PROPHYLACTIC ONLINE SOCIAL NETWORK BASED ON USER PREFERENCE WITH PRIVACY PRESERVATION TECHNIQUE

Bhavani.S[1], Mageswari.K[2], Deepa.D[3(ASSISTANT PROFESSOR)]

Department Of Computer Science and Engineering.
Prince Dr.K.Vasudevan College Of Engineering and Technology,
Chennai, Tamil Nadu, India.

ABSTRACT

Users and resources in online social networks (OSNs) are interconnected via various types of relationships. In particular, user-to-user relationships form the basis of the OSN structure, and play a significant role in specifying and enforcing access control. Individual users and the OSN provider should be enabled to specify which access can be granted in terms of existing relationships. In this paper, we propose a novel user-to-user relationship based access control (UURAC) model for OSN systems that utilizes regular expression notation for such policy specification. Access control policies on users and resources are composed in terms of requested action, multiple relationship types, the starting point of the evaluation, and the number of hops on the path. In this system, Mutual Balanced Privacy preservation Algorithm (MBPA) is used to determine whether the required relationship path between users to be offered or not. We offer the opportunity to every OSN users to offer the right privacy for all their friends in the network. Our approach gives the way to protect our friends from the unrelated friend's network. Access control policies on users and resources are composed in terms of requested action, multiple relationship types. We validate the feasibility of our approach by implementing a prototype system and evaluating the performance of these two algorithms.

Keywords–*Access Control, Mutual Relationship, Online Social Network, Social Network Sites*

1. INTRODUCTION

This document tells us about the use of Online Social Network that is used by large number of people all over the world and the security that is provided by the OSNs. Some network are used to share only videos. But in some Online Social Networks like "Facebook" not only videos but also all type of information are shared in that network. Many users are joining the OSNs are generally they are connected to each other and share a large amount of information which may be private or public. These information sharing are kept secured since there are more options are available in each OSNs where they provide security and that gives user a privacy for sharing any form of information. The Security and privacy in OSNs are maintained well in both media and research community [1], [10]. These views indicates that there is a need for access control for any unauthorized access over the OSNs. An Access Control in every network there are more unique characteristic that provides more security and privacy for sharing the information. Here, the user and resources are more considered since more information is shared between them such as photos, videos, songs, etc,. and other information (such as photo tagging) where they can me exposed, since not all the users are aware of using the privacy options in the OSNs. There are more policies and specifications that are based on user-to-user relationship provides more security and privacy to the users.

In OSNs, user's access to the resources are based on the relationship that is between a user and other user connected through the network which is found to be the target in the graph representation of the social network. This relationship type which is based on the access control which refers to ReBAC (referred as Relationship based access control model) provides the relationship of the particular sequences or existences of the relationship and express the polices of access control on terms of user-to-user relationship.

Consider some social network like "Google+" and "Facebook" provides some privacy options such as "private", "public", "friends list", "circles" and "friends of friends". These are some predefined options that are mostly used in the OSNs and provides privacy to the user groups. There are some researches who proposed some advanced model which is related to relationship based access control model such as [2], [4], [5], [7], [8], [9], [11], [12], [13], [14] can be given with multiple types of relationship based access control. Here [7],[8],[9] provides a decentralized security framework, Rule-based access control and enforcing access control over web based social network.

In this document, we provide a privacy and security for User-to User Relationship Access Control Model which gives the user to access others information in the depth of the relationship of that user.

Here, In Facebook, consider there are three users Alice, Bob and John. Alice is a friend of Bob and John. But Bob and John are not friends. Here, Alice tries to hide Bob's information from John. For this Alice checks the relationship between Bob and John, If the relationship does not exist then Alice will hide Bob's information from John. This is done only if John tries to get Bob's information through Alice, then Alice will hide Bob from John. So that John cannot find Bob when he try searching in any place.

