Photo Sharing and Privacy Control Decisions

Ms. Nampalli Divyalaxmi R.
Department of Computer Engineering
RMDSCOE, Warje, Savitribai Phule Pune University
Pune, Maharashtra
divya.nampalli@gmail.com

Prof. Dange Trupti K.
Department of Computer Engineering
RMDSCOE, Warje, Savitribai Phule Pune University
Pune, Maharashtra
trupti.dange@gmail.com

***Abstract*—**Photo sharing is a tempting module which enhances Online Social Networks. Unfortunately, there are several security crises. All are permitted to post, comment and tag the other users. The misuse of photos can happen. We study the situation when a client shares a photograph containing people other than her (termed co-photograph for short). We need to minimize the security breaches that happen during uploading/posting the photos of people without the knowledge of people involved in photo i.e. Co-owners. As a solution for this we need a facial acknowledgement face recognition framework that can identify each user involved in the photograph. Online social network provides the attractive means of sharing information but do not provide any privacy or security policies to restrict the access to shared information. So proposed an approach to enable the security of shared information associated with multiple users in online social networks. For this concern we proposed an access control model to capture intrinsic nature of the multiparty authorization requirement along with the privacy specification scheme and a policy enforcement mechanism. We validate that our framework is better than other conceivable approaches as far as acknowledgment proportion and effectiveness. Our mechanism is executed as a proof based on prototype of Facebook's stage. Proposed application will not infect to true users and get polluted by unauthorized users and their posting the photos in unsecure way. Hence proposed social application will be secure and safest as it enforces security to shared information.

Keywords: *Photo privacy, secure multi-party computation, collaborative learning, multiparty access control, online Social networks.*

*****

I. INTRODUCTION

Social sites have become chief part of our everyday life. Social sites such as Facebook, Google+, Orkut and sound of birds are implemented to make people to post/share personal and public information, make social connections with friends, co-workers, persons having similar likings and dislikes, family, and even with strangers. Anybody can post anything on these social kind of social sites. Anybody can share any images/photos as there is no control as such for sharing information. But this kind of activities makes a permanent record which is everlasting on social sites. Later consequences can be dangerous, people may use it for different surprising and unwanted purposes. As an example a posted photo of a celebrity with mafia may reveal the mafia relationship of the celebrity. Profile of a user majorly includes statistics like with respect to the users work history, work place, birthday, age, sex, residential location, likings, education, and, travel information and contact information. To add, users upload the pictures of their known once and tag them even though if they are not interested to be the part of uploaded image/content.

When other people are tagged or their image gets shared with others the situation becomes more complicated. The user uploading the image is completely unaware of the consequences that arise after sharing of the image. Currently nobody can stop such unavoidable situation which are happening on large scale [2]. We should have a control on sharing to minimize the impact. Currently, instead of providing the security provisions, sites like Facebook, Orkut and Instagram are encouraging people to share more and more pictures to more and more people, which impacts the user's privacy.

Most of the times user does not wish that his photos get tagged or being exposed without his permission. Is it considered as violation if we share/spread the picture without taking a permission from all the people involved in picture? To provide answer this question we need to explain the privacy and security issues over the social sites.

Whenever a photograph or any sensitive information is shared it includes everybody's security, which can be put to risk, if the required permissions are not sought. We need to provide and enhance maximum level of privacy and security of the content being uploaded over OSNs. So while using the OSNs one can feel desired level of confidence, trustworthiness and security. People can confidently make use of OSNs without worrying or photos being shared in insecure and unauthorized way and without the fear of being them misused. Level of privacy and security should be enhanced [1] and it is a first important thing for a user using OSNs.

With respect to current infrastructure and implementations of OSNs, either user will feel alone because highly imposed security constraints else will be impacted by several security issues due to low security mechanisms. Many authors studied about the security challenges because of lack of collaborative control over the photos being shared over the online social sites [1]. This subject has a much importance in today's life as many people use OSNs extensively.

Users for whom privacy and security matters 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 or questions in mind.

We should have a secure approach to gain efficiency and privacy. Efficiency and privacy can be achieved by simultaneously comparing the current and previous experiments.

- The users in a shared photo are automatically detected without being tagged by somebody.
- We propose a secure sharing of private photos by making use of social context to have personal FR Engines and MPAC Model.
- Decision of Photo Sharing is entirely based on user uploading it, and he can control its sharing further.
- We can achieve privacy, security and efficiency.

