ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Significance of Multiparty Authorization Requirements with a Multiparty Policy Specification Scheme

Ms. Fatima Masood Quadri
M.Tech Student,
Department of CSE,
Shadan Women's College of Engineering & Technology,
Khairatabad, Hyderabad.

Ms.Medapati Lalitha
Assistant professor,
Department of CSE,
Shadan Women's College of Engineering & Technology,
Khairatabad, Hyderabad.

Ms. Saleha Farha
HOD,
Department of CSE,
Shadan Women's College of Engineering & Technology,
Khairatabad, Hyderabad.

Abstract:

In recent year, most popular websites are social media, it has tremendous growth take in consideration as a fast network to connect a people and thus it's give idea of overload of millions of internet user. These social network offer to carry out desirable means for digital social inter connection and information involvement, but also come again a number of security and privacy problems. Right to use manage mechanism is provide to restrict shared data, they currently do not provide any mechanism to minimize problem of multiuser shared data. To this end, we carry out an approach to allow the protection of shared data accompanying with multiple users in social network. We gives a stand to user to share their data in protected manner. We also discuss a proof-of-concept prototype of methodology as part of a framework on social network and provide usability study and system evaluation of our method.

Keywords:

Social network, multiple user access control, Security mode, Specification and management, Data Sharing.

INTRODUCTION:

social networking sites like Face book, twitter given that real names and other private information is encouraged by the site (onto a page known as a „Profile„).because these sites are more trusted sites.. These information are most of contain of user basic identity of the user. Some sites also take into consideration to allow the user for their likes and dislikes such as interests, hobbies, favourite's books or films, and even relationship status. Thus, this is not secure to expose their identity in anywhere in the untrusted web media. On the basis of literature survey on social media, we consider two social site that have more similarity identity in between their personal information and photos which is overlapping the identity of same user Most of the user had not modify their basic information (the default setting originally agreed friends, friends of friends, and non-friends of the similar network to have full view of a user's profile). The natural human being can block the profile of the other user if he don't want, and would therefore come into the picture not to be usually used for a wide number of people. So that user can't be determine which security feature that they want to use. Face book was disapproved due to the perceived tolerance regarding privacy in the default setting for users. Data sharing on social network is more flexible .but main important thing is that data is going to be in secure manner. there is no of feature in social media for users to partaking messages, invitations, photos, open dais applications and other applications are often the platform for others to gain access to a user's private information.

A typical online social web access is give platform for each user to give up their data over the virtual space enclosing user shared photos, wall post, user's friend. With the use of this feature, user not only can upload their photos but also tag the other photos in virtual space of ONSs. The photo tagging is the important feature in social media that contain link of each user which are appear in the photo. For the security of user data, existing system gives indirect security environment for each user. In this paper, we create one framework that gives direct security environment for each user to protect data from such existing issue. We begin by examining how the lack of multiple random user management for data sharing in OSNs throughout the security problem can undermine the protection of user data. The project work find out challenge, . In particular, we have to know the conceptual study of two fundamental. First, we want to deep theoretical study of social media like Face book, twitter and find out the challenges with respect to user pattern recognition. Second, we want to over simplify the social media access control mechanism,

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

by analysing the user pattern behaviour as the same network. At the end of these we have to initiate one paradigm which can generalise all user problem and give the user friendly platform to the user . The model can be instantiated into a Face book is family of social network, each with a recognizably different access control mechanism, so that Face book is one can be best generalise model to show our derive implementation over social network.

BACKGROUND:

Today, online social networks have been a very important application to students, professors, employers, business persons etc. As the OSN's is serving not only for sharing pictures, data, videos, but also sharing the business information, private information. But sharing the private information among OSN's is a big concern when regards to security. Particularly when sharing the data between multiple users.In the proposed method the users can specify the privacy policy to have a control on the data. A user can specify his privacy policies as either permit or deny to authorize the data. I would concentrate on the photos as the data items, and apply access control mechanisms on it.My project is based on the existing problems in OSN's and in Face book as a special case which is popular among all OSN's, to provide a privacy access control mechanisms on shared data, to whom the data to be shared.

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

PROBLEM STATEMENT:

In present online social networks security is weak and there are no particular access control policies like in Facebook, twitter. In these present existing OSN applications, sharing information from one user to another user is not efficient. In the present scenario if any user comments on image or any data, that comment is visible by all friends. There is no security for comments in images or any data. There are no particular privacy settings for comments in existing Online Social Network systems.In present existing OSN applications one person upload the image in wall. That image is visible to all friends and any person sharing that image to other persons. So there is no privacy for shared documents in present OSN applications. Any person comment on shared data is shared by any other friend. But that comments details are visible by all other friends . There is particular privacy setting for comments in my present OSN application.

Drawbacks :

•There is no particular privacy setting for shared data .
•There is no particular security for upload documents or images.
•There is no privacy for comments on data.
•Any type of data is shared by all members.
•There is no particular options for sharing data in friends or family.

