Enhanced Multiparty Access Control in Online Social Network

Smita Vishnu More
PCE, Department of Computer Engineering, New Panvel, Mumbai University
Email- smitavmore@mes.ac.in

Madhumita Chatterjee
PCE, Department of Computer Engineering, New Panvel, Mumbai University
Email- mchatterjee@mes.ac.in

***Abstract*— Todays Generation has totally been dependent on online social sur ng and their usage as a part of entertainment. People share their valuable information through these social surfing sites, content shared includes their interests such as, like's dis-likes and other favorite contents. Several social networking sites, individuals are not aware of the numerous security risks that exist in the networks. As per the recent studies, OSN's reveal many of the crucial and personal data like the relationship status, date of birth, school name, email address, phone number, and even home address. In order to secure these types of information some steps regarding the privacy managements has to be taken. Multiple users accessing a specific content need to be properly managed in OSNs, hence some access control modules have been introduced in the following work in order to obtain the optimal security.**

Keywords—online social networking, OSN, browsing, surfing

I. INTRODUCTION

OSN's have gained a vast popularity in the recent years, its use has increased on a wider scale. Millions of users today exists on different OSN's sharing their personal and professional data. These contents are exposed to the outer world, through which communication and interaction happens. OSNs like Facebook, Google+, LinkedIn, Twitter, and Orkut have hundreds of millions of daily active individuals. While such networks do allow users to control what they share with whom, hence the access policies need to be managed properly as they can be misused by the predators or intruders. This raises the question of whether OSN users' personal settings match their sharing intentions or not? Hence a secured accessing mechanisms is needed to handle these their information.

Access control mechanisms for OSN plays a major role in authentication and accessing rights to a particular user. Likewise the Traditional access control was based on a particular user whereas the advanced access control comprises of multiparty means more than one user and their accesses. In this work, multiparty access control mechanisms are initiated in some of the security domains like the authorization rights. The modules like Fake Identity attack and Parental Control are introduced with the Filtered Authorization rights given to a specific individual. Accordingly, the content on the social media can be managed with specific decision making module along with the sensitivity score.

II. LITERATURE SURVEY

In this section, the relevant literature survey that uses various techniques for different access control mechanisms. Multiparty Access Control and Relationship access control policies along with the filtering policies are described in this section. The Policy language specification is also included in this section along with all other references related to access control in Online Social Networking.

Michael Fire, Roy Goldschmidt, and Yuval Elovici 2014 [1] share a vast review on the existing Online Social Network threats and solutions which elaborate and provides a thorough review of the different security and privacy risks, which threaten the well-being of OSN users in general, and children in particular along with an overview of existing solutions that provides better protection, security, and privacy for OSN users. There are remedies to these threats, which have offered a range of solutions to help protect an OSN user's privacy and security.

Multiparty Access Control for Online Social Networks: Model Jan Jorgensen 2013 [2], proposed a MPAC Model consisting of the MPAC Access specification and the MPAC policy evaluation mechanism. An MPAC model was formulated, along with a multiparty policy specification scheme and corresponding policy evaluation mechanism. A proof-of- concept Implementation of the solution called MController has been derived, followed by the usability study and system evaluation.

Relationship-based Access Control for Online Social Networks: Beyond User-to-User Relationships 2012 [3], proposes the User-to-User, user-to-resource (U2R) and resource- to resource (R2R) relationships. The paper have developed an access control model for OSNs that provides finer-grained access control for users usage and administrative access by utilizing user-to-user, user-to-resource and resource-to-resource relationship-based policies. The ReBac model introduced plays a major role is establishing the defined relations between the user and resources.

A Semantic Web Based Framework for Social Network Access Control 2009 [4], in this paper the policy are derived from the OWL (Web Ontology Language) and SWRL (Semantic Web Rule Language). An extensible fine grained online social network access control model based on semantic web tools is derived. The User to Resource model is explained by specifying a trusted relationships; the paper majorly focuses on the Authorization and Filtering Policies for Privacy and security control in the Online Social Networking Sites.

