Journal of Engineering Sciences
Vol 11, Issue 4 , April/2020
ISSN NO:0377-9254

TRUST BASED PRIVACY POLICY PHOTO SHARING IN ONLINE SOCIAL NETWORKS

Dr.P.C.SENTHIL MAHESH[1], N.UZMA[2], S.SABEEHA[3], G.REVATHI[4], K.SAI VINEEL[5]
[1]Professor, Dept of CSE, AITS, Rajampet, AP, India.
[2,3,4,5]Student, Dept of CSE, AITS, Rajampet, AP, India.

Abstract— With the development of social media technologies, sharing photos in online social networks has now become a popular way for users to maintain social connections with others. However, the rich information contained in a photo makes it easier for a malicious viewer to infer sensitive information about those who appear in the photo. How to deal with the privacy disclosure problem incurred by photo sharing has attracted much attention in recent years. When sharing a photo that involves multiple users, the publisher of the photo should take into all related users' privacy into account. In this paper, we propose a trust-based privacy preserving mechanism for sharing such co-owned photos. The basic idea is to share photo based on trust value acceptance by owners. A owner can give trust value acceptance for friends and friends of friends, based on trust value acceptance the photos will be visible to friends and friends of friends. Simulation results demonstrate that the trust-based photo sharing mechanism is helpful to reduce the privacy loss, and the proposed threshold tuning method can bring a good payoff to the user.

Keywords- social trust, anonymization, privacy preserving, photo sharing, online social networks.

I. INTRODUCTION

Social media, which enable people to interact with each other by creating and sharing information, has now become an importation part of our daily life. Users of social media services create a huge amount of information in forms of text posts, digital photos or videos. Such user-generated content is the lifeblood of social media. However, user-generated content usually involves the creator's sensitive information, which means the sharing of such content may compromise the creator's privacy. How to deal with the privacy issues caused by information sharing is a long active topic in the study of social media. A major form of the content sharing activities in social media websites is the sharing of digital photos. Some popular online social networking services, such as Instagram1, Flicker2, and Pinterest3, are mainly designed for photo sharing. Compared to textual data, photos can deliver more detailed information to the viewer, which is detrimental to individual's privacy. Moreover, the background information contains in a photo may be utilized by a malicious viewer to infer one's sensitive information. On the good side, it is more convenient for a user to hide his sensitive information, without too much damage to insensitive information, by sharing image based on user trusted values. In this paper we study the privacy issue raised by photo sharing in online social networks (OSNs). Privacy policies in current OSNs are mainly about how a user's information will be explored by the service provider, and through which methods a user can control the scope of information sharing. Most OSNs offer a privacy setting function to their users.

A user can specify, usually based on his relationships with others, which users are allowed to access the photo he shares. It should be noted that the photo shared by a user may relate to other users. If the sharing of such photos is fully controlled by one user, then the privacy of other related users may be compromised. This privacy issue can be further explained via the following example. Suppose that Alice takes a photo of herself and her friend Bob, and then shares the photo to her colleague Charlie without telling Bob. If Bob does not know Charlie well, then the sharing of the photo will becomes a privacy invasion to Bob. In the above example, the photo is actually co-owned by Alice and Bob. When Alice wants to share the photo with others, she should solicit Bob's opinion, or at least, she should take some measures to reduce the possible privacy loss to Bob. For example, Alice can use a photo editing tool to make Bob's face blurred, so that Bob can hardly be identified by Charlie. Given a photo, or more generally, a data item, related users usually have different opinions on whether a user is allowed to access it. Researchers have proposed different approaches to resolve the conflicts among users' access control policies.

In most studies, an aggregated policy, which is essentially a set of users who are authorized to access the data item, will be generated by a mediator (e.g. the service provider). In our work, a trust-based mechanism is proposed for collaborative privacy management in OSNs. The proposed mechanism requires a user to solicit related users' opinions before sharing a data item with others. The trust values between users are

utilized to generate an aggregated option. By comparing the aggregated option with a threshold, the user decides whether to share the data item.

