A PHOTO PRIVACY FOR TAGGED IMAGES USING RULE – BASED ACCESS CONTROL IN SOCIAL NETWORKS.

Shaik Subhani 1*, M.Rajasekhar 2*

1. *Research scholar, Avr and Svr Engineering College, Kurnool*
2. *Asst Prof, Avr and Svr Engineering College, Kurnool.*

Abstract: *Online social networks provide user relationships and increase information and resource sharing between a large amount of users. Communications by social networks overtake the emails, and it poses enormous security challenges in this platform. Numerous privacy leakages arise while unauthorized users can access information at anywhere and anytime. This paper presents Usage Decision Online Social Network (UDOSN) model to protect private data from illegal access before and during the usage in online social networks. The authentication function controls the access requests before the usage, and right requests are done by the authorization function during the usage. Presented scenarios show the process of both functions. Moreover, Usage Decision Online Social Network model is reusable and environment-independent, and it is defined for social network with formal descriptions.*

1. INTRODUCTION

Nowadays, social network is one of the most important available approaches to communicate over the internet [1]. It was defined as web-based services and a bounded system that includes profiles for each user. An articulated list of friends is specified by profiles. Friends are also users of the system, and they can communicate with each other via comments, private messages and chats [2].

Roughly speaking, user relationships and resource sharing are provided by online social networks (OSN). Attractive features like media sharing and easy messaging rapidly increase the number of social network users, and communication in this platform has overtaken email usage [1].

Unfortunately, most social network users lack awareness of the privacy risks [3]. They often share their data and information with friends, and sometimes naively, with strangers [4]. Consequently, it causes security problems and privacy leakage [5], and many personal data are divulged or sold to third party advertisers. Indeed, access control mechanism of this platform should be different from other systems [6].

Based on policies, social network access control mechanisms are categorized into four groups: user-based, role-based, implementation mechanism-based and mandatory access control. These mechanisms have several problems and drawbacks. First, there are some issues of fine-grained access control guarantees [7]; secondly, specific access has some restrictions [8]; third, social network sites disclose private data of unaware users [7]; fourth, online social networks do not support sessions with user control and policies [9] and session encryption solution does not work with third-party application [1]. The last and critical point is the social network access control system manages resource access and decides which user has permission for the rights at access point. Indeed, right permission has been not considered during the usage.

**** Shaik Subhani***
Research scholar, Avr and Svr Engineering College, Kurnool.

In online social networks, all attributes and polices are individualized for each user, and they can customize attributes and policies. Conversely, Online Social Networks need a decision making system for accessing user's data and shared resources not only before the access but also during the usage. We proposed a flexible usage decision model for online social networks.

This paper is organized as follows: Section 2 presents related works of social network security, while Section 3 introduces a brief overview of usage control. Section 4 describes usage decision models for online social networks, including the authentication and authorization categories. An authentication scenario and an authorization scenario is expressed in Section 5. Finally, Section 6 concludes the paper and outlines our future work.

II. RELATED WORKS

The first recognizable social network site was launched in 1997 and a small-world could be exhibited by networks. There were several sites before that, which has one or two features of social networks, but these features were combined by SixDegreesfor first time in 1997 [2]. SixDegrees for promoted itself, improved digital communications, and afterwards online social networks grew rapidly. Social networks were created in different infrastructures and were developed for various activities.

The rise of social networks created security concerns in this area such as data leakage and divulging private information [10], data sharing and trust [11], information accuracy [12] and vulnerable

social network structure [13]. Some methods have been proposed to dominate these security issues in online social networks. R. Koch[1] considered transparent data encryption methods which support data privacy. Moreover, Baden[14] defined a user's resource access control system based on encryption methods in 2009, although dependency to decryption key made the system vulnerable.

A role-based access control model presented by Carminati [15] was based on trust level and enforces a selective dissemination of information by exploiting cryptographic techniques. Thereafter, a fine-grained access control polices was proposed to provide user requirements and solve some data sharing and trust issues in this area [5]. Lockr [16] provided an access control model to protect privacy for social networks but the model only supported direct friend's relations. A trust based access control model for social network named ACSoNet has been proposed [17]. It had some privacy problems due to revealing the trust level of two nodes.

Recent researches in social network security focus on statistical analysis techniques [18], trust-based access control [19], security level of users and resources in social networks [20], and centralized access control [17]. Existing systems provide limited access control models using specific groups like friends, private and public groups [4]. Therefore, one of the most important issues is the management of complex access control policies. Current works are not able to control the access of dynamic content continuity [6]. This paper presents an overview of usage control and then proposes a usage decision model to protect private data from illegal access before and during usage in online social networks.