Sakshi Jain ,Juan Lang, Neil Zhenqiang Gong, Dawn Song, Sreya Basuroy, Prateek Mittal [5] in their paper New Directions in Social Authentication proposed an architect system for social authentication that asks users to verify information about their social contacts and their interactions. The system leverages information which is secured by the privacy policies of Social Networks to restrict the attacks, such as questions based on private user interactions including exchanging messages and poking social contacts.

Detecting and resolving privacy conflicts for collaborative data sharing in online social networks 2011 [6], this paper proposes a systematic mechanism to identify and resolve privacy conflicts for collaborative data sharing. The authors have represented an effective and flexible mechanism to support privacy control of shared data in OSNs. They have given an analysis of data sharing associated with multiple users in OSNs, which articulate several typical scenarios of privacy conflicts for understanding the risks posed by those conflicts. Hence, the paper gives defined mechanism to support privacy control of shared data in OSNs.

Enforcing Access Control in Social Network Sites 2010 [7], proposes a practical, SNS (Social Network Service) platform-independent. Solution, for social network users to control their data. The paper uses encryption to enforce access control for user's private information based on the privacy preferences. Hence the model have implemented the model as a Firefox extension. A general approach to describe the management of accessing restrictions for different OSN's platforms is described in the paper.

Georgios Kontaxis, Iasonas Polakis, Sotiris Ioannidis and Evangelos P. Markatos, 2011 [8] proposes a prototype based approach in their Detecting Social Network Profile Cloning paper. The architectural design and implementation details of a prototype system can be employed by users to enquire whether they have fallen victims to any such malicious attack.

From the above literature, we can conclude that some of the Conflicts in the policy need to be resolved and some security and privacy modules need to be added for securing Online Social contents and information , hence the motivation for the work includes Fake identity prevention, Image security and Parental Control up to an extent.

III. PROPOSED SYSTEM

OSNs have been a developing medium for communication in the social environment, hence as of technological growth there has also been issues related to OSNs. The upcoming OSN threats are generally related to the Identity concerns. Hackers, Bots and other have increased their malicious activities by targeting specific audiences. In order to overcome these issues some prior mechanisms are needed before getting started with the OSN. These mechanisms are related to the fake identity and controlling mechanisms, also the recommendation techniques in OSN need to be improved. The architecture relates to such multiparty privacy settings. Accordingly the proposed architecture majorly work to resolve the OSN identity related threats along with the Improved Parental control mechanisms and Image security module.

A. Proposed OSN Architecture

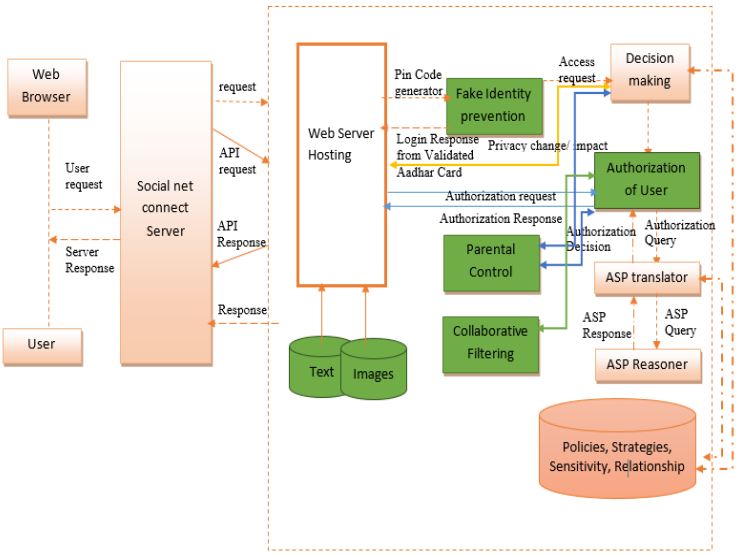

Figure 1:- Block diagram of proposed system

The above Figure shows the overall proposed architecture comprising of the enhancements including the Fake Identity attacks and parental control. Along with the authorization rights for accessing the social profiles.

