Secure communication in online social networks by using access control policies

Yedukondalu Ravuri[1], Srinivasa Rao Yarlagadda[2]

[1]Yedukondalu Persuing M.Tech
CSE in Vignan's Lara Institute of
Technology & Science,Vadlamudi,Guntur

[2]Y.Srinivasarao Working As Asst.Professor
in Vignan's Lara Institute of Technology
& Science,Vadlamudi,Guntur

ABSTRACT

A network which consists of many users and maintains the relationship between them is said to be a social network. The usage of social networks like Facebook, Google+, twitter etc is playing a vital role in the internet world. These networks can be accessed from the entire world. Social Networks are very much helpful in finding and communicating with the known and unknown ones. This communication is processed based on the user request and response. Once the user accepted the request of the requested person, then they are ready to chat with one another (like face to face talk). Now they are eligible to share the information whatever they need like photos, videos, text etc. behind the social network. While the process of sharing information they are maintained limited security credentials. This paper deals a security constraint, which is while sharing the information like personal photos to another one there is a chance to share the same information by the third person. In order to overcome this problem we are generating a question tag below of the information to be shared with the other. If anyone knows the exact answer to that question they are permitted to watch those photos, videos etc., otherwise they are not eligible. Nothing is maintained secrecy in the social networks.

Keywords: Social network, multiparty access control, security model, policy specification and management.

1. INTRODUCTION

Online social networks plays a vital role in todays communication. social networks like facebook , twitter, linked in, google+ .each social network has different different securities measure, rules &regulation and policy .In this mainly security for user is not up to the mark. In face book if a person wants to share a video to friend if he share that video it is publicly available in social network .and every one see it even if he shares only with his friends if his friend likes it then it is to all the friends in his list can see it .so privacy and security is not there. In time line there is no security for cover photos.In this if we add security question for everything shared by applying member ship criteria like friend ,family etc. then if his friend wants to see it he must give security answer for the question .and he cannot share it. this can be very helpful in providing user level security . In this facebook must add this security tag . for user security in sharing information. By using access control policies & question tags we can provide Secure communication in online social networks .ONLINE social networks (OSNs) such as Face book, Googlle+, and Twitter are inherenttly designed to enable people to share personal and public information and make social connections with friends, coworkers, colleagues, family and even with strangers. In recent years, we have seen have unprecedentted growth in the application of OSNs. For example, Facebook, one of representative social network sites, claims that it has more than 800 million active users and over 30 biillion pieces of conttentt (web links, news stories, blog posts, notes, photto albums, etc.) shared each month . To protect user data, access controll has become a centtral feature of OSNs . A typiical OSN provides each user with a virtual space conttaining prov de profile information,, a list of the user's friends, and pr web pages, such as wall in Facebook, where users he and friends can post content and leave messages. A nd ve user profile usually includes information with us respect to the user's biirthday, gender, interests education and work history, and contact information. In addiition, users can not onlly upload content intto their own or otthers' spaces butt also tag otther users who appear in the conttentt. Each tag is an expllicit reference that links to a user's space. For the protection of user data, current OSNs indiirectly requiire users to be system and policy administrators for regullating their data, where users can restrict data sharing to a specific set of trusted users. OSNs often use user relationshiip and group us membershiip to diistinguish between trusted and untrusted users. For example, in Face book, users can allow friends, friends of friends, groups or publlic to access their data, dependiing on their personal authorization and privacy requirements

2.Back ground:

ONLINE social networks (OSNs) such as Facebook, Google+, and Twitter are inherently designed to enable people to share personal and public information and make social connections with friends, coworkers, colleagues, family and even with strangers. In recent years, we have seen unprecedented growth in the application of OSNs. For example, Facebook, one of representative social network sites, claims that it has more than 800 million active users and over 30 billion pieces of content (web links, news stories, blog posts, notes, photo albums, etc.) shared each month [3]. To protect user data, access control has become a central feature of OSNs. A typical OSN provides each user with a virtual space containing profile information, a list of the user's friends, and web pages, such as wall in Facebook, where users and friends can post content and leave messages. A user profile usually includes information with respect to the user's birthday, gender, interests, education and work history, and contact information. In addition, users can not only upload a content into their own or others' spaces but also tag other users who appear in the content. Each tag is an explicit reference that links to a user's space. For the protection of user data, current OSNs indirectly require users to be system and policy administrators for regulating their data, where users can restrict data sharing to a specific set of trusted users. OSNs often use user relationship and group membership to distinguish between trusted and untrusted users. For example, in Facebook, users can allow friends, friends of friends, groups or public to access their data, depending on their personal authorization and privacy requirements. Although OSNs currently provide simple access control mechanisms allowing users to govern access to information contained in their own spaces, users, unfortunately, have no control over data residing outside their spaces. For instance, if a user posts a comment in a friend's space, s/he cannot specify which users can view the comment. In another case, when a user uploads a photo and tags friends who appear in the photo, the tagged friends cannot restrict who can see this photo, even though the tagged friends may have different privacy concerns about the photo. To address such a critical issue, preliminary protection mechanisms have been offered by existing OSNs. For example, Facebook allows tagged users to remove the tags linked to their profiles or report violations asking Facebook managers to remove the contents that they do not want to share with the public. However, these simple protection mechanisms suffer from several limitations. On one hand, removing a tag from a photo can only prevent other members from seeing a user's profile by means of the association link, but the user's image is still contained in the photo. Since original access control policies cannot be changed, the user's image continues to be revealed to all authorized users. On the other hand, reporting to OSNs only allows us to either keep or delete the content. Such a binary decision from OSN managers is either too loose or too restrictive, relying on the OSN's administration and requiring several people to report their request on the same content. Hence, it is essential to develop an effective and flexible access control mechanism for OSNs, accommodating the special authorization requirements coming from multiple associated users for managing the shared data collaboratively. In this paper, we pursue a systematic solution to facilitate collaborative management of shared data in OSNs. We begin by examining how the lack of multiparty access control for data sharing in OSNs can undermine the protection of user data. Some typical data sharing patterns with respect to multiparty authorization in OSNs are also identified. Based on these sharing patterns, a multiparty access control (MPAC) model is formulated to capture the core features of multiparty authorization requirements which have not been accommodated so far by existing access control systems and models for OSNs. Our model also contains a multiparty policy specification scheme. Meanwhile, since conflicts are inevitable in multiparty authorization enforcement, a voting mechanism is further provided to deal with authorization and privacy conflicts in our model. Another compelling feature of our solution is the support of analysis on multiparty access control model and systems. The correctness of implementation of an access control model is based on the premise that the access control model is valid. Moreover, while the use of multiparty access control mechanism can greatly enhance the flexibility for regulating data sharing in OSNs, it may potentially reduce the certainty of system authorization consequences due to the reason that authorization and privacy conflicts need to be resolved elegantly. Assessing the implications of access control mechanisms traditionally relies on the security analysis technique, which has been applied in several domains (e.g., operating systems, trust management, and role-based access control). In our approach, we additionally introduce a method to represent and reason about our model in a logic program. In addition, we provide a prototype implementation of our authorization mechanism in the context of Facebook. Our experimental results demonstrate the feasibility and usability of our approach. The rest of the paper is organized as follows

Related work:

Analysis of Problem

Although OSNs currently provide simple access control mechanisms allowing users to govern access
to information contained in their own spaces, users, unfortunately, have no control over data residing outside their spaces. For instance, if a user posts a comment in a friend's space, s/he cannot specify which users can view the comment. In another case, when a user uploads a photo and tags friends who appear in the photo, the tagged friends cannot restrict who can see this photo, even though the tagged friends may have different privacy concerns about the photo. To address such a critical issue, preliminary protection mechanisms have been offered by existing OSNs . For example, Face- book allows tagged users to remove the tags linked to their profiles or report violations asking Face- book managers to remove the contents that they do not want to share with the public. However, these simple protection mechanisms suffer from several limitations. On one hand, removing a tag from a photo can only prevent other members from seeing a user's profile by means of the association link, but the user's image is still contained in the photo. Since original access control policies cannot be changed, the user's image continues to be revealed to all authorized users. On the other hand, reporting to OSNs only allows us to either keep or delete the content. Such a binary decision from OSN managers is either too loose

or too restrictive, relying on the OSN's administration and requiring several people to report their request on the same content. Hence, it is essential to develop an effective and flexible access control mechanism for OSNs accommodating the special authorization requirements coming from multiple associated users for managing the shared data collaboratively .