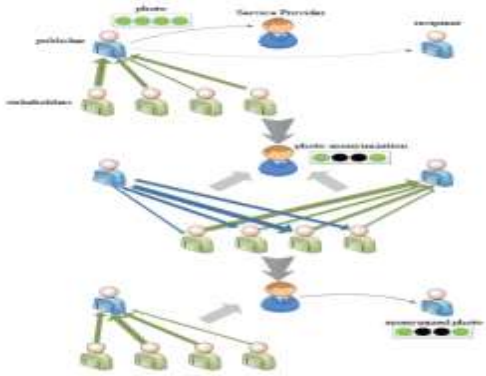


Fig.1: System Architecture

To find a balance between privacy preserving and photo sharing, we propose a method to make the threshold adaptive to the trust relationship between users. The main contributions of this paper are summarized as follows: A trust-based mechanism is proposed for photo sharing in OSNs. The trust values between users are utilized to determine whether a user's privacy will be protected. The trust values are updated according to the privacy loss, and the proposed mechanism can prevent the user from ignoring other users' privacy. To balance between photo sharing and privacy preserving, we propose a method to tune the threshold that determines the number of users deleted from a photo. We have conducted a series of simulations to demonstrate the effectiveness of the proposed methods.

II. EXISTING SYSTEM

A privacy-preserving photo sharing framework which uses visual obfuscation technique to protect user's privacy. When processing a photo, the proposed framework considers both the content and the context of a photo. Current System does not provide trust based photo sharing between friends.

DRAWBACKS:

- There is no Trust value for Users in Photo Sharing in online social network.
- Less security due to no fine-grained privacy management of photo sharing.

III. PROPOSED SYSTEM

In the proposed, the system considers a photo-sharing scenario where the user who publishes the photo, referred to as publisher, decides how to process the photo so as to protect privacy of related users. A trust-based mechanism is proposed to help the publisher make a proper decision. Instead, the publisher predicts the privacy loss to each related user in case that the photo is shared with a certain user based on trusted value.

ADVANTAGES:

- More Security due to Trust-based Photo Anonymization and Trust-based Privacy-Preserving Approaches.
- Trust based photo sharing protects users data access by other users.

SYSTEM ARCHITECTURE

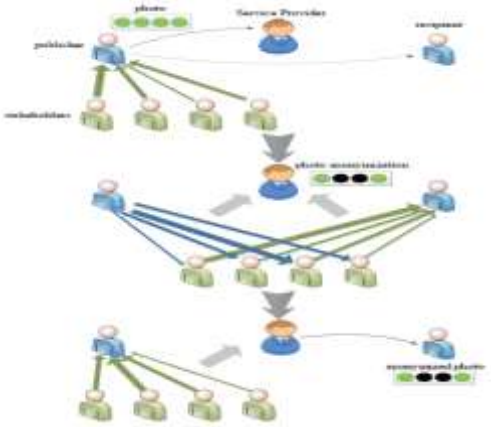


Fig.2: Cloud Centric Authentication Architecture

MODULES

Admin Module

Administrator Module Provides Add Image, View all Images with Policy, View All Images Ranking, View All Image Details, View Search History, View All Users.

User Module

User Module Provides Add Images, Trust Value Acceptance to Users, Sharing of Images, Search of Images and View of Images Based on trust Value.

UML DIAGRAMS

UML stands for Unified Modeling Language. UML is a standardized general-purpose modeling language in the field of object-oriented software engineering. The standard is managed, and was created by, the Object Management Group.

The goal is for UML to become a common language for creating models of object oriented computer software. In its current form UML is comprised of two major components: a Meta-model and a notation. In the future, some form of method or process may also be added to; or associated with, UML.

The Unified Modeling Language is a standard language for specifying, Visualization, Constructing and documenting the artifacts of

software system, as well as for business modeling and other non-software systems.

The UML represents a collection of best engineering practices that have proven successful in the modeling of large and complex systems.

The UML is a very important part of developing objects oriented software and the software development process. The UML uses mostly graphical notations to express the design of software projects.

GOALS

The Primary goals in the design of the UML are as follows:

1. Provide users a ready-to-use, expressive visual modeling Language so that they can develop and exchange meaningful models.
2. Provide extendibility and specialization mechanisms to extend the core concepts.
3. Be independent of particular programming languages and development process.
4. Provide a formal basis for understanding the modeling language.
5. Encourage the growth of OO tools market.
6. Support higher level development concepts such as collaborations, frameworks, patterns and components.
7. Integrate best practices.

The development for the world wide web while making some things simpler, has exacerbated these architectural problems.

- Class diagram
- Use case diagram
- Sequence diagram
- Activity diagram

CLASS DIAGRAM

In software engineering, a class diagram in the Unified Modeling Language (UML) is a type of static structure diagram that describes the structure of a system by showing the system's classes, their attributes, operations (or methods), and the relationships among the classes. It explains which class contains information.