1. Decision Making Module

The Decision making module, works on the access requests and responses, accordingly by considering the decision through the involved individuals and sensitivity voting the accesses is given in the form of either permit or deny. It is the most vital component of the overall architecture. To evaluate an access request the accessing policies of each controller of the objected content are enforced first to generate a decision for the owner. Then, all controller's decisions are aggregated to yield a final decision as the response of the request.

2. Authorization of User

This module is entirely responsible for giving the authorization to the respective users, when asked the details entered with unique ids, are saved and given authorization for the access. This module is connected to web server hosting and accordingly the responses is achieved. Parental Control module is also connected to authorization module.

3. ASP Translator/ ASP Reasoner

Answer Set Programming, Translator and Reasoner plays the analytical role in the architecture. They can be formulated in any languages. They provide the translating and reasoning of the policies and the queries. The analysis part is done by the ASP Translator which works in collaboration with the ASP Reasoner. Hence, they allow individuals to analyze the complicated for of queries through the translator and the reasoner.

4. Fake Identity Prevention

The main purpose of this module is to eliminate the fake and false identity accounts. Methods for Fake Identity Theft Attack the module works in the following manner:-

- Fake Identity Attack Prevention mechanism is done by using PIN for every time login, which is Session password module.
- Accordingly the Privacy preserving module is further used wherein the shared can be allowed to be displayed as per the privacy user space in private and public as per the user want.

Things which are mandatory to be entered during registration are- correct contact no, alternative contact and email address, accordingly select the settings of the wall-private/public/ both private and public and further save details and proceed.

The new Friend request thereafter will be managed by searching the user, than adding a defined relationship of the user and then accordingly sending the request. Similarly, if the friend request is to be accepted the notification will be checked and accordingly the request will be either accepted or declined.

Working mechanisms of the Fake identity Module- This module accepts the request through a Pin Generator from the Web server hosting and sends back the log in response from the valid Aadhar Card registration database. Hence the new registered user here are validated as unique individuals assuring there credentials with identities. Further, the access request is only given via the Decision making module.

5. Image Security Module

The image security module deals with the images and their contents, it gives a proper authorization to the main user to access his/her own image published on their social web page. This module starts its working after the valid authorization account which is obtained from Fake Identity module. Accordingly the sensitivity of every image is set, and the image is shared only with the specified users.

As the owner of image, the owner is supposed to select an image, set the sensitivity level, select the user to whom want to share and then select the wall on which you want to share that image.

Method used for Image Security-

For example-when a new user has visiting the Social Website. They are first ask for registration and accordingly diverted to the registration page. '*' Fields which are mandatory like the correct contact no, alternative contact and email address, users Aadhar card number, the division of wall or user space in private and public and both as per user want ; hence a new user has to fill information as well as select the settings of the wall private/public/ both private and public. Accordingly, save the details of new user and divert him/her for login.

For the New user login -

- Ask that user for the username and password
- For each session, we have to generate Pin as OTP for that user
- Send OTP to contact number
- If login credential is valid and correct; then login
- Else ask for correct password

Sensitivity level calculation through MPAC Policy -

A MPAC policy is a 5-tuple [2]-

$< controller, ctype, accessor, data, effect >$

where,

- $controller \in U$ is a user who can regulate the access of data;
- $ctype \in CT$ is the type of the controller;
- accessor is a set of users to whom the authorization is granted; Accessors are a set of
- us'ers who are granted to access the shared data. Accessors can be represented with a set of user names, a set of relationship names or a set of group names in OSN
- data is a set of data set which is based on sensitivity level ranging from 0 to 1
- $effect \in \{permit; deny\}$ is the authorization effect of the policy

As per the MPAC strategy, suppose a controller can leverage five SLs: 0.00 (none), 0.25 (low), 0.50 (medium), 0.75 (high), and 1.00 (highest) for the shared data.