A. Motivation

The existing system on which studies have been carried out shows the simple access control model. That model does not recognize the trustworthy and untrusted people on OSN. Also Social user have not been given the more freedom and privacy regarding the information which is shared. But many people yet use the OSNs. The impact and usefulness of faithful management for data sharing in social network has been explained by current work [5]. A framework for authorization is designed and studied to catch the significance of authorization requirements in OSNs.

II. Related Work

A Paper on "On the Move to Meaningful Internet Systems" by authors M B. Carminati, E. Ferrari, and A. Perego, Designed and recommended a framework for a constraint-based process modeling language and its implementation which describes about the usage of constraints for imposing limitations. This mentioned approach supports both ad-hoc and dynamic changes.

A Paper on "Face recognition for improved face annotation in personal photo collections shared on online social networks" by authors M. Bellare, C. Namprempre, and G. Neven, Proposed a new collaborative face recognition framework focuses on the correctness of face annotation by effectively making use of many Recognition engines available in an OSN. In particular collaborative FR framework consists of two major parts, select FR engines and merge multiple FR results [2]. Collaboration is explained in terms of integration of results of multiple sources. Effective solutions for integration Face Recognition results are adopted old fashioned techniques for merging many classifier results. Privacy needs are studied.

A Paper on "Moving Beyond Untagging: Photo Privacy in Tagged World" by authos Andrew Besmer & Heather Richter Lipford, Department of Software and Information Systems, Examined privacy and security concerns and mechanisms for tagged images. Using a focus group authors have explored the needs and concerns of social users, resulting in a design consideration collections for tagged photo privacy and security.[3] Proposed a privacy enhancing mechanism based on their findings and experimentation, and tested it using a mixed methods approach. Results which are studied identify the social tensions that tagging generates, and the needs of privacy tools to address photo privacy management issues.

Many authors have proposed comprehensive techniques to enhance the security and privacy, most of them have experimented and shown significant results.

III. Problem Definitiion

To design a systematic solution to facilitate collaborative management of shared data in Online Social networks. We begin by examining how the lack of collaborative or multiparty access control (MPAC) for data sharing in OSNs can undermine the protection of user data. The main aim is control of photo sharing and spreading to unauthorized users, by which security is enhanced with privacy policy specification [3].

IV. Proposed System

In Presented System, we would implement Facebook like application for the collaborative management of shared data, called MController. Application allows multiple associated users to specify their authorization policies and privacy/security preferences, to control a shared data item. It is worth noting that our current implementation was to handle photo sharing in OSNs [5]. Approach designed can be generalized to deal with other kinds of data sharing. The proposed system shows a new solution for collaborative management of shared data in OSNs.

A multiparty access control model is designed, along with a multiparty policy specification scheme and corresponding policy evaluation mechanism. In addition to this, we have introduced an approach for representing and reasoning about proposed model. Also designed guidelines to evaluate the performance of proposed solution.

A. MPAC Model

It considers the sharing decision of each individual involved in the transit, it consists of following stakeholders:
Owner: Data item in the space of a user in the OSN.
Contributor: Data item published by a user in someone else space in OSN.
Stakeholder: When data item in space of a user in the online social network. The set of tagged users associated with data item, are called a stakeholder of data item (here it is photo).
Disseminator: When data item shared by a user from someone else's space to his space.

V. System Architecure

A. Overview

This system is highly dependent on the impression of social network security. Multiparty authorization infrastructure helps you to make secure communication between trustworthy and untrusted person. We are providing the security to social site users and protection of data which is common to all user which is getting accessed in the social network website. So factor of safety is most important and it's a mandate, and sharing will be made secure by using proposed system [4].

In the architecture diagram, the first step to checks the input request against the policy specified by each controller and later it takes a decision for the controller. The accessor element in a policy decides whether the policy is applicable to a request. If the user who sends the request belongs to the user

set derived from the accessor of a policy, the policy is applicable to it and the evaluation process returns a response with the decision (either allow or refuse) indicated by the effect element in the policy, as shown in fig. 2. Response yields deny decision if the policy is not applicable to the request. In the second step, decisions from all controllers responding to the access request are aggregated to make a final decision for the access request.

B. *Objectives of Multiparty Authorization Technique*

1) Specification of security policies
2) Control of unauthorized access
3) Determine malicious activities.
4) OSN with user defined privacy policies.

