International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Multiparty Authorization for Data Shares in Online Social Networks

S. Ramijaanaki

PG Scholar, Rajalakshmi Engineering College, Chennai, Anna University, India

Abstract: ***Data share in Online Social Network OSN is a global event in digital world that enables digital social interactions. OSNs are dominant medium for social interaction experienced by real world to communicate and share data. OSN such as Facebook has several million users worldwide sharing abundant data items in real world. OSN provides security at the user level but no protection over data present outside user level. OSN lacks method to enforce security problems over shared data associated with multiple users in the real world. MPAC model (Multiparty access control model) is formulated to resolve the multiparty authorization issues. The issues not focused by existing access control methods. In addition to this, a voting mechanism, threshold policy added deals with the authorization and security issues. The use of MPAC mechanism enables flexibility of shared data in OSNs greatly reducing authorization and privacy conflicts in digital world.***

Keywords: OSN, MPAC model, Voting mechanism, Threshold policy, Access control systems.

1. Introduction

In the Cutting Edge technological field, the Online Social Networks facilitate Digital social interactions and information sharing around the world. There are a number of diversity of usage served by OSNs like Face book, Twitter, Google+, LinkedIn etc, Social networking is essentially vital for entrepreneurs, business people, students for connecting and sharing information with friends all over the world. OSNs facilitates its user's to share information like photos, videos, image content, links, news stories, messages, create user groups with common interests, write comments, tag photos, photo album and so on. Most familiar social networking sites such as Facebook enable sharing of data items like photos, videos, news feeds, etc,. Facebook contains more millions of users uploading and downloading billions of information in the real world. Several billions of data contents of data shared per day. When a user signs up in a Social network, like Facebook user can create user profile containing personal information like name, age, DOB, gender, education, job profile etc., and contact information. Social networking site facilitates the users to send friend requests and accept friend requests from friends across the world. OSN also offers a space such as 'Wall' in Facebook where users can write content and send messages. User can also upload or download a content photo/video and share with friends. User can set personal authorization like friends, friends of friends FOF, groups or view the uploaded content. OSNs provide security at the user space but there is no protection for data residing outside user's space. The user's apart from uploading the content like photo in the user's space or others' space, user's can also tag other users present in the photo.

When a user uploads a photo and shares to user's friends, the user's friend can not only view the shared photo but also tag to the latter's friends. But the tagged friends may have different privacy concerns about the photo. To resolve this type of critical issue existing OSN Facebook allows tagged users to remove the tags linked to user's profile or report violations requesting Facebook managers to remove the content of user's interest (i.e., Content that user considers private). Neither of the above resolutions provided addresses the issue. The reason being that removing a tag can restrict other users from viewing the user's profile, however user's image is still present in the photo. Also reporting to OSN managers only has twofold options either keep file or remove it. Data security is highly indispensable to protect user's data and prevent privacy issues. As some of the privacy concerns are inexorable in multiparty data sharing, there is a need for a highly steadfast access control model to address the privacy concerns over shared data and enable flexible data share.

Figure 1: Online Social Networks

1.1 Types of Online Social Networking

Geo-social Networking is a type of social networking that facilitates geographic services such as geocoding and geotagging enabling additional social dynamics. User oriented location data or geolocation techniques can allow social networks to connect and coordinate users with local people or events that match their interests. Geolocation on web-based social network services can be IP-based or use hotspot trilateration. For mobile social networks, texted location information or mobile phone tracking can enable location-based services to enhance social networking.

Mobile social networking is social networking where individuals with common interests communicate and connect with one another using their mobile phone and/or tablet. Much like web-based social networking, mobile social networking occurs in virtual communities. A current trend for social networking websites, such as Facebook, is to create mobile apps to give their users instant and real-time access from their device.

Personal networking is the view of building and maintaining a personal network, which is more often undertaken over an extended period of time. Personal networking is often encouraged by large organizations, in the hope of enhancing productivity, and also a number of tools exist to enable the maintenance of networks. Many of these tools are IT-based, and use Web 2.0 technologies.

