICAL FEASIBILITY

This study is carried out to check the economic impact that the system will have on the organization. The amount of fund that the company can pour into the research and development of the system is limited. The expenditures must be justified. Thus the developed system as well within the budget and this was achieved because most of the technologies used are freely available. Only the customized products had to be purchased.

### TECHNICAL FEASIBILITY

This study is carried out to check the technical feasibility, that is, the technical requirements of the system. Any system developed must not have a high demand on the available technical resources. This will lead to high demands on the available technical resources. This will lead to high demands being placed on the client. The developed system must have a modest requirement, as only minimal or null changes are required for implementing this system.

### SOCIAL FEASIBILITY

The aspect of study is to check the level of acceptance of the system by the user. This includes the process of training the user to use the system efficiently. The user must not feel threatened by the system, instead must accept it as a necessity. The level of acceptance by the users solely depends on the methods that are employed to educate the user about the system and to make him familiar with it. His level of confidence must be raised so that he is also able to make some constructive criticism, which is welcomed, as he is the final user of the system.

## EVALUATION

Our system is evaluated with two criteria: network-wide performance and facial recognition performance. The former is used to capture the real-world performance of our design on large-scale OSNs in terms of computation cost, while the latter is an important factor for the user experience. In this section, we will describe our Android implementation first and then the experimentsto evaluate these two criteria.

### Implementation

Our prototype application is implemented on Google Nexus 7 tablets with Android 4.2 Jelly Bean (API level17) and Facebook SDK. We use Open CV Library 2.4.6to carry out the face detection and Eigen face method to Fig. System structure of our application carry out the FR. Fig.4 shows the graphical user interface (GUI). A log in/out button could be used for log in/out with Facebook. After logging in, a greeting message and the profile picture will be shown. Our prototype works in three modes: a setup mode, a sleeping mode and a working mode. Running in the setup mode, the program is working towards the establishment of the decision tree. For this purpose, the private training set Xi and neighborhood Bi need to be specified. Xi could be specified by the user with the button “Private training set”. When it is pressed, photos in the smart phone galleries could be selected and added to Xi. To setup the neighborhood Bi ,at this stage, a user needs to manually specify the set of“ close friends” among their Facebook friends with the button “Pick friends” as their neighborhood. According to the Facebook statistics, on average a user has 130friends, we assume only a small portion of them are “close friends”. In our application, each user picks up to 30 “close friends”. Notice that all the selected friends are required to install our application to carry out the collaborative training. With Xi and Bi specified, the setup mode could be activated by pressing the button “Start”. Key operations and the data flow in this mode are enclosed by a yellow dashed box on the system architecture Fig. During the training process, a socket is established exchange local training results. After the classifiers ar eobtained, decision tree is constructed and the program switches from the setup mode to the sleeping mode. Facebook allows us to create a list of friends such as“ close friends” or “Acquaintances”. We can share a photo only to friends on list. According to the proposed scheme, this friend list should be intersection of owner’s privacy policy and co-owners’ exposure policies. However in Facebook API, friend lists are read-only items, they cannot be created or updated through the current API. That means we cannot customize a friend list to share a co-photo. Currently, when the button “Post Photo” is pressed, co-owners of x are identified, then notifications along with x are send to the co-owners to request permissions. If they all agree to post x, x will be shared on the owner’s page like a normal photo. In this sense, users could specify their privacy policy but their exposure policies are either everybody on earth or nobody depending on their attitude toward x. The data flow for a photo posting activity is illustrated by the solid red arrows. After the requests are sent out, the program will go back to the sleeping mode. If Xi or Bi is modified, the program will be invoked to the setup mode. In this case, the operations in the yellow dashed box will be performed again and decision tree will be updated.

### Network-wide performance

At this stage, a large number of users are absent for
us to carry out the network-wide evaluation. We simulate
a real-life social network with the small-world network[24]. The simulations are conducted on a desktop with Intel i3 550 3.4 GHz and 4.0 GB memory. We use the database of "Face Recognition Data, University of Essex, UK" to assign training set for each simulatedusers. The database contains photos for 395 individuals and 20 images per individual with varying poses andfacial expressions. Users are assigned with photos from the same individual randomly.