For example: -Here, Eve is the stakeholder (the tagged users associated with the data item) shares image trek.img with his friends hence the relationship is RN in a group, GN trekking of the sensitivity score 0.75 meaning 'high' allowing them to access the photo by stating permit as the decision.

p = (Eve, ST, {< friend Of, RN>, <trekking, GN>}, <trek.img, 0.75> permit).

The decision voting mechanisms here also need the same content as that of fake identity and accordingly the Image is to be allowed to be displayed on the owners wall by the owner.

Decision Voting Mechanisms-

MPAC decision voting [2] value (DV) derives a policy evaluation which is defined as follows, where Evaluation (p) returns the decision of a policy p:-

$$DV = \{0 \text{ Evaluation } (p) = permit$$

$$DV = 1 \text{ Evaluation } (p) = deny\} \quad (1)$$

$$DV_{avg} = (DV_{ow} + DV_{cb} + \sum_{i \in SS} DV^{i}_{st}) \times (1/m) \quad (2)$$

Table (1)- DV_{avg} results and Status

SN	DV_{ow}	DV_{cb}	DV_{st}	m	DV_{avg}	Status
1	0	0	0	3	0	Deny
2	0	0	1	3	0.333333	Deny
3	0	1	0	3	0.333333	Deny
4	0	1	1	3	0.666667	Permit
5	1	0	0	3	0.333333	Deny
6	1	0	1	3	0.666667	Permit
7	1	1	0	3	0.666667	Permit
8	1	1	1	3	1	Permit

In Table (1) the DV of the owner, contributor and the stakeholder are given by 0 the permit and 1 deny static value, as 3 controllers are involved owner, contributor and the stakeholder; hence the DV_{avg} is calculated.

$$DV_{avg} = (w_{ow} \times DV_{ow} + w_{cb} \times DV_{cb} + \sum^{n}_{i=1} w^{i}_{st} \times DV^{i}_{st}) \times (1/ w_{ow} + w_{cb} + \sum^{n}_{i=1} w^{i}_{st}) \quad (3)$$

Table (2) - DV_{avg} through defined values of weights

SN	DV_{ow}	DV_{cb}	DV_{st}	w_{ow}	w_{cb}	w_{st}	DV_{wavg}	Status
1	0	0	0	3	5	5	0.18	Permit
2	0	0	1	3	4	5	0.416667	Deny
3	0	1	0	4	2	1	0.285714	Deny
4	0	1	1	1	4	6	0.909091	Permit
5	1	0	0	5	7	6	0.205556	Deny
6	1	0	1	4	3	2	0.666667	Permit
7	1	1	0	5	6	3	0.785714	Permit
8	1	1	1	4	5	7	1	Permit

In Table (2) the weights w_x assigned for Decision Voting mechanism in Table (2) are based on the trust and reputation level, hence it is represented in the integer format n, here it is been considered integer values ranging from 1-10 which are to be assigned by the controllers.

Here in Table (2) these weights are statically assigned and accordingly the DV_{avg} is calculated.

Table (3) Final average status

Status DV_{avg}	Status DV_{wavg}	Final Status
Deny	Permit	Permit
Deny	Deny	Deny
Deny	Deny	Deny
Permit	Permit	Permit
Deny	Deny	Deny
Permit	Permit	Permit
Permit	Permit	Permit
Permit	Permit	Permit

Table (3) gives the Final Decision status by considering the DV_{avg} and DV_{wavg} OR values.

Hence, the Decision voting involves the Individual Decision and the weights assigned by the controllers, on which the decision is given.