Professional networking service (in an Internet context, merely a professional network) is a kind of social network service that is focused exclusively on communications and relationships of a business environment rather than including personal, non-business environment.

Virtual community is a social network of persons who interact through precise social media, potentially crossing geographical and political boundaries in order to track mutual interests or goals. Some of the most invasive virtual communities are online communities working in social networking services.

1.2 Features of Online Social Networks

Online social networking sites share a variety of technical features that allow individuals to: construct a public profile, articulate a list of other users that they share a connection with, and view their list of connections within the system. The most basic of these are visible profiles with a list of "friends" who are also users of the site. In an article entitled "Social Network Sites: Definition, History, and Scholarship," Boyd and Ellison adopt Sunden's (2003) description of profiles, as unique pages where one can "type oneself into being". A profile is generated from answers to questions, such as age, location, interests, etc. Some sites allow users to upload pictures, add multimedia content or modify the look and feel of the profile. Others, e.g., Facebook, allow users to enhance their profile by adding modules or "Applications.". Many sites allow users to post blog entries, search for others with similar interests and compile and share lists of contacts. User profiles often have a section dedicated to comments from friends and other users. To protect user privacy, social networks typically have controls that allow users to choose who can view their profile, contact them, add them to their list of contacts, and so on. Some social networks have additional features, such as the ability to create groups that share common interests or affiliations, upload or stream live videos, and hold discussions in forums. Geo-social networking co-opts Internet mapping services to organize user participation around geographic features and their attributes.

2. Related Work

The primary issue in today's OSN is display of unwanted content on the user's wall. Users need to eliminate unwanted information posted on the user's wall so users must be certain to customize the contents put up in the user's wall, to evade the display of unwanted data. This is accomplished by use of rule-based system that facilitates users to customize the filtering criteria on the wall [2]. Also the Machine Learning based soft classifier finds its importance in content-based filtering, thus enabling the labelling of messages. Users need to eliminate unwanted information posted on the user's wall so users must be certain to customize the contents put up in the user's wall, to evade the display of unwanted data. This is accomplished by use of rule-based system that facilitates users to customize the filtering criteria on the wall. Content-based filtering is chains user preferences and item contents correlating with each other. Content-based filtering is based on induction of pre-classified data to the classifier. The challenging task is classification of short text strings by Content-based filtering.

Potential technologies like Web services, SOA, Cloud computing have increased the performance of business world. Despite this, the user's experience severe security leakages as the Web access control policies are prone to errors. Logic-based policy management is realised to evade the issue. Web access control policies that focus on XACML (extensible Access Control Mark-up Language) and RBAC (Role-based Access control) are extensively used by Web-oriented technologies. The adoption of Answer Set Programming to devise XACML enhances logical analysis and reasoning. XACML2ASP method along with XACML policies in real-world software systems are evaluated [5]. XACML (Extensible Access Control Mark-up Language), an XML-based language standardized by the Organization for the Advancement of Structured Information Standards (OASIS). XACML is highly flexible to enhance access control models. XACML, an efficient standard for access control policies and offers a large set of built-in functions, data types, algorithms, and standard profiles for defining application oriented features.

Novel management of personal photos in OSNs is highly significant in real world. The proposed Collaborative FR (Face Recognition) method enhances accuracy of Face annotation by multiple FR engines in OSN and design is also suitable for a decentralised zone. It facilitates selection of FR engines and fusion of multiple FR results. For this strategy social context in personal photo collections in OSN and the combination of results from multiple classifiers are used [3]. The execution of labeling persons (i.e., names of individuals or subjects) on personal photos is called face annotation or name tagging. Most of the OSNs only enable manual face annotation, a time-consuming and demanding task. The number of personal photos shared on OSNs grows at a fast pace.