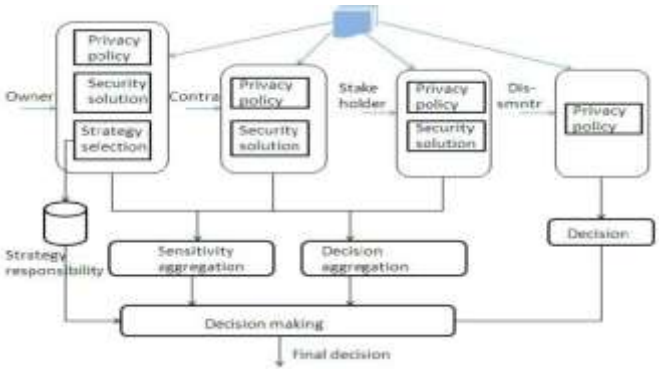

Fig. 1. Architecture of Proposed System

C. *Data Flow Diagram*

Flow Diagram that visually depicts information which is interrelated such as events, steps in a process, functions, etc., in an organized fashion, such as sequential manner. Flow diagram is a collective Data Sharing in OSNs term for a diagram representing. A flow or set of dynamic relationships in a system. Flow diagram is also used as synonym of the flowchart. Flow diagrams are used to structure and order a complex system, or to reveal the underlying structure of the elements and their interaction.

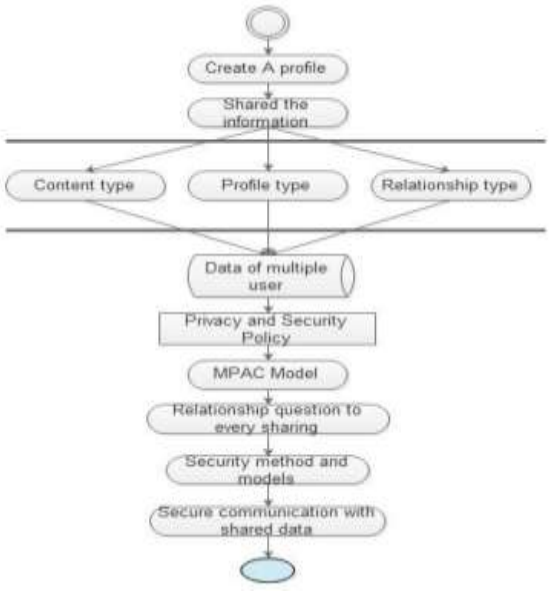

Fig. 2. Data Flow diagram of Proposed System.

VI. IMPLEMENATATION DETAILS

A. *Algorithm*

Following step are followed to implement a privacy preserving model for sharing images.

1. Identify Pi(x), list of users who can access photo x.
2. Identify Vi(x), list of users who can access photo x when user is involved.
3. Take intersection of both to get access policy.
   S=Pi(x) Vi(x)
4. Share photo to people in S.

1) *Algorithm :Classifier Computation Algorithm*

```
Initial as Ci = Φ for all I € N
    For i € N do
      For j € Bi do
        If uij  not set of ci then
          uij=F(xi,xj)
          uij=-uij
          ci=(uij,ci);cj=(uij,cj)
          End
      End
    End
For i € N do
  For j € Bi || k !=j do
    If ukj not subset of ck then
          Ukj=F(xk,xj)
    Else
          Request ujk from user j
    End
    Ci={ujk,ci}
  End
End
```

B. *Mathematical Model*

1) Let the System S=Set of whole system consist of
   S= {UR, GR, UP, RT, R, DS, CT}

UR	It is set of N number of Users.
GR	It is set of N number of groups like gr1, gr2,…gN.
UP	Is collection of N number of user profile like up1,.., upN
RT	It is set of relationship.
R	It is set of user relationship like r1, r2, rN.
DS	It is set of Dataset.
CT	It is set of controller type like owner, contributor, stakeholder, disseminator.

Decision voting:

DV =Decision Voting Value

$$DV = \begin{cases} 0 & if evaluation(P)=Deny \\ 1 & if evaluation(P)=Permit \end{cases}$$

$$DV_{ag} = \left(DV_{ow} + DV_{cb} + \sum_{i \in SS} DV_{st}^{i} \right) \times \frac{1}{m}$$

Sensitivity Voting:

Sc =Sensitivity Score

$$Sc = \left(SL_{ow} + SL_{cb} + \sum_{i \in SS} SL_{st}^{i} \right) \times \frac{1}{m}$$

C. Experimental Setup

The System is built using the Java Framework (version jdk 1.8) on the windows platform. The Eclipse IDE (version 2.0.0) is used as a development tool. Mysql is used to store the dataset. The Apache Tomcat server is used for deployment of the application. The system does not require any specific platform o run, as standard machine is capable to run the application. The system analysis is carried out.