Sensitivity Voting Mechanism

In MPAC [2], each controller assigns an SL to the shared data item to reflect her/his privacy concern. A sensitivity score (Sc) (in the range from 0.00 to 1.00) for the data item.

$$Sc = (SL_{ow} + SL_{cb} + \sum_{i \in SS} SL^{i}_{st}) \times (1/m) \quad (4)$$

Table (4)- Sensitivity count and ratings results

SN	Sc_{ow}	SC_{cb}	SC_{st}	m	SC	Level
1	0.25	0.75	0.5	3	0.5	medium
2	0.1	0.5	0.15	3	0.25	low
3	0	0	0.1	3	0.033333	none
4	1	0.75	0.5	3	0.75	high
5	1	0.75	1	3	0.916667	highest

In Table (4) the level decides the preference of the content to be shared with the number of the controllers over the OSN. As per the level the number of audiences can be controlled.

Hence, the aggregation of Decision and Sensitivity voting is considered for giving the authorization to any of the content.

6. Parental Control Module

This module represents the Parent- Child relationship, in which the parent as an individual guardian can access the child's social account. In order to track their activities. These activities are viewed on static basis wherein the database once viewed cannot be regained.

The Registration Method are used for Parental Control mechanisms- There are two registration forms are required, the Parent form and the Child form:-

- Parent form requirements (above 25):- Parent email, Parent age, Parent Aadhar card Details (unique identity), Child Details and the Relationships
- Child Form requirements (below 14):- Child details, Child Birthday, Child-Email, Child Aadhar card details, Child Surname

The child details entered by Parent will be matched with the Child details entered by child. At a time only one email will be

allowed from parent side to be tracked to that o child. If child is attempting to open another account than the questions will be asked whether pre-account exist or not. Further if details vary than birth-date can be traced with the other details and accordingly the account will be trapped. After the registration the One Time Password will be generated and accordingly can be used to access every time. Hence through random OTP parent can access the child's pro le statically in screen shot format which after viewing once will get deleted.

For example: any session in policy can be formulated as - If the child is trying to upload any content like photo and if the parent is trying to view it, the child has uploaded a photo along with tags, then the parent gets the precedence to view the photo. The following [3] has been formulated with SWRL and OWL notations.

Policy-

if

{

child<upload, (tag Λ photo)>

then

<view(parent>@)>

parent <view, (child Λ photo)>

}

Here, the 'Λ' notation denotes the Conjunctive Connective relation which denotes the conjunction of multiple path specs. '@' denotes the precedence value assigned to any user.

Hence similar policy can be generated for other activities also.

8. Policies, Strategies, Sensitivity Related Analysis

These are the inventory system wherein the assigned policies, strategies and accordingly the sensitivity analysis is stored. The policies generated are judged on the sensitivity score. The analysis section including the ASP Translator and Reasoner is associated with these system. Hence these play a major role in entire architecture and its mechanisms.

Hence, these modules interacts with the existing architecture which comprises of-

9. Interactive Modules

- Web Browser- Web browser can be any browser available on the internet, it is the platform provided for surfing, right now there are many web browsers existing for example the internet explorer, Mozilla Firefox, google chrome and many more. These provide the base to the browsing activity.

- User- A user here means the owner or the participants who browses over the web browser and is willing to surf over the social networking sites.

- Social Net Connect Server- The social net connect server provides an entry point via the social network application page, and provides references to photos, friendships, and feed data through API calls. Social net server accepts inputs from users, then forward them to the web server hosting server.

- Web Server Hosting- Web server hosting is an application server which is responsible for the input processing and collaborative management of shared data received from the social net connect server. Information related to user data such as along with the API request and other request like the user identifiers, friend lists, user groups, and user contents are accepted and accordingly the response is sent back after processing through the various parameters.

IV. COMPARISON WITH THE EXISTING SYSTEM

The following Table (5) represents the existing and proposed work of the OSN, some of the mechanisms and methods have been implemented in the proposed architecture.