The Access control model for Facebook Facebook-style social Network Systems (FSNSs) sets a graph-theoretic relation between resource owner and accessor in social graph. The topology of the social graph may be changed by pseudonymous persons who gains illegal access. This type of Sybil attack can be eliminated by Denning's Principle of Privilege Attenuation (POPA). A static policy to check POPA compliance of FSNS is formulated [4]. A unique feature of FSNSs is that every access control policy specifies a graph theoretic relationship between the resource owner and the resource accessor (e.g., the owner and accessor share or more common friends). Access is granted when the stated relationship is realized in the social graph. It is demonstrated that some FSNSs, when improperly configured, are amenable to Sybil attacks as said by J. R. Douceur. In a classical Sybil attack, a malicious user of a peer-to-peer system creates multiple pseudonymous identities, and uses their combined influence to bypass the status of the system.

Essential need in today's OSN is facility of user to manage messages posted on user's own clandestine space. This is done by twofold methods 1) Flexible rule-based system that facilitates filtering option applied to user walls by user. 2) Machine learning based soft classifier capable of labeling messages relying on content-based filtering method [6]. A flexible rule-based system, allows users to customize the filtering criteria to be applied to their walls, and a Machine Learning based soft classifier which automatically generate membership labels in support of content-based filtering.

It is challenging to realise formal models in the system development phase. The Model Driven Development (MDD) approach applied deals with such a critical issue for building high assurance software systems. The MDD approach consent rates on the transformation of high-level design models to system implementation modules. However, this emerging development approach lacks a sufficient approach to address security issues derived from formal security models. An empirical framework to integrate security model representation, security policy specification, and systematic validation of security model and policy, which would be eventually used for accommodating security concerns during the system development, has been proposed by Gail Joon Ahn et al. [7] The gap between security models and the development of secure systems and its security has been described. Also an overview of a proof-of-concept prototype of the tool that facilitates existing software engineering mechanisms to achieve the above-mentioned features of the framework has been elaborated.

Topology-based access control is a yardstick for securing resources in On-line Social Networks OSNs including all research community and commercial social networks. Based on this the authorization restraints identify the relationships levels that should occur between the requestor and the resource owner to make enable access to the required resource. It is shown how topology-based access control can be improved by exploiting the collaboration among OSN users, which is the quintessence of any OSN. The requirement of user collaboration during access control enforcement begins due to the fact that, different from traditional settings, in most OSN services users can reference other users in resources (e.g., a user can be tagged to a photo). It is generally not feasible for a user to control the resources uploaded by other user. A collaborative security policies, access control policies identifying a set of collaborative users involved during access control enforcement is elaborated. Moreover, elaboration on user collaboration for policy administration is done by B. Carminati and E. Ferrari [8] 2011. Also architecture on supporting collaborative policy enforcement is proposed.

The OSNs rely on access control systems that are different from the traditional access control systems. Gates invented the Relationship based access control also termed ReBAC. The interpersonal relationships between social network users are studied and policies and expressions are coined and evaluated based on the interpersonal relationships between users. Resource owner and resource accessor relationships form the basis of authorization decisions in the social network systems. The uniqueness of the model is that it captures the contextual nature of relationships. A policy language based on modal logic for creating access control policies that enhance the trust entrustment.

3. Proposed Approach

The proposed system shows a fresh solution for collaborative management of information sharing in OSNs. It enables secure posting of information and secure tagging. OSN contains users, groups, friends, FOF friends of friends, posted / shared data such as photo, video or event.

Owner: When 'user' posts a data d in user's own profile, then user is coined the name 'Owner'. Data may be personal information and professional information of the user.

Contributor: When 'user' uploads a data d in other's space , then user is coined the term 'Contributor'. All the users of the OSN are contributors at some point of time. Contributors are the active users of online social network.

Stakeholder: When a user 'Alice' posts a photo to other user (user's friend) 'Bob', then the latter is termed 'Stakeholder' of data.

Disseminator: When a user 'Alice' shares a data to user 'Bob', and the friend of 'Bob' i.e., user 'Carol' views the data via user Bob, then user 'Carol' is disseminator ie., FOF friend of friend to user 'Alice'.