III. USAGE CONTROL OVERVIEW

The rapid progress of computer system entails new security requirements in data preserving, and traditional models are unable to control data access completely. Access grant to resources was evaluated by the access control systems at the access point. Right granting was defined by the systems in successful authentication, and did not change during the usage. Usage control emerged in 2002 [21] with the UCON model, and it was extended in 2004 with the addition of ongoing usage [22]. More precisely, usage control generalized access control and became the next generation of access control models [23]. Usage control concept includes traditional access control, privacy management, digital right management, and trust management. Moreover, it represents object rights for these concepts [24].

The relationship between access control and usage control is shown in "Figure 1. ".

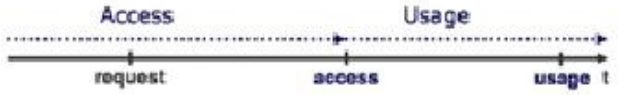

Figure 1. Usage Control Defenition [24]

Usage control has been comprehensively representing three decision factors: authentication, obligation and condition [25]. Resource access permissions are granted to users based on these factors. Usage restrictions and essential action are two aspects of usage control requirements, which are defined by a formal specification language [26]. Control mechanism features which are essential for usage control areas were determined later in 2007 [27].

IV. ONLINE SOCIAL NETWORK USAGE DECISION

This research focuses on authentication and authorization since obligations and conditions are assumed to be the same for all types of social networks.

In this section, a formal usage decision model is discussed for online social networks in usage control systems. Firstly, the elements of the model are introduced. Then, the model is presented based on authentication and authorization categories. The proposed model tests the subject's account attributes before system access, and it also tests subject's account attributes, object rights, object attributes and object owner's account attributes during the usage for the correct permission.

In this model, we use the following elements:

• Subject: Subject is a set of object requesters who are registered in a social network. Each subject member (Sub) holds the rights and executes the action which is granted by the rights. They are defined by their attributes.
Subject == $\{Sub_i \mid i=1\ldots n\}$
Sub ↔ Subject Account
Subject Account =SubAcc where sub ∈ Subject
Subject Account Attribute: Subject Account Attribute is a set of all subject properties (ATT (SubAcc)) such as id, role, name and a set of objects which subject is their creator. Subject account attributes are used during the usage for making decision. The main subject attribute is subject type, and it encompasses creator, owner, friend and public.
Subject Account Attribute == $\{(ATT_j\ (SubAcc)) \mid j=1\ldots n\}$ Where Sub ∈ Subject

• Object: Object is a set of entities or resources that subject can access according to the permitted rights. Each object has a creator. Object == {Obj_j | j=1…n}

• Object Attribute: Object attribute is a set that includes all object properties (ATT (Obj)). They can be used during the usage to decide the correct permission. Object attributes have different types like image, video and personal information. Object Attribute == {ATT_j (Obj) | j=1…n} Where Obj ∈ Object

• Object Right: Object right is a permission that represents the access type of a subject to an object, such as read and write. They are granted according to usage policy and the creator's usage permissions. Subject type defines the permissions, for example, all right are permitted for creators. Object Right == {$ObjR_j${C,P,F,O} | j=1…n} C: Creator, P: Public, F: Friend, O: Owner Where Obj ∈ Object

• Object Owner's Account Attribute: Object owner's account attribute is the same as the subject's account attribute and is shown by ATT (Obj OwnerAcc). Obj Owner ∈ Subject Object Owner's Account Attribute = Subject Account Attribute

• Authentication: Authentication verifies subject identity. Authentication function evaluates the access request of a subject system by testing the subject attributes. It is shown by OSNAe and executes at access points.

• Authorization: Authorization function is shown by OSNAo. It evaluates permissions based on the subject's account attributes, object rights, object attributes and object owner's account attributes. Evaluation is done based on periodic time and event during the usage. Periodic time is defined by the administrator.=T_P 10^{ms} means the evaluation has to be done in every 10 milliseconds.

Event includes any modifications that have direct effect on the evaluation, such as any changes on object attributes, object rights or subject attributes.

In this model, initial policies have to be defined by the administrator, and some of them are listed here.

- Subject can create an object and is named object creator.
- Object creator has all object rights.
- Object creator is an object owner but each owner is not a creator.
- Owner: the subject who has all available object rights (some object rights are specific for the creator,e.g. delete).
- Each subject has at least one object.
- Each object has one creator and at least one owner.
- Creator can assign object rights to other subjects.