2. RELATED WORK

Online Social Network (OSN) user are interconnected via various relationship. Only the relationship between user to user is being identified. These relationships are controlled by access specification. Access are being provided by user and system with their policy.

- **Private -** If setting is private then those who are "FRIENDS" can only view our friend's list.
- **Public** - If setting is made on public then everyone can view our friend's list.
- **Only me** - No one can view our friend's list.
- **Acquitance -** They can't view our timeline.
- **Restricted -** If the setting is made public then they can view only post and profile information.
- **Blocking -** They can't be our friend anymore.

In this, user to user relationship based access control in OSN has been enhanced by the authorization made typical by tracking the existence of user to user relationship. We develop a relationship based access control for OSN that incorporates not only U2U relationship but also user to resource and resource to resource relationship. Our model captures controls on user's administrator activities. The relationship has been patterned by the authorization policies based on the hop count limit of these path. Policy conflict resolution is discussed between positive and negative authorization arise due to generality or specificity. Each user can specify individual policies, policy conflicts occur where data resource may belong to multiple users. User, session, resources, policies, social graph, decision making are the components of Relationship based access model. Thus we provide hiding concept in our proposed system. **[4]**

The existence of online social network include person specific information create interesting opportunities. Security and privacy concern need to be addressed for creating such applications. This depend on authorization, admin filtering policies among various users. These are modeled based on trust relationship using SWRL. It support flexible admin policies which bring several access control policies specified by distinct user can be applied to same resource. When a photo is shared by an admin, where admin and other user have their own policies. To enforce access control the framework have to decide how the specified access control policy have to be integrated. So we propose an advanced concept of this paper by providing access control to our own various relationship. **[5]**

OSNs offer attractive means of digital social interaction and information sharing, but also raise number of security and privacy issue. OSN allow users to restrict access to shared data, they do not provide any mechanism for privacy concern over data associated with multiple users. This approach is to enable the protection of shared data associated with multiple users in OSNs. This formulate an access control model to capture the essence of multiparty authorization requirements, along with a multiparty policy specification scheme and a policy enforcement mechanism. Users may be involved in the control of a larger number of shared photos and the configurations of the privacy preference. Thus sharing can be avoided through disabling the right click.

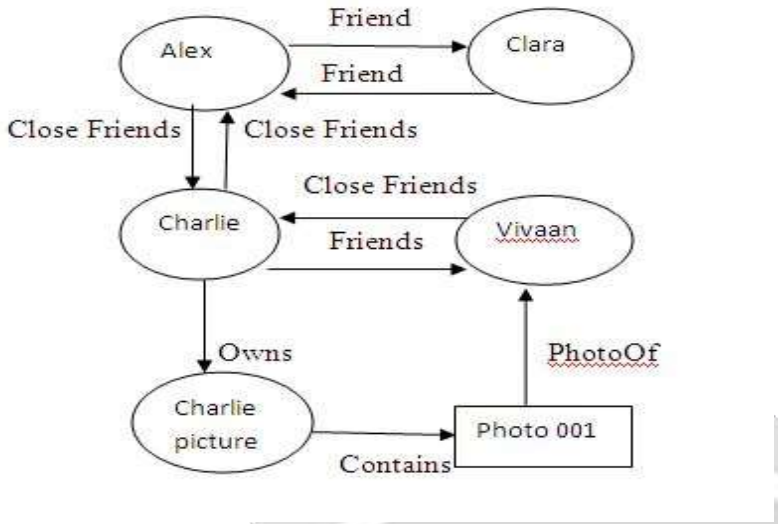


Fig 2.1 Photo sharing

In this figure 2.1, we can able to that Charlie and Alex are close friends so they can see each other picture and comment anything related to that. But the same picture can be viewed by all the other friends of Charlie and Alex. The photo is being shared among the Social Network. So there is no security to our picture which is uploaded by us or our friends. Therefore, this feature also plays an important role.