In a small world network, there are three input parameters:the total number of vertex N, the averagenode degree _D and rewire probability p. In the rest of this section, we use _D and the number of neighbors interchangeably to denote the average number of users in one's neighborhood. To construct a small-world network, first we arrange the vertices and connect them in a ring. Then we connect every vertex with its _D nearest neighbors. Finally, for each vertex, with probability p, its existing edge is rewired with another randomly selected vertex. It is shown in [14] that the rewire probability is highly related to the geodesic distance (the average shortest distance between any two vertices). We want to show that in a small-world network, there exist a lot of complete sub graphs, which greatly reduces the setup time by reusing the existing classifiers. Due to resource limitations, we simulate on a network with 3000 vertices. The the computation cost is measured by total computation time. Figure both plot our simulation results in a network of 3000 nodes with a fixed rewire probability of 0.3 and a varying _D from 6 to 18. Specifically, as in Fig, the one-against-all (OVA) approach and our proposed one against- one (OVO) approach are compared in terms of total computation cost. We can see that the computation cost of the proposed OVO approach is much lower and the efficiency gain is increasing with number of neighbors. In the previous section, we argued that this phenomenon is caused by two reasons: first, the average number of iterations to converge in our OVO approach should be much smaller; second, the classifiers could be reused with the existence of complete sub graphs .Fig. illustrates the results for the computation cost.

Fig: total computation cost and the efficiency gain against the number of neighbors

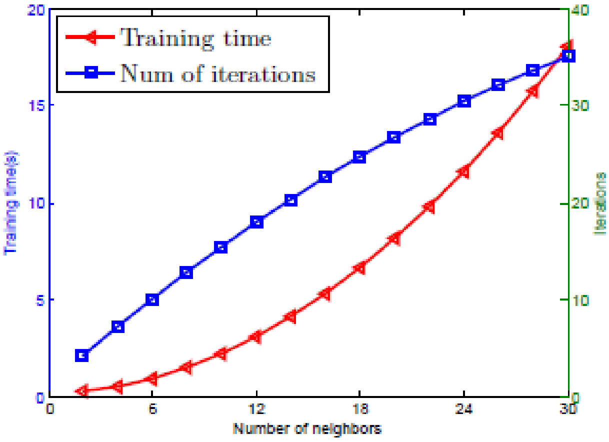


Fig: The average training time and iterations against the number of neighbors

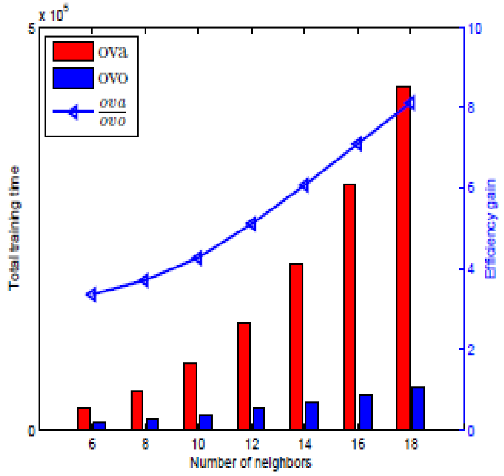
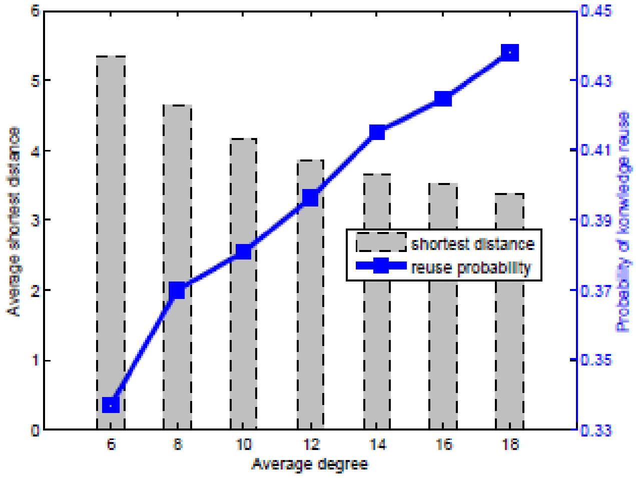


Fig: The average shortest distance and knowledge reuse proability against average degree