When the stakeholder shares a data such as photo/video to a friend, disseminator of stakeholder can view the shared data or photo. Secure posting evolves in this scenario when the disseminator is restricted from being aware of the identity of the Owner.

In an OSN such as Facebook, there may be several groups with similar interest users. When a person in the group shares a data, puts it in the group all the members of the group views the shared data or information. Our objective is restricting the members of the group from the knowledge that all the members of the group are aware of the received file. This is similar to one to one graph-theoretic relationship wherein the owner sends data/file to a stakeholder.

MPAC Methods: The two essential objectives are secure posting of the data and secure tagging of data. These can be accomplished by MPAC (Multiparty access control) which incorporates Decision making, Threshold policy and voting mechanism. Multiparty access control deals with the fact of multiple users incorporating a collaborative control over a shared data item. The shared data item refers to a photo or video posted online.

Decision making: When Owner uploads a photo to the group, the decision to make the photo private or public depends on the users concern. Decision making equation is described based on the above scenario involving binary values 0 or 1. 'Avg' refers to average as seen in the below equation.

$$\text{Decision} = \{\text{Allow if } D_{avg} = 1$$
$$\text{Reject if } D_{avg} = 0\}$$

Voting mechanism: In the Alice, Bob, Carol and Dave scenario, Owner Alice shares the data with Bob privately and in turn Bob sharing with Carol publicly, depending on how many users are willing to make photo public (non-confidential) or how many users are willing to make the photo private (confidential) vote is evaluated and the weight age is given accordingly.

The votes of the users are considered and value '1' is assigned when the photo is 'permitted' by users or the value '0' is assigned when the photo is 'denied' by the users.

A decision voting value (DV) put from the policy and is defined as follows, where the decision valuation (p) returns the decision of a policy p, policy p is user voting the photo 'public' or 'private'.

$$DV = \{0 \text{ if valuation } (p) = \text{Allow}$$
$$1 \text{ if valuation } (p) = \text{Reject}\}$$

Threshold policy: Considering the above mentioned scenario, the basic idea is that based on the weight age given to the photo depending on the Voting mechanism, results can taken or decided whether to permit or deny that photo based on the below equation.

When majority of users had given 'allow' consent for the photo i.e. 'permit' Dave average is more than half the number of users then the photo is allowed. Similar condition is evaluated for 'Deny' scenario.

$$\text{Decision } D = \{\text{Allow if } D_{avg} \geq 1/2$$
$$\text{Reject if } D_{avg} \leq 1/2\}$$

4. System Architecture

The proposed and implemented system concentrates on secure posting, secure sharing of information and secure tagging concerned with multiple users of online social network.

When a user access the social site, the user sends HTML request to the social site, and return response HTML response is received by the user from the social site. Internally, the social site network accepts the HTML request from the user and sends the API (Application interface) response to the Application server. The Application server processes the response received from the Social Site application and in turn sends the API (Application interface) Call to the Social Site application (Fig 1). The Social Site application receives the API Call from the Application server and in turn the Social Site application sends the HTML response to the user. All the MPAC methods including policies, mechanisms, are managed by the Application server. Fig 2 shows the data flow in online social network.