The access control paradigm behind the privacy preservation mechanism of Facebook is distinctly different from such existing access control paradigms as Discretionary Access Control, Role-Based Access Control, Capability Systems, and Trust Management Systems. This work takes a first step in deepening the understanding of this access control paradigm, by proposing an access control model that formalizes and generalizes the privacy preservation mechanism of Facebook. The model can be instantiated into a family of Facebook-style social network systems, each with a recognizably different access control mechanism, so that Facebook is but one instantiation of the model. We also demonstrate that the model can be instantiated to express policies that are not currently supported by Facebook but possess rich and natural social significance. This work thus delineates the design space of privacy preservation mechanisms for Facebook-style social network systems, and lays out a formal framework for policy analysis in these systems. Some of the access control that are used in Facebook provides privacy. To make them more secured, additional features have to be added. In our proposed system, we add our feature that make the Facebook a secured one. **[11]**

3. PROPOSED SYSTEM

To create a system which efficiently prevents the users from the untrusted users. There will be many users whom will access our profiles without our knowledge. Even if we apply the policies there are some people who can access our friends. To safeguard the friend whom we trust the most so that their information will be highly secured. There are many issues faced by the people who are using OSN. To minimize these problem we provide security to the images which is uploaded by us and our friends. This can be done by disabling the right click option so that our pictures can only be viewed.

The system architecture of the paper will be given below in the figure

The architecture diagram shows the overall functions that take place in the project. The user has to register first of all, then login into the Facebook. The friends we know will be in our friends list by accepting their request. Then the information is being shared by them. Apply the privacy for the friend we want so that we can protect them from other users.