Proposed Work and Objectives:

In Proposed System we implemented a proof- of-concept Facebook application for the collaborative management of shared data, called MController. Our prototype application enables multiple associated users to specify their authorization policies and privacy preferences to co-control a shared data item. It is worth noting that our current implementation was restricted to handle photo sharing in OSNs [10]. Obversely, our approach can be generalized to deal with other kinds of data sharing and comments, in OSNs as long as the stakeholder of shared data are identified with effective methods like tagging or searching. The proposed system shows a novel solution for collaborative management of shared data in OSNs. A multiparty access control model was formulated, along with a multiparty policy specification scheme and corresponding policy evaluation mechanism. In addition, we have introduced an approach for representing and reasoning about our proposed model [11]. A proof- of-concept implementation of our solution called MController has been discussed as well, followed by the usability study and system evaluation of our method. Indeed, a flexible access control mechanism in a multi-user environment like OSNs should allow multiple controllers, who are associated wi th the shared data, to specify access control policies. As we identified previously in the sharing patterns in addition to the owner of data, other controllers, including the contributor, stakeholder and disseminator of data, need to regulate the access of the shared data as well. In our multiparty access control system, a group of users could collude with one another so as to manipulate the final access control decision [9].

Scope & objective:

On-line Social Networks (OSNs) are platforms that allow people to publish details aboutthemselves and to connect to other members of the network through links. Recently, the popularity of OSNs is increasing significantly. For example, Face-book now claims to have more than a hundred million active users. The existence of OSNs that include person specific information creates both interesting opportunities and challenges. For example, social network data could be used for marketing products to the right customers. At the same time, security and privacy concerns can prevent such efforts in practice. Improving the OSN access control systems appears as the first step toward addressing the existing security and privacy concerns related to online social networks. However, most of current OSNs implement very basic access control systems, by simply making a user able to decide which personal information are accessible by other members by marking a given item as public, private, or accessible by their direct contacts. In order to give more flexibility, some online social networks enforce variants of these settings, but the principle is the same.

Objectives:

A .security policies
b. un authorized excess control
c. Provide policy and privacy for multiple user to specify there authorization
d. Discover potential malicious activities using collaborative control
e. An Online Social Network with User- Defined Privacy

Desired Implications:
MODULE DESCRIPTION:

Number of Modules After careful analysis the system has been identified to have the following modules [12]:

1. Owner Module
2. Contributor Module
3. Stakeholder Module
4. Disseminator Module
5 . MPAC Module

Owner module:

In Owner module let is a data item in the space m of a user u in the social network. The user u is called the owner of d. The user u is called the contributor of d. We specifically analyze three scenarios—profile sharing, relationship sharing and content sharing—to understand the risks posted by the lack of collaborative control in OSNs. In this the owner and the disseminator can specify access control policies to restrict the sharing of profile attributes. Thus, it enables the owner to discover potential malicious activities in collaborative control. The detection of collusion behaviors in collaborative systems has been addressed by the recent work.

Contributor module:

In Contributor module let d be a data item published by a user u in someone else's space in the social network. The contributor publishes content to other's space and the content may also have multiple stakeholders (e.g., taggedusers). The memory space for the user will be allotted according to user request for content sharing. A shared content is published by a contributor

Stakeholder Module:

In Stakeholder module let is a data item in the space of a user in the social network. Let T be the set of tagged users associated with d. A user u is called a stakeholder of d, if u 2 T who has a relation ship with another called stake holder stakeholder, shares the relationship with an access or. In this scenario, authorization requirements from both the owner and the stakeholder should be considered. Otherwise, the stakeholder's privacy concern may be violated. A shared content has multiple stakeholders.

Disseminator element:

In Disseminator module let d be a data item shared by a user u from someone else's space to his/her space in the social network. The user u is called a disseminator of d. A content sharing pattern where the sharing starts with an originator (owner or contributor who uploads the content) publishing the content, and then a disseminator views and shares the content. All access control policies defined by associated users should be enforced to regulate access of the content in disseminator's space. For a more complicated case, the disseminated content may be further re-disseminated by disseminator's friends, where effective access control mechanisms should be applied in each procedure to regulate sharing behaviors. Especially regardless of how many steps the content has been re- disseminated, the original access control policies should be always enforced to protect further dissemination of the content

MPAC Component:

MPAC is used to prove if our proposed access control model is valid. To enable a collaborative authorization management of data sharing in OSNs, it is essential for multiparty access control policies to be in place to regulate access over shared data, representing authorization requirements from multiple associated users. Our policy specification scheme is built upon the proposed MPAC model. Assessors Specification: Assessors are a set of users who are granted to access the shared data. Assessors can be represented with a set of user names, asset of relationship names or a set of group names in OSNs.