VII. Results and Discussion

Different modules to be implemented which are part of the application are covered in the below section:

A. Login Screen

Very first screen of the system, where use needs to enter the credentials to get authorized by the system.

Fig. 3. Home Page screen of system.

Fig. 4. Login screen of system.

B. Profile Inforamtion

It contains the user's profile information like name, DOB, place, academic details, contact numbers, profile picture, etc.

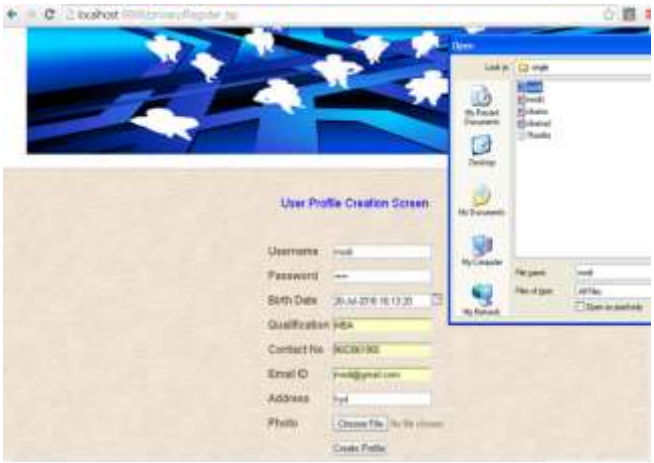

Fig. 5. Profile creation screen of system.

C. Friend request and acceptance

Users can see the available list of users who use the social site. The can send friend request to anybody ad same they can accept the friend request from others.

Fig. 6. Friend request and acceptance screen.

D. Upload and Share Images

User will be able to upload the group photos, that he wish to and share it across his friends. This is very important module as the privacy specifications are done here and decisions are taken for the control of photo sharing.

Fig. 7. Upload screen for the picture.

Fig. 8. Uploaded the picture will be visible once it is approved by the co-owners.

VIII. CONCLUSION

A multiparty access control model is designed using a policy specification and evaluation scheme. Solution is designed with proof-of-concept implementation called MController. For future, we will plan to study more comprehensive privacy conflict resolutions for data being shared across. We would explore more standards to evaluate the features of proposed MPAC model. For the management study of large number of photos and information users will be involved. As a solution to this, we would study inference-based techniques for automatically configure privacy preferences for OSN. One more area which we would study is systematically integrating the idea of trust and reputation into MPAC model and investigate a comprehensive solution to cope with collusion attacks which will provide a robust MPAC service in OSNs.

ACKNOWLEDGMENT

I would like to acknowledge my vigorous thanks to Prof. Trupti K. Dange for giving her valuable suggestions I also express my special thanks to my friends for supporting me in my research work.

REFERENCES

[1] I Altman Privacy regulation Culturally universal or culturally specific Journal of Social Issues 33 3 66 84 1977

[2] A Besmer and H Richter Lipford Moving beyond untagging photo privacy in a tagged world CHI '10 pages 1563 1572 New York NY USA 2010 ACM

[3] S Boyd N Parikh E Chu B Peleato and J Eckstein Distributed optimization and statistical learning via the alternating direction method of multipliers Found Trends Mach Learn 3 1 1 122 Jan 2011

[4] J Y Choi W De Neve K Plataniotis and Y M Rao, Improved face annotation and Collaborative face recognition Multimedia IEEE Transactions on 13 1 14 28 2011

[5] B Carminati E Ferrari and A Perego, Rule based access control for social networks, OTM 2006 Workshops,Science pages 1734 1744 Springer Berlin Heidelberg 2006

[6] Kaihe Xu, Student Member, IEEE, Yuanxiong Guo, Member, IEEE, Linke Guo, Member, IEEE,Yuguang Fang, Fellow, IEEE, Xiaolin Li, Member, IEEE, My Privacy My Decision: Control of Photo Sharing on Online Social Networks. 10.1109/TDSC.2015.2443795, IEEE Transactions on Dependable and Secure ComputingG. Eason, B. Noble, and I.N. Sneddon, “On certain integrals of Lipschitz-Hankel type involving products of Bessel functions,” Phil. Trans. Roy. Soc. London, vol. A247, pp. 529-551, April 1955. (*s*)