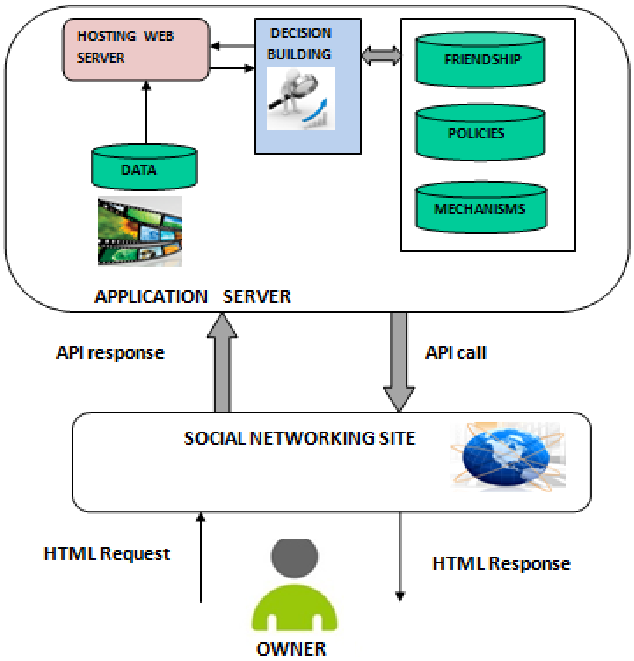

Figure 2: Architecture of MPAC

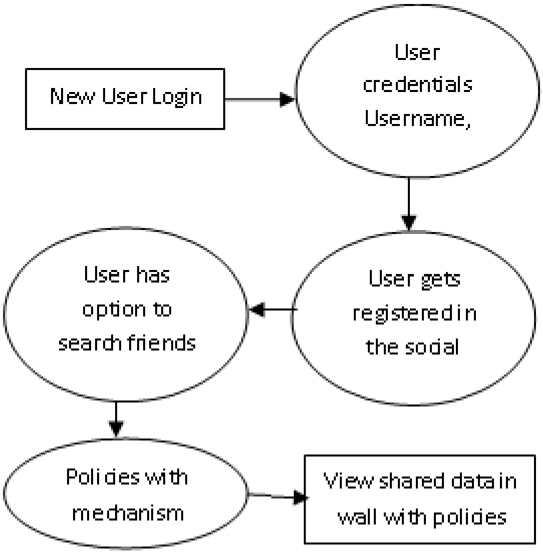
New User Login
User credentials Username,
User gets registered in the social
User has option to search friends
Policies with mechanism
View shared data in wall with policies

Figure 3: Data flow in OSN

5. Implementation

A. Handling Social Network
B. Profile & relationship shares
C. Photo/video sharing

5.1 Handling Social Network

Using social network application is instantiated when user registers and logs on to the social network. It also integrates the start of personal user profile with Name, Age, Date of Birth, Gender and contact information. When Owner Alice shares a data, the data shared by Alice is accessed by the stakeholders.

When Alice posts a data photo or video the stakeholders, friends of Alice can not only view the photo but also share with the friends, Disseminator FOF for Alice. The Disseminator has the information about identity of user Alice. The MPAC Multiparty access control methods and policies used provide effective solution.

5.2 Profile and Relationship Shares

Online social network allows users to share user's personal details, professional details contact information and many more. The relationship within Owner, Stakeholder, Contributor, Disseminator are analysed based on the flow of information within them (Fig 4)

When Alice uploads a photo to Bob privately, Bob can not only view the photo shared by Alice but also share the photo to Bob's friends. If Bob shares the photo publicly to Carol, Carol will be unaware of the identity of Alice on using MPAC policies and methods.

5.3 Photo/Video Sharing

The initiation of 'Groups' in social networks are indispensable in real world. Groups are created by users of common interest. Several types of groups are present in the real world social network. Some of the groups are personal interest, family group, profession group, business group, work groups etc.

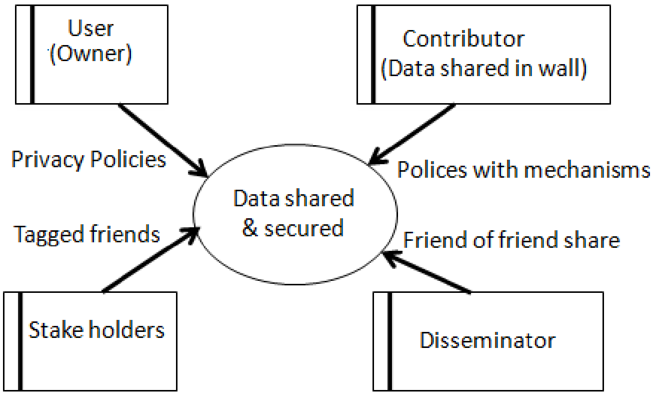

Figure 4: Data flexibility and Security

When user in the group shares a data, it all the members of the group are aware of the shared data and every member in the group is aware that particular data can be accessed by all the members of the group. Using MPAC methods it is possible to share data in a group without the knowledge that each other member is aware of that particular data item similar to one to one data share. It is all possible for the Owner to exclude that data share to particular member in the group of Owners interest and share the data to remaining users in the group, yet the members of the group are unaware about the knowledge of other member accessing the shared data item