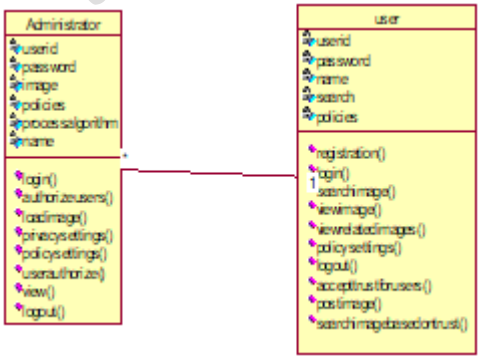


Fig.3: Class Diagram

USE CASE DIAGRAM

A use case diagram in the Unified Modeling Language (UML) is a type of behavioral diagram defined by and created from a Use-case analysis. Its purpose is to present a graphical overview of the functionality provided by a system in terms of actors, their goals (represented as use cases), and any dependencies between those use cases. The main purpose of a use case diagram is to show what system functions are performed for which actor. Roles of the actors in the system can be depicted.

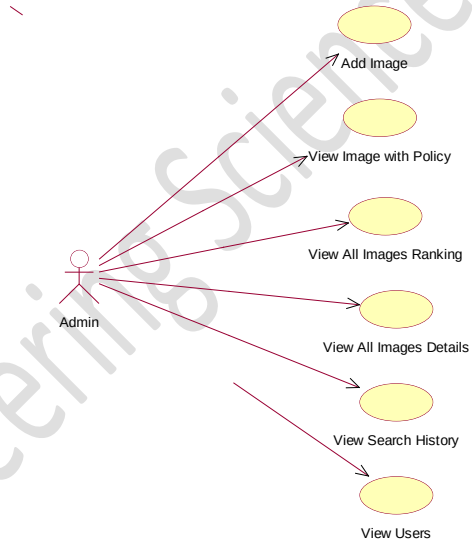
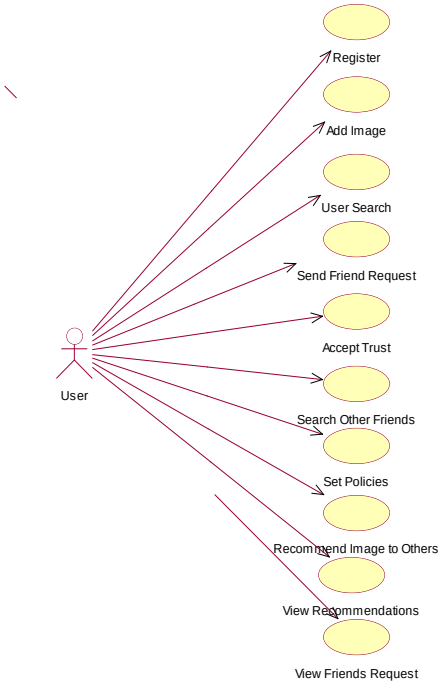


Fig.4: Use Case Diagram



SEQUENCE DIAGRAM

A sequence diagram in Unified Modeling Language (UML) is a kind of interaction diagram that shows how processes operate with one another and in what order. It is a construct of a Message Sequence Chart. Sequence diagrams are sometimes called event diagrams, event scenarios, and timing diagrams.

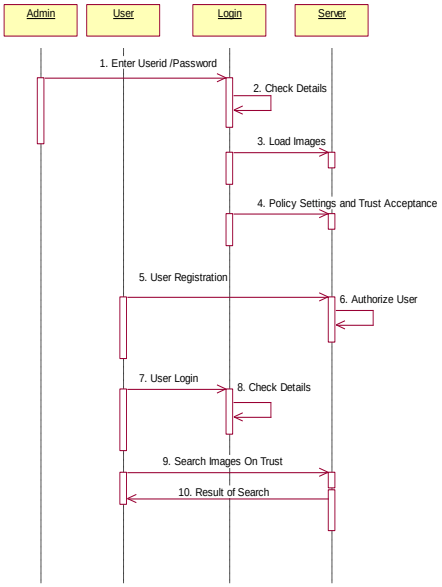


Fig.5: Sequence Diagram

ACTIVITY DIAGRAM

Activity diagrams are graphical representations of workflows of stepwise activities and actions with support for choice, iteration and concurrency. In the Unified Modeling Language, activity diagrams can be used to describe the business and operational step-by-step workflows of components in a system. An activity diagram shows the overall flow of control.