Scientific Challenges :

SN sites are perfect for illegal online activities as they consist of a huge number of users with high levels of trust among them. As a result there is a high range of security risks, threats and challenges. SN sites provide some mechanisms for privacy settings to protect users, but these mechanisms are not enough to protect the users. The top and primary privacy problem is that SN sites are not informing users of the dangers of spreading their personal information. Thus users are not aware of the extent of the risks involved. The second problem is the privacy tools in SN sites, which are not easy to use and do not offer the flexibility for users to customize their privacy policies according to their needs. The third problem is the users themselves who cannot control what other users can reveal about them such as tagging their photos or related information to other friends' profiles

Process of providing security to social network communication content:

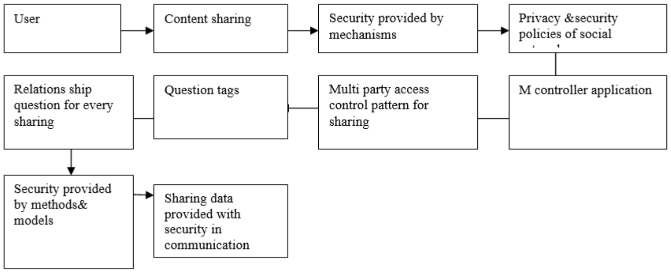
User
Content sharing
Security provided by mechanisms
Privacy &security policies of social
Relations ship question for every sharing
Question tags
Multi party access control pattern for sharing
M controller application
Security provided by methods& models
Sharing data provided with security in communication

Fig: real time execution of security in sharing data in online social networks.

Theoretical explanation off background process of security in data sharing in online social networks.:
First use login to his account then if he share data like photos,videos then security mechanisms like privacy &security policies of social network comes into act then mpac controller module application plays a key role then we apply new concept of question tags for every sharing and seeing the post after answering the question then the content is displayed this is how we provide security in online social networks for content sharing.

Conclusion:

In this paper, we have proposed a novel solution for collaborative management of shared data in OSNs. A multiparty access control model was formulated, along with a multiparty policy specification scheme and corresponding policy evaluation mechanism. In addition, we have introduced an approach for representing and reasoning about our proposed model. A proof-of- concept implementation of our solution called MController has been discussed as well, followed by the usability study and system evaluation of our method. As part of future work, we are planning to investigate more comprehensive privacy conflict resolution approach and analysis services for collaborative management of shared . data in OSNs. Also, we would explore more criteria to evaluate the features of our proposed MPAC model. For example, one of our recent work has evaluated the effectiveness of MPAC conflict resolution approach based on the tradeoff of privacy risk and sharing loss [21]. In addition, users may be involved in the control of a larger number of shared photos and the configurations of the privacy preferences may become time- consuming and tedious tasks. Therefore, we would study inference-based techniques [15], [34] for automatically configure privacy preferences in MPAC. Besides, we plan to systematically integrate the notion of trust and reputation into our MPAC model and investigate a comprehensive solution to cope with collusion attacks for providing a robust MPAC service in OSNs.

Reference:

[1] Face book Developers. http://developers.facebook.com/.

[2] Face book Privacy Policy. http://www.facebook.com/policy.php/.

[3] Z. Besmer and T. Richter Lipford. Moving beyond un-tagging Photo privacy in a tagged world. In Proceedings of the 28th international conference on Human factors in computing system

[4] t. Carminati and F. Ferrari. Collaborative access control in online social networks In Proceedings of the 7th International Conference on Collaborative Computing: Networking, Applications

[5] o. Choi, W. De Neve, K. Plataniotis, and Y. Ro. Collaborative face recognition for improved face annotation in personal photo collections.

AUTHOR PROFILES:

Ravuri Yedukondalu, Pursuing M.Tech in Department of CSE at Vignan's LARA Institute Of Technology & Science, Vadlamudi Guntur Dist., A.P., India. His research interest includes in Software Engineering, Data Mining

Y.Srinivasarao, Asst.Prof, Department of CSE, Vignan's LARA Institute Of Technology & Science, Vadlamudi Guntur Dist.,A.P., India. He has done his M.Tech at Vignan University in the year 2009 .