And the average number of iterations, which are increasing with the number of participants. In this simulation, each user has 20 training samples and each sample is a vector of 20 features. The stopping criteria is set to be 5%, which means the algorithm will return ui if its variation is less than 5% between two adjacent iterations. On the one hand, we can see from Fig.6 that for 2 users ,it only takes less than iterations to converge, while for 30 users, it takes more than 30iterations. Moreover, for 30 users, each iteration involves 30users,both the computation and communication cost are much higher than the case where there are only 2 users. As a result ,the training time in total for 30 users is 100 times more than that for 2 users. The probability of classifier reuse is studied in Fig in which we plot the probability of reuse together against the average shortest distance. By reusing a classifier, we mean that when user i and user j attempt to compute a classifier uij , instead of conducting the iterative algorithm immediately, they first try to look up at the local table. If uij exists in the table, this classifier could here used. Fig. shows that with a small average shortest distance, the reuse probability is high because a smaller distance between vertices means the vertices are “well connected”, in which a complete sub graph is more likely to exist.

### Facial recognition performance

In this subsection, we study the recognition ratio against the number of friends and the number of strangers. Standard face detection in [23] is used for face detection and eigen face [22] is used to extract features and vectorize the training image. However, the standard eigen face method is a centralized approach, it may not be applicable to our distributed case. To address this, we assume principle components have already been extract to form a vector space S. User’s facial photos are projected into this space as feature vectors. Based on our simulation results ,we find that this modification is reasonable due to the fact that the important features on human face lie on only a few directions. Facial feature extraction is beyond the scope of this paper. Better facial feature extraction method can be applied to our system to obtain a better recognition ratio .In Fig, we show the recognition ratios of our proposed scheme and the scheme with DAG decision tree. As in Fig., when there are no strangers, both our proposed scheme and the DAG scheme could achieve every high recognition ratio of more than 80% when the number of users is fewer than 30. While in Fig ,among the users, 10% of them are strangers, we can see that the recognition ratio of our scheme has a higher recognition ratio than the DAG scheme by 5%. The reason is that our scheme is able to reject strangers. The solid line on each figure represents recognition ratio of strangers ps, which is increasing with number of users. Intuitively, if there are more users, there will be more classifiers and the chance that a stranger gets contradictory decisions will be higher. Fig. shows a similar case where there are 30% strangers. In this case, our scheme out performs the DAG scheme by 10% in terms of recognition ratio. This is achieved by the ability of identifying strangers. With 30 users, the probability of identifying a stranger is around 35%. Another criterion to measure the performance is the false positive rate. In the previous section we argued that a false positive recognition will reveal the test image to the wrong person. Thus, a low false positive rate is desirable. If there are no strangers, the false positive rate is only determined by the recognition accuracy. If there are strangers, the false positive is also determined by misclassification of the strangers. Fig illustrates both false positive rate and false negative rate of our scheme and the DAG scheme. We observe that false positive rate of our scheme is 10% lower than original DAG scheme on average. Notice that false negative recognitions could also be introduced by our stranger detection scheme, according to Fig the more users, the higher chance a user is recognized as a stranger.

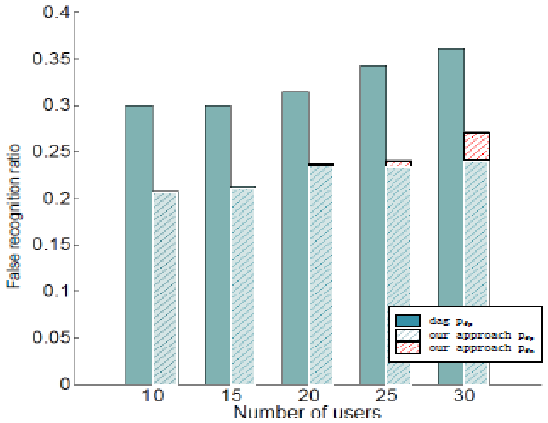
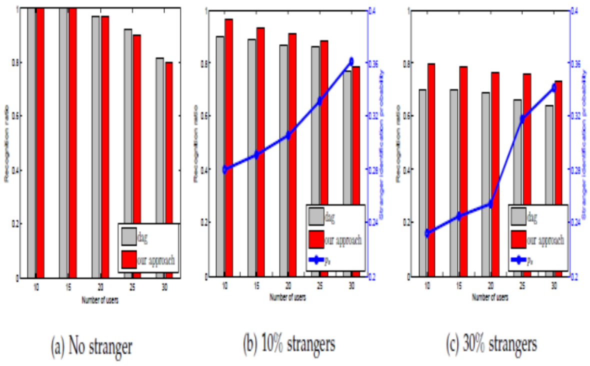