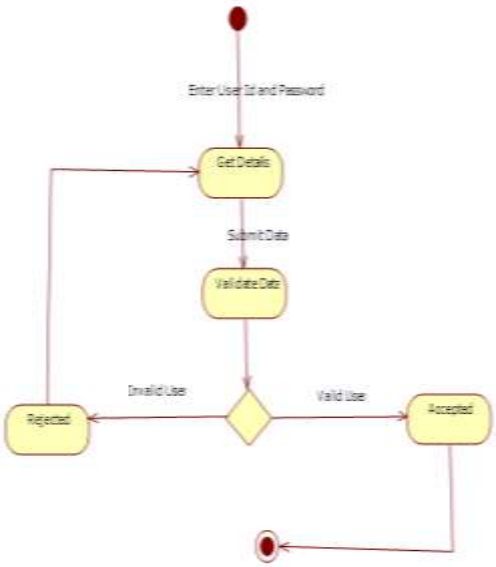


Fig.6: Activity Diagram

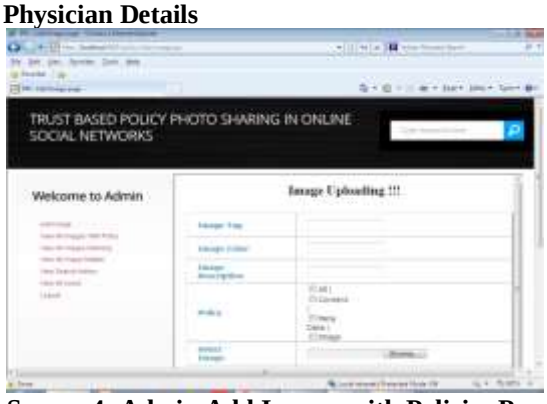
IV. OUTPUTS

Screen 1: Home Page of Project

Screen 2: Admin Login Page

Screen 3: Admin Menu Page

Physician Details



Screen 4: Admin Add Images with Policies Page

Journal of Engineering Sciences
Vol 11, Issue 4 , April/2020
ISSN NO:0377-9254

Screen 5: List of Images with Policies

Screen 6: User Information View

Screen 7: List of Images with Rank

Screen 8:List of Images with User Content

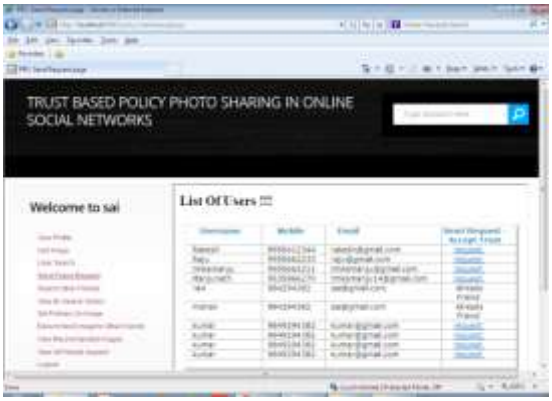
Screen 9: Report Showing List of Users

Screen 10: Report Showing List of Users with Authorization

Screen 11: User Login Page

Screen 12: User Menu Page

Screen 13: List of Users with Trust Acceptance



Screen 14: Report showing List of Trust Acceptance

Screen 15: Menu to Search Trusted user Data

Screen 16: User Searching Friends Information

Screen 17: User Searching Based on Trusted Friend

V. CONCLUSION

Sharing one co-owned photo in an OSN may compromise multiple users' privacy. To deal with such a privacy issue, in this paper we propose a privacy-preserving photo sharing mechanism which utilizes trust values to decide how a photo should be anonymized. The photo that a user wants to share is temporarily holden by the service provider. Based on the trust relationship between users, the service provider estimates how much privacy loss the sharing of the photo can bring to a stakeholder. Then by comparing the privacy loss with a threshold specified by the publisher, the service provider decides if a stakeholder should be deleted from the photo. After the photo is shared, each stakeholder evaluates the privacy loss he has really suffered, and his trust in the publisher changes accordingly. This trust-based mechanism motivates the publisher to protect the stakeholders' privacy. However, the anonymization operation leads a loss in the shared information. Considering that the threshold specified by the publisher controls the trade-off between privacy preserv- ing and information sharing, we propose a service providerassisted method to help the publisher to tune the threshold. By using synthetic network data and real-world network data, we conduct a series of simulations to verify the proposed photo sharing mechanism and the threshold tuning method. Simulation results demonstrate that incorporating trust values into the photo anonymization process can help to reduce user's privacy loss, and adaptively setting the threshold is necessary for the publisher to balance between privacy preserving and photo sharing.