A. OSNAe: OSN Authentication Category

OSN Authentication category is performed before the access and it has the following elements: Sub, ATT (SubAcc) and authentication usage decision Boolean function OSNAe. OSNAe predicates authentication function and inspects whether a subject can access the social network or not. It is based on the subject attributes and executes whenever the system receives a subject access request. OSNAe is shown in "Fig. 2".

a) OSNAe (ATT (SubAcc)) Permitted Access (Sub) Where Sub ∈ Subject

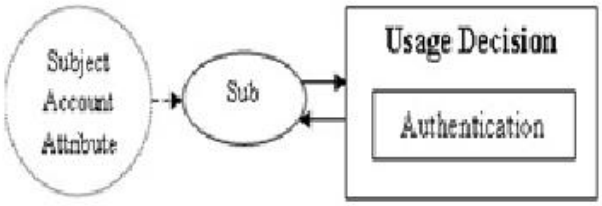

Figure 2. OSNAe Category

Where P => Q means P is a necessary condition for Q. This predicate indicates that if OSNAe is true for subject, then subject can access her or his social network account and access is possible for the subject.

B. OSNAo: OSN Authorization Category

OSN Authorization category is used to check authorizations during the usage. The OSNAo Category has the following elements: Obj, ObjR, ATT(Obj), ATT (Obj OwnerAcc), Sub, ATT (SubAcc) and authorization usage decision Boolean function OSNAo. OSNAo is shown in "Fig. 3".

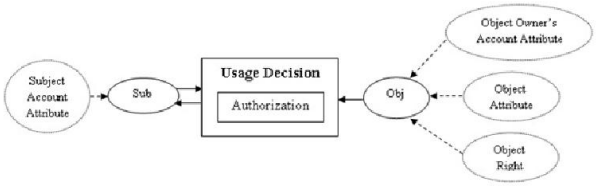

Figure 3. OSNAo Category

a)Permitted Access (Sub) => true This is a prerequisite OSN Authorization for subject.
b)Access Terminated (Sub) => ¬ (OSNAe (ATT (Sub'Acc)))
c)OSNAo (ObjR, ATT (Obj), ATT (Obj OwnerAcc), ATT (SubAcc))=>Permitted Right Request (Obj, ObjR, Sub)
d)Right Request Revoke (Obj, ObjR, Sub) => ¬(OSNAo(ObjR,ATT (Obj), ATT (Obj Owner'Acc), ATT (Sub'Acc)))

OSNAo checks whether the subject can continue accessing the object or not. OSNAo is executed based on periodic time and event.

The data stored in the cloud storages is similar with the ones stored in other places and needs to consider three aspects of

V. SCENARIO

A. System Access Request

User X with initial attributes has been introduced as a member of a social network subject set. The evaluation of access request is shown in "Fig. 4".

X ∈ Subject
ATT(X) = {ID(1), Name(X)}
Step 1- X sends UDOSN a request to login to thesocial network.
Step 2- Authentication process starts and OSNAe (ATT(X)) executes. OSNAe(ATT(X)) considers access permission according to ATT(X), authentication data sent at login time and X as a member of subject set.
Step 3- UDOSN sends X the acceptance of request, i.e. the permission is granted.
Step 4- The login process is successful and X can access his or her own account.

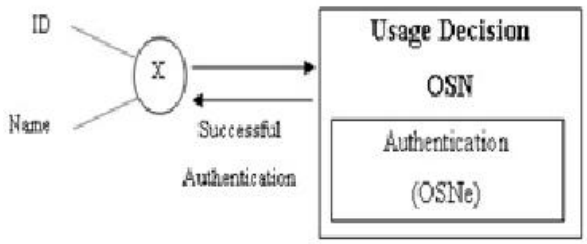

Figure 4.OSNAe Scenario

B. Right Access Request

X and Y are members of social network subject set. X has a request to grant right to an object belonging to Y, objY1. Evaluation of system access request is shown in "Fig. 5".

Subject = {X, Y}
ATT(X) = {ID(1), Name(X), Creator{ObjX1}, Friend{Y}} ATT (ObjX1) = {ID(11), Name(ObjX1)}
ObjRObjX1 = {Read{c,p,f,o}, Write{c,o}, download{c}}

ATT(Y) = { ID(2), Name(Y), Creator{ObjY1}, Friend{X}} ATT (ObjY1) = {ID(21), Name(ObjY1)}
ObjRObjY1 = {Read{c,f,o}, Write{c}}

Step 1- X sends UDOSN a request "permission to read ObjY1"
Step 2- Authorization process starts:
a) Authentication of X is done and Permitted Access (X) is true.

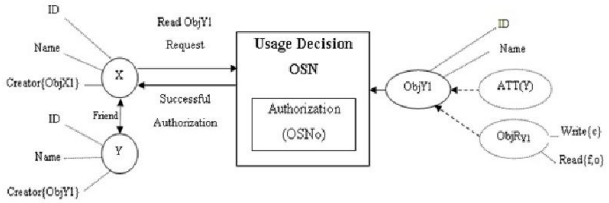

Figure 5. OSNAo Scenario

b) User X is a member of the Subject set. So, OSNAe(ATT(X)) is true and access is continued.
c) OSNAo (ObjRobjY1,ATT(objY1), ATT(Y)) executes based on user X's request. Read is a member of ObjRobjY1 and this right is permitted for friends. Consequently, X as a friend has read permission on ObjY1.