Fig: The false negative and false positive ratios

## CONCLUSION AND DISCUSSION

Photo sharing is one of the most popular features in online social networks such as Facebook. Unfortunately, careless photo posting may reveal privacy of individuals in a posted photo. To curb the privacy leakage, we proposed to enable individuals potentially in a photo to give the permissions before posting a co-photo. We designed a privacy-preserving FR system to identify individuals in 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. We expect that our proposed scheme be very useful in protecting users’ privacy in photo/image sharing over online social networks. However, there always exist trade-off between privacy and utility. For example, in our current Android application, the co-photo could only be post with permission of all the co-owners. Latency introduced in this process will greatly impact user experience of OSNs. More over, local FR training will drain battery quickly. Our future work could be how to move the proposed training schemes to.



(a) No stranger

(b) 10% strangers

(c) 30% strangers

Fig: Recognition ratio with varying number of users

## REFERENCES

[1] Bonatti P. A, Duma C, Fuchs N. E, Nejdl W, Olmedilla D, Peer J and Shahmehri N, 2006. Semantic web policies - a discussion of requirements and research issues. In *Proceedings*

*of 3rd European Semantic Web Conference,Budva, Montenegro, 11th–14th June 2006*, volume 4011 of *LNCS*, 712–724.

[2] Gavriloaie R, Nejdl W, Olmedilla D, Seamons K. E and Winslett, M. 2004. No registration needed: How to use declarative policies and negotiation to access sensitive resources on the semantic web. In Proceedings of the First European Semantic Web Symposium, Heraklion, Crete, Greece, May 10-12, 2004, volume 3053 of LNCS, 342–356. Springer.

[3] Ching-man Au Yeung, Lalana Kagal, Nicholas Gibbins, Nigel Shadbolt, "Providing Access Control to Online Photo Albums Based on Tags and Linked Data".

[4] Tootoonchian A, Gollu K. K, Saroiu S, Ganjali Y, and Wolman A. 2008. Lockr: social access control for web 2.0. In WOSP '08: Proceedings of the first workshop on Online social networks, Seattle, WA, USA, August 18, 2008, 43–48. New York, NY, USA: ACM.

[5] Yag¨ue M. I, Antonio Ma n, Lopez J, and Troya J. M. 2003. Applying the semantic web layers to access control. In DEXA '03: Proceedings of the 14th International Workshop on Database and Expert Systems Applications, 622. Washington, DC, USA: IEEE Computer Society.

[6] Agarwal S, and Sprick, B. 2004. Access control for semantic web services. In ICWS '04: Proceedings of the IEEE International Conference on Web Services, 770. Washington, DC, USA: IEEE Computer Society.

[7] B. Carminati, E. Ferrari, and A. Perego, "Rule-based access control for social networks", Springer Berlin Heidelberg, Vol.278, pp.1734 - 1744, 2006.

[8] JaeYoung Choi', Wesley De Nevel, Yong Man Ro l, and Konstantinos N Plataniotis,"Face Annotation for Personal Photos Using Collaborative Face Recognition in Online Social Networks", 16th International Conference on Digital Signal processing, pp.1-8, 2009.

[9] Barbara Carminati, Elena Ferrari, Raymond Heatherly, Murat Kantarcioglu, Bhavani Thuraisingham, "Semantic web-based social network access control", pp. 108-115, 2011.

[10] 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.

[11] Alessandra Mazzia Kristen LeFevre and Eytan Adar, "The PViz Comprehension Tool for Social Network Privacy Settings", Tech. rep., University of Michigan, 2011.

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

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

[14] Sergej Zerr, Stefan Siersdorfer, Jonathon Hare, Elena Demidova, "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.

[15] C. A. Yeung, L. Kagal, N. Gibbins, and N. Shadbolt, "Providing access control to online photo albums based on tags and linked data", pp. 9–14, 2009.

[16] Anna Cinzia Squicciarini, "Privacy Policy Inference of User-Uploaded Images on Content Sharing Sites", IEEE Transactions on Knowledge and Data Engineering, Vol. 27, no. 1, January 2015.

[17] A. C. Squicciarini, M. Shehab, and F. Paci., "Collective privacy management in social networks", In Proceedings of the 18th International Conference on World Wide Web, pp. 521–530, 2009.