Multiuser Access Control for online Social Medias: Beyond Single user Protection

Shwetha S [1]
PG student, Dept of CSE,
CIT ,Gubbi ,
Karnataka, India

Prof. Shantala C. P [2]
HOD, Dept of CSE,
CIT ,Gubbi,
Karnataka, India

***Abstract*-Online social medias (OSMs) have seen a rapid growth in decade and has become a real gateway for millions of Internet users. These OSMs offer a digital social communications and information sharing. OSMs users unintentionally disclose certain kinds of personal information that attackers could get benefited from which there is a need for increased security and privacy issues. Online social medias (OSMs) with a billion users have severely raised concerns on privacy leakage. Hence OSMs allow its users to maximum access to mutual data, they currently do not provide any method to apply privacy concerns over data related with many users. Our work recognize what bits of information are currently being shared, how extensively, and what users can do to stop such sharing. Along with this we frame an access control model to internment the essence of multiuser authorization requirements, along with a multiuser policy requirement scheme and a policy implementation mechanism.**

Keywords*- *Online social medias (OSMs), tagging, information sharing, multiuser access control, multiuser policy requirement , multiuser policy implementation.

I. INTRODUCTION

Online social medias (OSMs) are planned to make people share their personal and public information and make social associations with a familiar or with strange person . From past decade we have seen tremendous growth in the application of OSMs. Many online social media sites has millions regular users and billion bits of data shared every month [1]. OSMs provides every user with a virtual space holding user profile evidence, a list of the user's contacts, along with web pages. A profile usually holds evidence about the user's date of birth, sexual category, goods, schooling and work ,relationship status and contact information. In addition, users can upload a content into their space or others' spaces and can tag others who appear in their contact list. Each tag is an clear reference to a user's virtual space. In some nations a simple exposure of basic information like place and birthdate of a user in online social medias can give his Social Security Number (SSN) [2]. For the protection of user data, current OSMs require its users to be a administrators for controlling their data, every users can predict data sharing to a explicit set of trusted users. OSMs allow users to create their relationship and groups with the friends in his profile. And this relationship and group membership help to differentiate between the trusted and untrusted users. Today's OSMs have low access control methods which allow its users to administer information confined in their own spaces but users, have no power over the data which is outside their space. Example when a user texts on his friends space he has no power on the data and he also cannot predict who can view his data through his friends space in other way when someone tags a photo, the tagged person have no control on the photo he is tagged in except he has a very low privacy setting on the data /photo he has been tagged. Currently OSMs provide its users to hide/ remove a photo/data they have been tagged but the original content is stored in the space of the user who owns this data. In this paper we provide a systematic solution for the management of data/photo related to multiple users by providing each user a control on the data he share or he has been tagged using MUAC (Multiuser Access Control) model.

II. BACKGROUND TECHNOLOGIES

A. Access Mechanism Models for OSMs

Here we find the path from the resource owner (data owner) to the resource users (tagged users) and the authorization needed for the level of association, along with association type and complexity . Access rules are in term of complexity, type and trust level with each single users in a flexible way. Access mechanism is a two level process, accordingly, reachability of the data owner through the search list and accessibility of the resource. In [3], Carminati et al proposed an access mechanism framework which used the relationships between OSMs user's and resources as the basis for access mechanisms and employed the Semantic Web Rule Language (SWRL) to define authorization, administration and filtering policies.

.

B. Policy Conflict Purpose

In OSMs possible policy conflicts is due to policies specified by different users convey different authorization . It has become unavoidable as long as each user can have need of individual policies. This policy conflict purpose is necessary to express an order of explicit plan, of a listed order of relationships between the policy makers and the user or resource that these policies apply to.

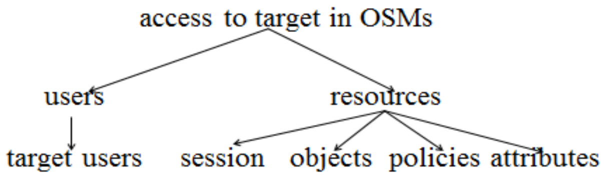

Fig.1 Access in OSMs

C. OSMs Characteristics Based on Access Mechanism

We categorize three important features that need to be addressed by OSMs access mechanism models, as follows