VI. FUTURE WORK

In current study, we mainly focus on the sharing between one publisher and one receiver. Considering that in practice, a user generally shares a photo with multiple users simultaneously, we'd

like to investigate such a one-to-many case in future work. The proposed threshold tuning method can be seen as a greedy method, in the sense that the publisher prefers to choose the threshold that brings him the maximal instant payoff. Due to the correlation between privacy loss and trust values, current choice of the threshold will affect the publisher's future payoffs. In future work, we'd like to investigate how to modify the tuning method so as to achieve a better result.

REFERENCES

[1] W. G. Mangold and D. J. Faulds, "Social media: The new hybrid element of the promotion mix," Business horizons, vol. 52, no. 4, pp. 357–365, 2009.
[2] A. M. Kaplan and M. Haenlein, "Users of the world, unite! The challenges and opportunities of social media," Business horizons, vol. 53, no. 1, pp. 59–68, 2010.
[3] J. A. Obar and S. S. Wildman, "Social media definition and the governance challenge-an introduction to the special issue," 2015.
[4] L. Xu, C. Jiang, J. Wang, J. Yuan, and Y. Ren, "Information security in big data: Privacy and data mining," IEEE Access, vol. 2, pp. 1149–1176, 2014.
[5] S. K. N, S. K, and D. K, "On privacy and security in social media a comprehensive study," Procedia Computer Science, vol. 78, pp. 114 – 119, 2016, 1st International Conference on Information Security and Privacy 2015. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1877050916000211
[6] C. Fiesler, M. Dye, J. L. Feuston, C. Hiruncharoenvate, C. Hutto, S. Morrison, P. Khanipour Roshan, U. Pavalanathan, A. S. Bruckman, M. De Choudhury, and E. Gilbert, "What (or who) is public?: Privacy settings and social media content sharing," in Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing, March 2017, pp. 567–580.
[7] A. C. Squicciarini, M. Shehab, and F. Paci, "Collective privacy management in social networks," in Proceedings of the 18th ACM International Conference on World Wide Web, April 2009, pp. 521–530.
[8] H. Hu, G.-J. Ahn, and J. Jorgensen, "Detecting and resolving privacy conflicts for collaborative data sharing in online social networks," in Proceedings of the 27th ACM Annual Computer Security Applications Conference, December 2011, pp. 103–112.
[9] J. M. Such and N. Criado, "Resolving multi-party privacy conflicts in social media," IEEE Transactions on Knowledge and Data Engineering, vol. 28, no. 7, pp. 1851–1863, July 2016.
[10] L. Xu, C. Jiang, Y. Qian, Y. Zhao, J. Li, and Y. Ren, "Dynamic privacy pricing: A multi-armed bandit approach with time-variant rewards," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 2, pp. 271–285, February 2017.
[11] M. Duggan and J. Brenner, "The demographics of social media users 2012," 2013.
[12] L. Yuan, P. Korshunov, and T. Ebrahimi, "Privacy-preserving photo shar- ing based on a secure jpeg," in *Computer Communications Workshops*, 2015, pp. 185–190.
[13] K. Xu, Y. Guo, L. Guo, Y. Fang, and X. Li, "My privacy my decision: Control of photo sharing on online social networks," *IEEE Transactions on Dependable and Secure Computing*, vol. 14, no. 2, pp. 199–210, March 2017.
[14] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute- based encryption," in *IEEE Symposium on Security and Privacy*, 2007, pp. 321–334.
[15] C. Ma, Z. Yan, and C. W. Chen, "Scalable access control for privacy- aware media sharing," *IEEE Transactions on Multimedia*, pp. 1–1, 2018.
[16] P. Ilia, I. Polakis, E. Athanasopoulos, F. Maggi, and S. Ioannidis, "Face/off: Preventing privacy leakage from photos in social networks," in *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '15, 2015, pp. 781–792.
[17] L. Chao, W. Wang, and Y. Guo, "A fine-grained multiparty access control model for photo sharing in osns," in *IEEE First International Conference on Data Science in Cyberspace*, 2016, pp. 440–445.
[18] N. Vishwamitra, Y. Li, K. Wang, H. Hu, K. Caine, and G.-J. Ahn, "Towards pii-based multiparty access control for photo sharing in online social networks," in *Proceedings of the 22Nd ACM on Symposium on Access Control Models and Technologies*, June 2017, pp. 155–166.
[19] W. Sherchan, S. Nepal, and C. Paris, "A survey of trust in social networks," *ACM Computing Surveys*, vol. 45, no. 4, pp. 47:1–47:33, August 2013.
[20] A. Datta, S. Buchegger, L. H. Vu, T. Strufe, and K. Rzadca, *Decentral- ized Online Social Networks*, 2010.