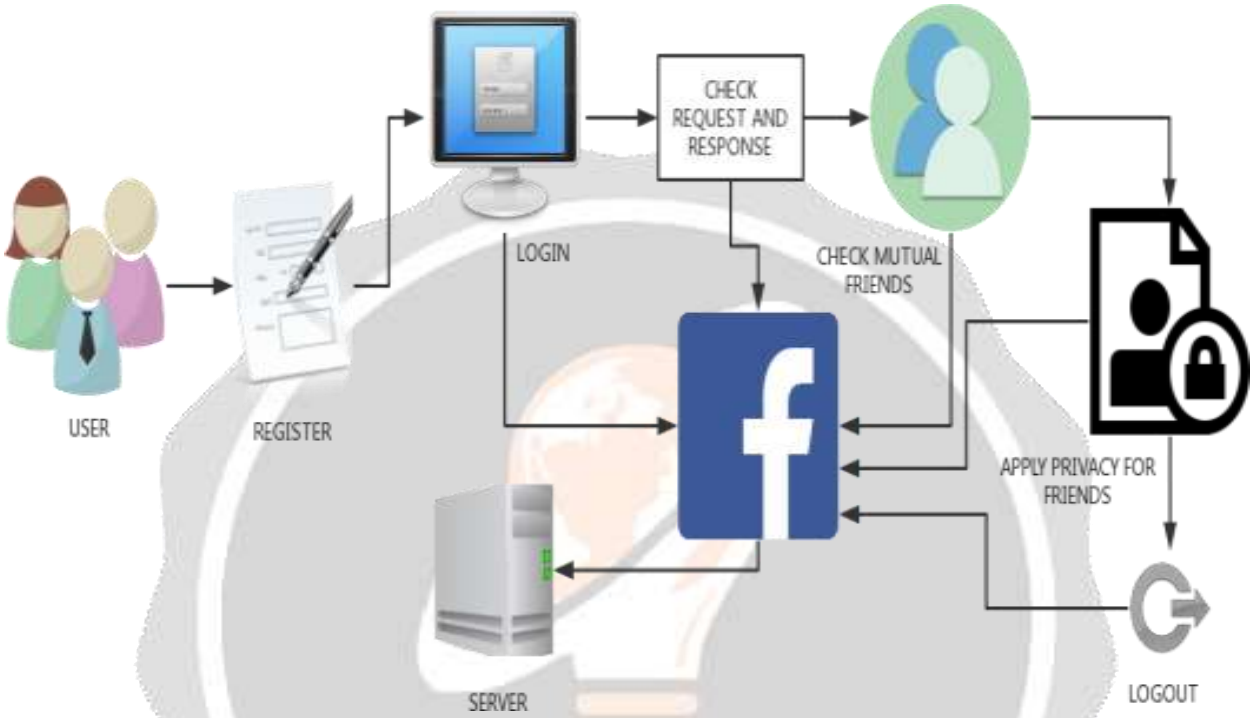


Fig 3.1 System Architecture

To determine the required relationship path between users to be offered or not. The opportunity to every OSN users to offer the right privacy for all their friends in the networks. Access control policy on users and resources are based on multiple relationships. Since there exist multiple relationship user may prefer to safeguard their friend from other persons. Thus, the trusted friends are protected from our friend list. So that many unwanted situations can be avoided. The images can be downloaded and misused by somebody that is avoided by restricting the downloading option.

A. ADMIN PROCESS

Admin module is the highest powerful user role in our system. Admin can view all the details available in the system. Admin can control all the operations in our system. Admin can view the users list. Admin can see the community list also. So whenever changes has been made to the privacy it will refer admin.

B. RELATIONSHIP AMONG USER

Users are key module of our system. This module provides the facility to register for their account. After creating an account the users can search for friends and can give friend request. Users can accept the friend request given by others. Users can have information sharing between the friends. The various relationships like friend, family, colleague etc.

C. FRIENDS REQUEST

Friend's network is the key module for constructing network of friends. Making friends network by giving request and accepting friend request. This module facilitates to share their posts and view the posts posted by their friends. Friend request is given by searching friend from our friend's list.

D. MUTUAL RELATIONSHIP

Checks whether mutual relationship exist between the trusted and untrusted friends. It is based on the common friends between the two persons so it is needed to verify the relationships exist. It is necessary to check the mutual relationship because if there exist a relationship between two peoples then there is no chance to obscure the friend from other people.

E. APLLYING PRIVACY

Setting access permission for the friends is one of the features of our project. This module facilitates to protect a friend from another friend of a particular user. By setting an access permission for friends our system offers the privacy for their friends. So the trust among the relationship is achieved.

F. PREVENTING PROFILE PICTURE

Profile picture privacy means applying privacy to the profile picture. This module gives the security and privacy offering to the privacy settings to for our own profile pictures. In day to day life people are facing many problems on posting their pictures. So this will be the initial step of preventing the profile picture from untrusted users.

4. ALGORITHM

In this paper, we define a algorithm which is used for providing the privacy for the users. For this we use an extended access evaluation algorithm along with path checking algorithm is also used.

These algorithm is shown in the below table.
1: (Policy Collecting Phase)
2: **If** Target = Ut **Then**
3: Accessing User Policy Ua's Policy For Action, Target User Policy Ut's Policy For Action1, Specify Policies System's Policy For Action
4: **Else**
5: Accessing User Policy Ua's Policy For Action, Target Resource Policy Rt's Policy For Action1, SP System's Policy For Action; (R:typename; R:typevalue)
6: (Policy Evaluation Phase)
7: **For All** Policy In Accessing User Policy, Target User Policy/ Target Resource Policy And Specify Policies **Do**
8: Extract Graph Rules (Start, Path Rule) From Policy
9: **For All** Graph Rule Extracted **Do**
10: Determine The Starting Node, Specified By Start, Where The Path Evaluation Starts
11: Determine The Evaluating Node Which Is The Other User Involved In Access
12: (Path Checking Phase)
13: Extract Path Rule From Graph Rule
14: Extract Each Path Spec Path, Hopcount From Path Rule
15: Path-check Each Path Spec
16: Set The Access Permission Over The Existing Path
17: Configure the User Profile Privacy
18: Evaluate the Combined Result Based On Conjunctive or Disjunctive Connectives Between Path Specs And Negation On Individual Path Specs
19: Compose the Final Result From The Result Of Each Policy

Table 1.1 Extended Access Evaluation Algorithm.