a) Distinct Policy: OSMs allow each users to precise their own choice over access to the resources instead of than having a only system-wide access mechanism policy defined by the system security administrator. Also, users apart from the owner are also able to organize policies for users and data related to them. For example, Alice wants to block her co-workers from seeing the pictures which contain her image. The system here collect all of the individual users policies along with the system-identified policies for making access mechanism decisions.
b) Policy Management: OSMs play a very important role in policy management because each users specify the policy required by the OSMs to confirm that only the true users are authorized to specify policies. This model allows users to insist on policies for other users as long as they meet the relationship condition. The owner of the resource or tagged user of the same resource can control the resource's policy and can later alter it according to their need.
c) Different User-session: Different devices have different access mechanism policies and different privileges. A user can have many sessions with different sets of rights by creating different degrees of access mechanism policies with the original user. The different user-session enables better security and privacy mechanism by reducing a session's privilege to an suitable level. It becomes especially useful in OSMs environments as more and more keen devices and location-dependent applications are introduced into OSMs world [3].

III. REQUIREMENTS OF PRIVACY AND SECURITY FOR OSMS

Privacy is very important in OSMs. User‘s privacy deal with two things .Firstly it goes with unauthorized entities who should not get through the private information of the data owner. Secondly the unauthorized party should not be able to link multiple private data files to the profile of the data owner and also should not be able to leak any kind of useful information. OSMs has several broad categories related with user's privacy[4]:
a) Identity Privacy: The security of a user's identity is different for different types of OSMs. There is no user identity privacy because most applications trust on connecting user's profiles for their public identification. In some dating websites the use of actual labels and private contact data is discouraged. A random identifier is used to protect the open identification of a person.
b) Virtual Space Privacy : The view of a user's profile differ across different types of OSMs. Some OSMs allow users to choose their profile to be public or just to friends in their contact lists . But some other by default, make the profile visible to the users who are part of the same sub-network with permission given to owner to decide on to deny/ permit to those in their sub-network.
c) Communication Privacy : An OSM user may intentionally or unintentionally disclose personal information to the network operator or OSM provider using the network itself: data such as time and length of connections, location (IP address) of connection, other user's profiles visited, messages sent and received, and so forth. Therefore, additionally, communication privacy has to be met [4].

IV. TAGGING A MULTIMEDIA CONTENT

The capacity to upload and share photo albums on the social media was launched in October 2005 [6] . Since its start, the facility allowed users to tag their friends and post a comment on photos. When tagged, friends get e-mail alerts, drive lots of traffic to the website. Within a month of its launch, 85% of the contributed users were tagged at least once [6].

A. Privacy Breaches Related to Photo/Data Tagging

a) Place of Picture Taken:- Users should maintain some level of limited disclosure so they can interact better with others. Since tagging is a prevalent and suitable feature, users have a habit of not to inactivate it. It is the responsibility of a user who tag his/her friends in the photo/data, to protect his friends personal information from exposure.

b)Users Identification without a Profile Picture:- Some users may not upload any photo of them on social medias like Facebook. But if his/her friend uploads a photo and tags a person . Without his permission then he can be instantly recognized by others who have an access permission to the photo album, which may include all friends of a person who uploaded a photo or even everyone on social media.

c)Unintentional Audience:- The tagged picture takes personal information of a tagged user directly. Anyone who access the photo has also the option to share it. In the current tagging method, the tagged user has no control on the exposure of the picture because the control is given to the owner who has uploaded and tagged the other in the photo [5].

B. Trust Based Schema for Tagging

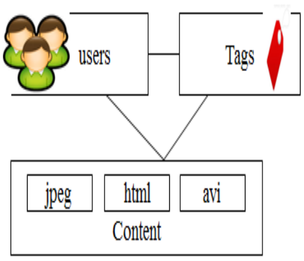

Fig 2 General model of social tagging system

Users upload the data/photo and share them through online social medias, and allow other users to comment, like or share it. This trend has created new challenges for accessing, searching, and retrieving of the content shared. The task of tagging is to find the correct tags for a given data and at the same time it filter out the noise and spammed content of the tag. In tagging system, spam or noise can be injected at distinct stages. Trust modelling can be done at each stage distinctly to produce the trust models.