Step 3- UDOSN sends X the acceptance of the request.
Step 4- X has permission of the requested right.

This procedure is repeated periodically, like every 10 milliseconds, and also based on events such as changing any policy, object rights and object existence.

VI. CONCLUSION AND FUTURE WORKS

The main feature of social networks is sharing data between authorized users. According to this feature, this paper has discussed a usage decision model for social networks. By our proposed model, a social network can be equipped with a usage decision model to control access not only at login time but also during usage. We have analyzed decision factors for usage control system in two categories. In the first category, authentication controls access requests before the usage, and right requests are considered by authorization at the second category. Scenarios in Section V showed the process of both functions.

Previous works on social networks have been extended by UDOSN in the ongoing continuity for access control and defined with formal statement. Furthermore, the formal statements can be used in different types of social networks and it makes a reusable model. Moreover, object right is controlled by UDOSN in a dynamic environment and it does not depend on specific environment. Consequently, our significant contribution is proposing a usage decision model which is reusable and environment-inpendent.

The future work includes implementing the proposed model by applying it to a model checker. The model checker provides an option to trace formal statements and find violated properties. Moreover, the outcome of the model checker will demonstrate the theoretical results of this model. Validation of our model can be shown by related real-world case studies.

REFERENCES

[1]R. Koch, D. Holzapfel, and G. Dreo Rodosek, "Data control in social networks," in Network and System security: IEEE, 2011, pp. 274-279.
[2]N. B. Ellison, "Social network sites: Definition, history, and scholarship," Journal of Computer and Mediated Communication, vol. 13, 2007, pp. 210-230.
[3]B. Krishnamurthy and C. E. Wills, "On the leakage of personally identifiable information via online social networks," SIGCOMM Computer Communication Review vol. 40, 2009, pp. 7-12.
[4]J. Li, Y. Tang, C. Mao, H. Lai, and J. Zhu, "Role Based Access Control for social network sites," in Pervasive Computing (JCPC): IEEE, 2009, pp. 389-394.
[5]A. Simpson, "On the need for user-defined fine-grained access control policies for social networking applications," ACM, 2008, p. 1.
[6]B. Carminati, E. Ferrari, R. Heatherly, M. Kantarcioglu, and B. Thuraisingham, "Semantic web-based social network access control," Computers & Security, vol. 30,2011, pp. 108-115.
[7]Q. Chen, J. Liu, and T. Shang, "A ralation declaration- based access control scheme for social networks," Artificial Intelligence, Management Science and Electronic Commerce (AIMSEC), IEEE, 2011, pp. 51-54.
[8]B. Carminati, E. Ferrari, R. Heatherly, M. Kantarcioglu, and B. Thuraisingham, "A semantic web based framework for social network access control," Proc. the 14th ACM symposium on Access control models and technologies, 2009, pp. 177-186.
[9]J. Park, R. Sandhu, and Y. Cheng, "A User-Activity-Centric Framework for Access Control in Online Social Networks," Internet Computing, IEEE, vol. 15, 2011, pp.62-65.
[10]I. Parris and T. Henderson, "Privacy-enhanced social-network routing," Computer Communications, vol. 35,2012, pp. 62-74.
[11]P. Nasirifard and V. Peristeras,"Uncle-share: Annotation-based access control for cooperative and social systems," On the Move to Meaningful Internet Systems: OTM 2008, pp. 1122-1130, 2008.
[12]M. Balduzzi, C. Platzer, T. Holz, E. Kirda, D. Balzarotti, and C. Kruegel, "Abusing social networks for automated user profiling," Proc. in Recent Advances in Intrusion Detection, Springer, 2010, pp. 422-441.
[13]A. Mislove, M. Marcon, K. P. Gummadi, P. Druschel, and B. Bhattacharjee, "Measurement and analysis of online social networks," Proc. the 7th ACM SIGCOMM conference on Internet measurement, 2007, pp. 29-42.
[14] R. Baden, A. Bender, N. Spring, B. Bhattacharjee, andD. Starin, "Persona: an online social network with user-defined privacy," Proc. the ACM SIGCOMM 2009 confon Data communication,. vol. 39: ACM New York, NY,USA., 2009, pp. 135-146.
[15]B. Carminati, E. Ferrari, and A. Perego, "Private relationships in social networks," Proc. Data Engineering Workshop, 23rd International Conference IEEE, 2007, pp. 163-171.