6. Conclusion

In this paper we proposed and implemented a solution for data sharing for social networks online. Furthermore the MPAC methods involving Voting mechanism, Threshold policy, Decision making effectively diminishes the privacy concerns and also improves the flexibility of data shares among online social network users. Also the inevitability for collaborative management of data sharing is realized and implemented.

7. Acknowledgement

The completion of this work could not have been accomplished without the support of our professor Dr.G.Sujitha and our teachers in our college. I am very much thankful to all of them. For the reference, we referred many articles and research papers of many authors and institutions those are available in online and offline. We offer our sincere appreciation for the learning opportunities provided by those authors and our institution. Our heartfelt thanks to all our family members for caring and supporting us.

References

[1] Hongxin Hu, Member, IEEE, Gail-Joon Ahn, Senior Member, IEEE, and Jan Jorgensen "Multiparty Access Control for Online Social Networks: Models & Mechanisms" IEEE Transaction on Knowledge and Data Engineering, JULY 2013

[2] Marco Vanetti, Elisabetta Binaghi, Elena Ferrari, Barbara Carminati, Moreno Carullo, "A System to Filter Unwanted Messages from OSN User Walls"IEEE Transaction on Knowledge and Data Engineering, Vol: 25 Year 2013.

[3] Jae Young Choi, Wesley De Neve, Konstantinos N. Plataniotis, and Yong Man Ro, IEEE "Collaborative Face Recognition for Improved Face Annotation in Personal Photo Collections Shared on Online Social Networks" IEEE Transaction on Multimedia , Vol. 13, No. 1, February 2011.

[4] Philip W. L. Fong "Preventing Sybil Attacks by Privilege Attenuation: A Design Principle for Social Network Systems" 2011 IEEE Symposium on Security and Privacy.

[5] Gail-Joon Ahn, Hongxin Hu, Joohyung Lee and Yunsong Meng "Representing and Reasoning about Web Access Control Policies".

[6] A. D. Swami, B. S. Khade "A Text Based Filtering System for OSN User Walls" International Journal of Advanced Research in Computer Science and Software Engineering Volume 4, Issue 2, February 2014**.**

[7] G. Ahn and H. Hu, "Towards Realizing a Formal RBAC Model in Real Systems," Proc. 12th ACM Symp. Access Control Models and Technologies, pp. 215-224, 2007.

[8] B. Carminati, E. Ferrari, and A. Perego, "Enforcing Access Control in Web-Based Social Networks," ACM Trans. Information and System Security, vol. 13, no. 1, pp. 1-38, 2009.

[9] J. Douceur, "The Sybil Attack," Proc. Int'l Workshop Peer-to-Peer Systems, pp. 251-260, 2002.

[10] P. Fong, "Relationship-Based Access Control: Protection Model and Policy Language," Proc. First ACM Conf. Data and Application Security and Privacy, pp. 191-202, 2011.

Author Profile

S.Ramijaanaki is currently a PG scholar in Computer Science and Engineering from the Department of Computer Science at Rajalakshmi Engineering College, Chennai. She received his Bachelor Degree with distinction in Computer Science and Engineering from RMK Engineering College, Chennai and Tamilnadu. Her Research areas include Computer Networking and Data Mining. She has served in the IT field for 5 years, worked at Patni Computer Systems, Mumbai now iGATE Global Solutions. Her Research areas include Computer Networking, Data Mining and Graph Theory applications.