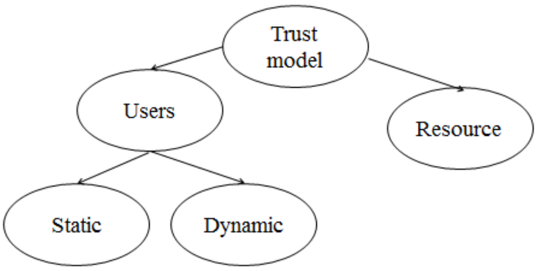

Fig.3 Trust model classes

a) Resource Trust Modelling:

Resource trust modelling is used to organize resources(e.g. web applications, images, and videos) as junk or spam . Here the target is resources and trust is based on the rank what it obtain and tags related to that particular resources. Here the power is given to the administrator to take action against the resources which is incorrect or considered as junk.This resource trust modelling uses the features of the resource information, profile information of the users who uses the resources and the tagged information to detect the spam resources. The ranking priority is given to the resources from high to low based on the tagging by many reliable users.

b) User Trust Modelling:

When compared this user trust model with the resource trust model .The user trust model looks more flexible than the resource trust model. In user trust modelling the trust is given to each user based the information extracted from users space, interaction with other users on online social medias and the relationship between the tags and the resources that user backed to the tagging system. User trust modelling can be a centralized or distributed trust modelling . In centralized user trust modelling, trust models are maintained by administrator. In distributed user trust modelling the control is given to each user to maintain his own account based on the interaction the user do with his contacts on online social medias. Today's social medias is a admin controlled user trust modelling systems while the distributed user trust modelling system is peer to peer networks. This model proposed an approach, which use the response from users who agree or disagree with a tag related with an image. The more variance a user has, the more distrusted the user is. A user's trust is calculated as the proportion between the number of suitably tagged images and the number of all images tagged by that user [7].

V. MUAC FOR OSMS

There are numerous characteristic that are used in sharing patterns of OSMs where different users have different requirements on a single resource. We examine three states a) Sharing Profile b) Sharing Relationship , and c) Sharing Resource .

a) *Sharing Profile*: Some OSMs support social applications developed by the third-party developers. To provide a better services, these social media applications save user profile information like name, birthday, activities, interests, and so on. Some social media applications on current OSMs platforms can also use the profile attributes of a user's friends. Here user selects a specific bits of profile information to be shared with the applications when their OSMs friends use the applications. And also the control is given to the owners friend who shared the application to filter the information of his application contributor.

b) *Sharing Relationship*: OSMs allow users to share their relationship with other users. And this relationship is bidirectional and hold a personal information that user never want to disclose. Even this feature is bidirectional the control given to the user is on a single direction. Example when user A decides not to disclose his friends list on the OSMs but the user B friend of user A have a policy which show all his friends list , through which the unintended users may get information about user A.

c) *Sharing Resource*: OSMs provides a method allowing users to connect and share resources with other users. Users can add grades , their thoughts, can upload photos and videos in their home spaces and can tag other user's to their resources, and share the resources with his friends. Users of online social medias also has a facility to write the note or to add the resources to his friends space and this resources may be linked with many users [8].

A. *MUAC model for OSMs*

OSMs are identified by the relationship network, total number of groups created by the user and user data. Here each node in the graph is identified as a user and each edge is denoted as relationship between two users. The label on the edge gives the type of the relationship. The direction of edge show the initial node of relationship edge and the terminal node of the edge. There are four controllers used in the multiuser access controller includes owner, contributor, stakeholder and disseminator.

a)Owner: Data items present in the space of user in the social medias and the user is considered as the owner of the data item. For example if user A posts some information in his own virtual space of the OSMs then user A is considered as the owner of the posted information.

b) Contributor: Data items present in the space of user in the social medias can be shared with other users of the same social medias who are in contact with the user. Here the one who shares the data from his own space to someone else space then the user is considered as contributor of the posted data.

c) Stakeholder: The data item in the users space in online social medias can be shared with the other users under the same media. The people or the users who get tagged to the data shared or uploaded is considered as the stakeholder of the particular data.

d) Disseminator: This is the reverse of contributor where the user who shares the data from the space of the contributor is considered as the disseminator[8].

B. *MUAC policy requirement*

It is important for multiuser access control policies to control access over shared data, signifying authorization requests from multiple associated users. Our policy requirement system is built upon the proposed MUAC model.

a)Accessor Requirement: A group of users to whom access is permitted to the shared data is usually called as accessor. Accessors can be denoted with a group of user names, a group of relationship names or a group of group names in OSMs.

b)Data Requirement: User data is classified into three major information type :user’s profile ,user relationship, user resources. Here sensation level of a data is calculated based on the multidimensional degree of sensation [8].