PROPOSED SYSTEM:

In the proposed system, I have tried to resolve the security issues in present online social network applications. This system provide security settings for data shared among multiple users.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

If a user uploads data he can specify it as a public or private. If the privacy allowed is private, the data cannot be shared further, If the privacy allowed is public as per the user interest, the data can be shared further. In this proposed system user can give comments on uploaded images and also can specify the privacy settings too to make sure who can view and who cannot view his/her comments. So comments are shared by based on privacy settings of comments.

IMPLEMENTATION SEARCH FRIENDS:

A user after creating his profile in the account logs in and searches for friends by giving his name/email. These friends are those who have already registered in the application. The users after searching can send the requests to each other and accept. While sending and receiving the requests users need to specify that in which relation/group he has to add the specific users. The relationship/group will be family/friends.

OWNER:

Owner is the other module, he is the one who shares the photos with group of his friends. He is the one who will have all the authorities on picture which he posts on his friends wall. The owner while uploading the images to his friends/family has to provide the privacy settings in specific who can view the picture and who cannot view the picture.

CONTRIBUTOR:

An owner will turn into a contributor when he/she shares a picture on his friends/family wall. Whenever the owner of the picture shares the image with group of people, he will give the access control on the picture.

FRIENDS AND FAMILY LIST (STAKEHOLDERS):

Whenever the user accepts the friend requests, he will have some friends formed in his list. So, the owner shares the picture with his friends/family becomes the contributor and the friends/family on whose wall the picture was shared becomes the stakeholders. The picture can be viewed only by the stakeholders with some privacy settings on it.

SHARE IMAGES (DESSIMINATOR):

A user can share the images of their friends, when the owner of the image has shared on this person's wall. But he will not have the full control over the image. This can be restricted by the actual owner of the image who shared like blocking the tags. So, whenever this user shares other images he will become the disseminator.

RELATED WORK:

Access control for OSNs is still a relatively new research area. Several access control models for OSNs have been introduced . Early access control solutions for OSNs introduced trust-based access control inspired by the developments of trust and reputation computation in OSNs. Distributed identity management system for OSNs, where relationships are associated with a trust level, which indicates the level of friendship between the users participating in a given relationship. introduced a new class of security policies, called collaborative security policies, that basically enhance topology-based access control with respect to a set of collaborative users. This work considers user collaboration during both access control enforcement and policy specification, and employs semantic web technologies to support a rich way for denoting collaborative users based on their relationships with the associated resources. In contrast, our work proposes a formal model to address the multiparty access control issue in OSNs, along with a general policy specification scheme and a simple but flexible conflict resolution mechanism for collaborative management of shared data in OSNs. In particular, our proposed solution can also conduct various analysis tasks on access control mechanisms used in OSNs, which has not been addressed by prior work.

MController:

Which is divided into two major pieces, Facebook server and application server. The Face book server provides an entry point via the Face book application page, and provides references to photos, friendships, and feed data through API calls. Face book server accepts inputs from users, then forwards them to the application server. The application server is responsible for the input processing and collaborative management of shared data. Information related to user data such as user identifiers, friend lists, user groups, and user contents are stored in the

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

application database. Users can access the MController application through Facebook, which serves the application in an iFrame. When access requests are made to the decision making portion in the application server, results are returned in the form of access to photos or proper information about access to photos. In addition, when privacy changes are made, the decision making portion returns change-impact information to the interface to alert the user. Moreover, analysis services in MController application are provided by implementing an ASP translator, which communicates with an ASP reasoner.

Users can leverage the analysis services to perform complicated authorization queries. Once a user installs MController in her/his Facebook space and accepts the necessary permissions, MController can access a user's basic information and contents. Especially, MController can retrieve and list all photos, which are owned or uploaded by the user, or where the user was tagged. Once information is imported, the user accesses MController through its application page on Facebook, where s/he can query access information, set privacy for photos that s/he is a controller, or view photos s/he is allowed to access.

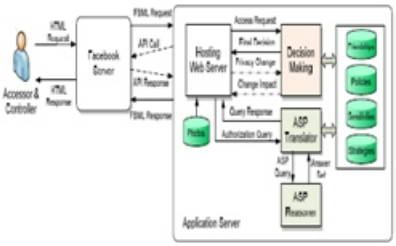

Fig:- Overall Architecture of MController Application

A core component of MController is the decision making module, which processes access requests and returns responses (either permit or deny) for the requests. Fig depicts a system architecture of the decision making module in MController. To evaluate an access request, the policies of each controller of the targeted content areenforced first to generate a decision for the controller. Then, the decisions of all controllers are aggregated to yield a final decision as the response of the request. Multiparty privacy conflicts are resolved based on the configured conflict resolution mechanism when aggregating the decisions of controllers. If the owner of the content chooses automatic conflict resolution, the aggregated sensitivity value is utilized as a threshold for decision making.

Otherwise, multiparty privacy conflicts are resolved by applying the strategy selected by the owner, and the aggregated sensitivity score is considered as a recommendation for strategy selection. Regarding the access requests to disseminated content, the final decision is made by combining the disseminator's decision and original controllers' decision adopting corresponding combination strategy discussed previously.