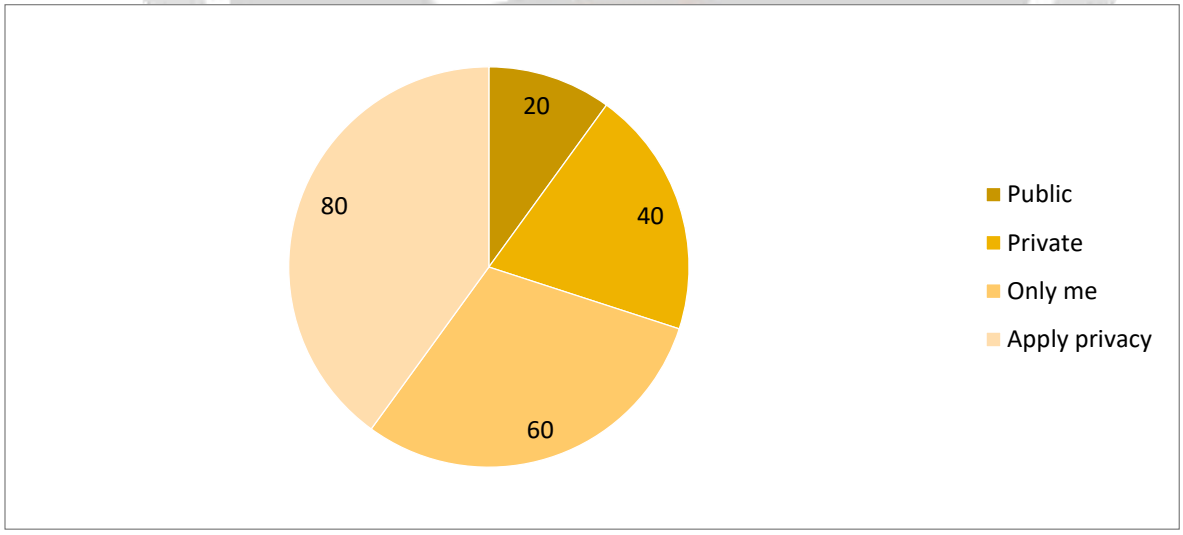
In the given algorithm, there are three types of phases. One is Policy Collecting Phase, where the policy in which the user want to collect from the other user who he needs to hide from his friend and after collecting the required information the user will hide the privacy through the next phase called Policy Evaluation Phase. Here the collected policy are evaluated and then the process is taken in the account with all the policy like User Access Control policy, Target User Policy and Target Resource Policy. These policies are collected before they are used in the process and after the information are collected the policy evaluation phase starts by checking the policy collected are correct and if the collected policy are not correct then the process of verifying the policy evaluation phase fails. This phase the policy are checked and then the target and the destination are fixed that who need to hide whose profile from whom is define here. The hopcount is the numerical value which gives the value of number of users or friends available in the friend list. By the hopcount value the process will be generated by which the policy and the user who must be hidden will be given by extracting the other values in the process.

Here path checking algorithm is used for searching or finding the path that need to be performed in the process. So each path by which who is friend of whom and if there is any relationship between them or not , all these are checked and the verified by the path checking evaluation phase. Here the value of hopcount is used for further path checking and evaluation of the process.

If the result is true then the process is done (i.e) one user is hidden from the other user. If the result is false then there is a relationship between those two users. At that time the evaluation cannot be performed.