C. *Evaluation of an access request over MUAC*

The performance is calculated in two different levels.

a)Access Request: When a user make request to access a resources. The request is cross verified with the policy generated for a particular request. if the verified accessor request matches the policy specified then the access to a particular resource is granted or else an exception is raised and the permission is denied .

b)Aggregated Decision: Here decision from all the controllers are aggregated and the final decision is made against the access request of a particular resources. Since multiple users share a same resource each user have their own privacy concern and a privacy policy for a particular type of data , therefore our system provide a policy controller for each users who share the same resources by which the common friends of both users can view the data posted by the users with control given to all the intended users.

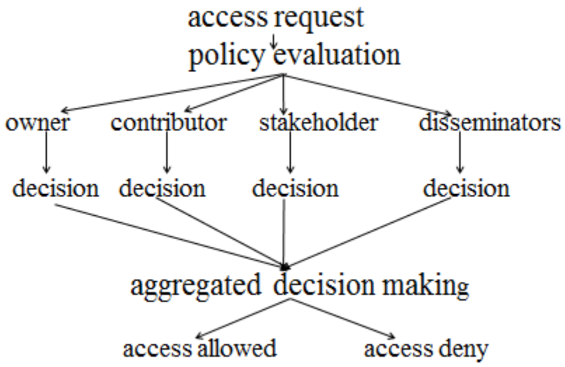

Fig.4 MUAC policy requirement

D. *Implementation of MUAC model*

Mcontroller application has been used here to get the authorization policy and privacy to control the shared data items. This Mcontroller is divided into two levels: social media server and application server.

a)Social media Server: The social media server provides an access point via the social media application page, and offers references to photos, friendships, and feed data through API calls. Social media server takes input from users and forwards them to the application server.

b)Application Server: This is responsive for the processing of user input and management of users shared data. Information related to user both personal and social are stored in the application server database.

This Mcontroller is a third party developed social media application held in an Apache tomcat application server supporting JSP and MySQL database. Once this application is installed in the users space this application keep all the basic information about the intended user and also keep the record of all the photos or data uploaded by the user and also he has been tagged in. then when user access his personal home page each and every photo/data shared or uploaded can be controlled based on the privacy issues and policies specified for each and every information separately. The core component of this application is decision making about the request for access and return the response based on the policies specified.

When a photo/data uploaded by the user through this application, each is specified with the values. The owner of the data possess highest value and he has the authority to specify the tagged users values based on which the tagged users (stakeholder) get control over the data they are tagged in with minimum values for them and these stakeholders have a right to specify the access control for the list of friends [8].

CONCLUSION

OSMs are trending in the so called virtual world i.e. Internet, where more and more users personal information’s are leaked. Hence forth this paper planned to bring out the privacy conflict and services provided by the OSMs. This paper also suggest the highly secured data sharing and tagging system handing over the control to every user through a MUAC model.

REFERENCES

[1] FacebookStatistics.http://www.facebook.com/press/info.php? statistics.

[2] R. Gross and A. Acquisti: “Information revelation and privacy in online social networks.” Proceedings of the 2005 ACM workshop on Privacy in the electronic society, pages 71{80, 2005}.

[3] Yuan Cheng, Jaehong Park and Ravi Sandhu: “Relationship-based Access Control for Online Social Networks: Beyond User-to-User Relationships”.

[4] Chi Zhang and Jinyuan Sun, Xiaoyan Zhu, Yuguang Fang: “Privacy and Security for Online Social Networks: Challenges and Opportunities”.

[5] João Paulo Pesce ,Diego Las Casas ,Gustavo Rauber ,Virgílio Almeida: **“**Privacy Attacks in Social Media Using Photo Tagging Networks: A Case Study with Facebook”.

[6] D. Kirkpatrick. The Facebook E_ect: “The Inside Story of the Company That Is Connecting the World.” Simon and Schuster, 2010.

[7] Ivan Ivanov, Peter Vajda, Jong-Seok Lee, and Touradj Ebrahimi: “In Tags We Trust[Trust modeling in social tagging of multimedia content].”

[8] Hongxin Hu, Gail-Joon Ahn, *Senior Member, IEEE,* and Jan Jorgensen :

“Multiparty Access Control for Online Social Networks: Model and Mechanisms”.