Table (5) Comparison Table

SN	Paper	Existing Work	Proposed work
1	Multiparty Access Control for Online Social Networks: Model and Mechanisms	MPAC Model and MController model is implemented for shared Photo; Decision and Sensitivity Voting mechanism is introduced.	The work can be ex- tended for Contents and videos also, along with Fake Identity detection and Collaborative Filtering
2	Relationship-based Access Control for Online Social Net- works: Beyond User-to-User Relationships	User-to-User, User-to- Resource (U2R) and resource-to-resource (R2R) relationships are extended for OSN. A ReBac model is introduced with Social Graph and HopCout Skipping concept.	Co-operative Parental Control can be achieved with effective Conflict Resolution Mechanism.
3	A Semantic Web Based Framework for Social Network Access Control	A Semantic Web Based Framework for Social Net- work Access Control model based on OWL and SWRL. The User to Resource model is explained by specifying a trusted relationships; along with Authorization and Filtering Policies.	The Authorization and Filtering policies can be used for Fake Identity and Parental Control mechanisms

V. CONCLUSION

A brief summary of the advanced access control models and their mechanisms are explained. The multiparty access control mechanisms includes groups or more than one user participation, wherein the access rights are also given to more

than one user. These are advanced type of accessing mechanisms wherein the fake profile identification can also be done by considering their unique identities prior to the activity on the OSN. The parental control module gives the authorization to the parent to access their child pro le statically and track their activities, and accordingly guide them in the future. The collaborative filtering mechanism recommend the most known and appropriate recommendation to the user, of their pro le and activities. Hence, we conclude that a secured type of online social networking site can be implemented with improvements in these proposed modules and their mechanisms.

REFERENCES

[1] Michael Fire, Roy Goldschmidt, and Yuval Elovici, Online Social Networks: Threats and Solutions, IEEE, 2014.

[2] Hongxin Hu, Gail-Joon Ahn, and Jan Jorgensen, Multiparty Access Control for Online Social Networks: Model and Mechanisms, IEEE, 2013.

[3] Yuan Cheng, Jaehong Park and Ravi Sandhu, Relationship-based Access Control for Online Social Networks: Beyond User-to-User Relationships, ASE/IEEE Inter-national Conference, 2012.

[4] Barbara Carminati, Elena Ferrari, Raymond Heatherly, Murat Kantarcioglu, and Bhavani Thurainsingham, A Semantic Web Based Framework for Social Network Access Control, SACMAT09, 2009.

[5] Sakshi Jain ,Juan Lang, Neil Zhenqiang Gong, Dawn Song, Sreya Basuroy, Prateek Mittal, New Directions in Social Authentication, ISBN, 2015.

[6] Hongxin Hu, Gail-Joon Ahn and Jan Jorgensen, Detecting and resolving privacy con icts for collaborative data sharing in online social networks, ResearchGate,2011.

[7] Hongxin Hu, Gail-Joon Ahn and Ketan Kulkarni, Anomaly Discovery and Resolution in Web Access Control Policies, SACMAT11, 2011.

[8] Barbara, Carminati, Elena Ferrari, Raymond Heatherly, Murat Kantar-cioglu,Bhavani Thuraisingham, Semantic web-based social network access control, ScienceDirect, 2010.

[9] Filipe Beato, Markulf Kohlweiss, and Karel Wouters, Enforcing Access Control in Social Network Sites, Concerted Research Action, 2010.

[10] Georgios Kontaxis, Iasonas Polakis, Sotiris Ioannidis and Evangelos P. Markatos, Detecting Social Network Pro le Cloning, IEEE, 2011.

[11] Ehsan Ahmadizadeha, Erfan Aghasianb,Hossein Pour Taheric, Roohollah Fallah Ne-jadda, An Automated Model to Detect Fake Pro les and botnets in Online Social Networks Using Steganography Technique, IOSR-JCE, 2015.