ANALYSIS:

After careful analysis, I have observed that I am success in applying the privacy settings for the content shared over OSN's. My contribution to this project can be described from the above provided screen shots, as I was able to develop an application which is similar to Facebook. In my application users can make friends and family relationships. They can share the data in a very secured options. They will have the full control over the data they are sharing. This is a big advantage of the application

CONCLUSIONS:

The application I have developed can be implemented over web servers. As I have implemented this application on apache tomcat server. It can be used to server the users who were facing the problems with privacy issues over OSN's. This application can be used as an extension to the present applications. Also this is very flexible and user friendly application where one can find the directions to allow the privacy settings on a specific image.I would like to extend my future work concentrating more on control over videos, comments which is being an inevitable content. So, far I did this project as per the time permitted. In the near future I would be extending my project on simplifying the privacy settings especially for the women world.

As the women content should be more private. Also, the business information should be secured as there is a lots of business content is shared among the users in OSN like LinkedIn.In this paper, we propose exclusive access control model for facility of collective management of share data in social network. We have given the analysis on multiple user on share data that can secure the identity information from the malicious user. We have describe here multiple user access control model on the basis of proof of concept of social network that can give secure user friendly platform to the each user and they keep their social data very private on the network.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Our future work, the supervise automated face recognition model for recognize the face from photo where the photo containing image of tag user .It is use when tag remove from photo but content remain in photo , the automated face recognize the face from photo is more effective.

REFERENCES:

[1] Facebook Developers. http://developers.facebook.com/.
[2] Facebook Privacy Policy. http://www.facebook.com/policy.php/.14
[3] Facebook Statistics. http://www.facebook.com/press/info.php?statistics.
[4] Google+ Privacy Policy. http://http://www.google.com/intl/en/+/policy/.
[5] OpenSocial Framework. http://code.google.com/p/opensocial-resources/.
[6] The Google+ Project. https://plus.google.com.
[7] A. Besmer and H. Richter Lipford. Moving beyond untagging: Photoprivacy in a tagged world. In Proceedings of the 28th international conference on Human factors in computing systems, pages 1563– 1572. ACM, 2010.
[8] L. Bilge, T. Strufe, D. Balzarotti, and E. Kirda. All your contacts are belong to us: automated identity theft attacks on social networks. In Proceedings of the 18th international conference on World wide web, pages 551–560. ACM, 2009.
[9] B. Carminati and E. Ferrari. Collaborative access control in online social networks. In Proceedings of the 7th International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom), pages 231–240. IEEE, 2011.
[10] B. Carminati, E. Ferrari, and A. Perego. Rule-based access control for social networks. In On the Move to Meaningful Internet Systems 2006: OTM 2006 Workshops, pages 1734–1744. Springer, 2006.
[11] B. Carminati, E. Ferrari, and A. Perego. Enforcing access control in web-based social networks. ACM Transactions on Information and System Security (TISSEC), 13(1):1–38, 2009.
[12] E. Carrie. Access Control Requirements for Web 2.0 Security and Privacy. In Proc. of Workshop on Web 2.0 Security & Privacy (W2SP). Citeseer, 2007.
[13] J. Choi, W. De Neve, K. Plataniotis, and Y. Ro. Collaborative face recognition for improved face annotation in personal photo collections shared on online social networks. Multimedia, IEEE Transactions on, 13(1):14–28, 2011.
[14] J. Douceur. The sybil attack. Peer-to-peer Systems, pages 251–260, 2002.
[15] L. Fang and K. LeFevre. Privacy wizards for social networking sites. In Proceedings of the 19th international conference on World wide web, pages 351–360. ACM, 2010.
[16] P. Fong. Preventing sybil attacks by privilege attenuation: A design principle for social network systems. In Security and Privacy (SP), 2011 IEEE Symposium on, pages 263–278. IEEE, 2011.
[17] P. Fong. Relationship-based access control: Protection model and policy language. In Proceedings of the first ACM conference on Data and application security and privacy, pages 191–202. ACM, 2011.

Author's:

Ms. Fatima Masood Quadri has completed her B.E. in Information Technology from Muffakham Jah College of Engineering and Technology, Osmania University, Hyderabad. Presently, she is pursuing her Masters in Computer Science Engineering from Shadan Women's College of Engineering and Technology, Khairatabad, Hyderabad, T.S, India. Her research interests include data security, database management , social networking.

Ms. .Medapati Lalitha has completed her M.SC information technology,Allagappa University and M.Tech CSE, Nagarjuna University.She is having 11 years of experience in teaching field. Currently, she is working as an Assistant Professor of CSE Department in Shadan Women's College of Engineering and Technology,Hyderabad, T.S,India.

Ms.Saleha Farha has completed her B.Ttech(Computer Science Engineering) and M.Tech (Software Engineering) from JNTUH University, hyderabad. She has five years of experience in teaching field. Currently, she is working as the Head of CSE Department in Shadan Women's College of Engineering and Technology, Hyderabad, T.S, India.