5. PERFORMANCE EVALUATION

In this, a new system that enables the users of OSNs to protect their personal data. By means of our proposal, they can exactly decide which individuals can access to their published information. Since there exist multiple relationship user may prefer to safeguard their friend from other persons. As a result, even the OSN that hosts the user data cannot obtain any protected information if this is not explicitly allowed by the user. Thus, the trusted friends are protected from our friend list. So that many unwanted situations can be avoided. The images can be downloaded and misused by somebody that is avoided by restricting the downloading option. In addition to that, the new scheme has been designed to work properly with well-known OSNs such as Facebook.



6. CONCLUSION

The opportunity to every OSN users to offer the right privacy for all their friends in the network. Access control policy on users and resources are based on multiple relationships. To enforce access control to decide the specified access control policies have been provided in proposal. Trust among relationship has been provided by giving access permission among friends. Thus one of the friend is hidden from another friend among friends list. Safeguard of friends, our privacy information such as photos misuse is prevented.

In future work, it would be interesting to try these concept. Tag can be avoided or notification can be given when tag has been given by your friend. The person you may be known can be suggested with the acknowledgement of the person or user. One user can have multiple accounts in Facebook that can be avoided. Even kids are having accounts in Facebook, there should be restriction in age limit for using it.

REFERENCES

[1] Jaehong Park, Ravi Sandhu, and Yuan Cheng "An Access Control Model for Online Social Networks Using User-to-User Relationships". IEEE, 2016.
[2] Alexandre Viejo, Jordi Castella- Roca, GuillemRufian. "Preserving the User's Privacy in Social Networking Sites". Data Engineering (ICDE), 2015.
[3] S. Braghin, V. Iovino, G. Persiano, and A. Trombetta. "Secure and policy-private resource sharing in an online social network". In PASSAT 2011, pages 872–875. IEEE, 2011.
[4] G. Bruns, P. W. Fong, I. Siahaan, and M. Huth. "Relationship based access control: its expression and enforcement through hybrid logic". In Proceedings of the second CODASPY, pages 117–124. ACM, 2012.
[5] B. Carminati, E. Ferrari, R. Heatherly, M. Kantarcioglu, and B. Thuraisingham. "A semantic web based framework for social network access control". In Proceedings of the 14th ACM SACMAT, pages 177–186. ACM, 2009.
[6] B. Carminati, E. Ferrari, and A. Perego. "Enforcing access control in web-based social networks". ACM Trans. Inf. Syst. Secur., 13(1), 2009.
[7] Y. Cheng, J. Park, and R. Sandhu. "Relationship-based access control for online social networks: Beyond user-to-user relationships". In PASSAT 2012, pages 646–655. IEEE, 2012.
[8] Y. Cheng, J. Park, and R. Sandhu. "A user-to-user relationship based access control model for online social networks". In Data and Applications Security and Privacy XXVI, pages 8–24. Springer, 2012.
[9]Chi Zhang, Jinyuan Sun, Xiaoyan Zhu, and Yuguang Fang. "Privacy and Security for Online Social Networks: Challenges and Opportunities". Springer, 2012.
[10] J. Crampton and J. Sellwood. "Path conditions and principal matching: a new approach to access control". In Proceedings of the 19th ACM SACMAT, pages 187–198. ACM, 2014.
[11] P. W. Fong, M. Anwar, and Z. Zhao. "A privacy preservation model for facebook-style social network systems". In Computer Security–ESORICS 2009, pages 303–320. Springer, 2009.
[12] H. Gao, J. Hu, T. Huang, J. Wang, and Y. Chen. "Security issues in online social networks". Internet Computing, IEEE, 15(4):56–63, 2011.
[13] H. Hu and G.-J. Ahn." Multiparty authorization framework for data sharing in online social networks". In Data and Applications Security and Privacy XXV, pages 29–43. Springer, 2011.
[14] 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 ACSAC, pages 103–112. ACM, 2011.
[15] H. Hu, G.-J. Ahn, and J. Jorgensen. "Multiparty access control for online social networks: model and mechanisms". Knowledge and Data Engineering, IEEE Transactions on, 25(7):1614–1627, 2013.