A Contextual Access Control Model for Online Social Network

Khalida Guesmia, Narhimene Boustia
Department of Computer Science
University of Saad Dahleb
Blida, Algeria
{khalida.guesmia@gmail.com nboustia@gmail.com}

Abstract— **The sharing of personal and sensitive data has emerged as a popular activity over online social network. The availability of this information obviously raises privacy and confidentiality issues. The current access control models provided by online social network do not allow users to specify their access control on base of time, location, or under other circumstances. In this paper, we propose an access control model for social networks to express much more fine grained access control policies than the existing models, the OrBAC model is used because it provides a complete model to specify contextual and dynamic access control requirements. We also propose a logic specification of OrBAC with Temporal Logic of Actions.**

Keywords-Online social network; access control; OrBAC; TLA; context.

I. INTRODUCTION

In the last few years, Online Social Network sites (OSNs) have increasingly been used by more and more people around the world which have become integrated into the daily practices of millions of users [1]. OSNs are used to communicate with friends and family, to publish and to share different types of information with other members. Therefore, an unexpected large number of users and massive amount of data which is mainly representing a real life of the users are available in OSNs [2]. As a result, many challenges of scalability, management, and maintenance are posed in OSNs [3]. Cloud Computing paradigm emerges to face these challenges. Most of OSNs shift to Cloud Computing [4] by using different services models (Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS)) to support the huge number of users and their activities in OSNs. In the same time, it raises security and privacy concerns. It is important to review and define what we exactly mean by privacy in this context. Privacy means the right to self-determination regarding data disclosure [5]. Most OSNs provide access control system for users to configure their privacy settings by specifying who may access to their own information. In fact, the available protection settings are based primarily on relationship depth so almost of users expose their contents to more or less users than expected [6], which may lead to serious consequences in some cases [7]. Further, the dynamic developments of OSNs and the variety of data exists in social networks introduce new access control requirements for privacy management, which cannot be able to meet through the available privacy configuration. It is clear that users should be provided with more expressive and flexible mechanisms to protect their information from unwanted disclosure and unauthorized access. Defining access control policies in OSNs is a non-trivial task due to their large number of members and their connections and to the complexity of their environment. Thus, our objective in this paper is to propose appropriate access control model for Facebook that enables users to specify their privacy preferences in an expressive way without overburdening the users or the system [8].

The remainder of this paper is organized as follows: in Section II, we give briefly an overview of the social network Facebook, the most popular OSNs in the world. In Section III, we discuss some related work of access control in OSNs. In Section IV, we outline the main features of Organization Based Access Control model. In Section V, we define the Temporal Logic of Actions that we will be used to specify our proposed security policy for Facebook which be presented in Section VI. In Section VII, we show how to specify various contexts in Facebook using our formalism. In Section VIII, we apply our work to an example in Facebook, and finally, in Section IX, we summarize this paper with future works.

II. THE SOCIAL NETWORK FACEBOOK

Recently, the popularity of Facebook increased significantly. Facebook is a platform for users to interact with each other; according to statistics in December 2013, Facebook is the busiest site on the internet with more than 700 million daily active users around the world and it has built an extensive infrastructure to support this growth. When a user joins Facebook, he/she has to create a profile of himself/herself with biographical data, then sends and accepts invitations to add other users as friends. A user can directly communicate with his/her friends by messaging or poking, he/she can upload different types of information (photo, video, etc.) and share it with others; he/she can also join groups, like fan pages, and organize events [9]. All activities performed by a user are organized chronologically in his/her Timeline through which other users, as well as the user himself/herself, can check his/her past activities conveniently. A user receives his/her friend’s updates on Newsfeed. When he/she finds something interesting, he/she can further perform actions, such as like, share and comment, on it. Facebook has expanded its development scope by adapting PaaS model. It opened up for third party application by releasing its development Application Programming Interface (API) in May 2007 [10]. The third party applications bring value both to the platform and its users by providing new features. So, users can add these applications to their profiles and use them without having to install new hardware or software. These applications are deployed on their own servers and Facebook only acts as a proxy for integrating the application's output to its own pages. The third party applications require user's data to perform its functionality. For example, a simple horoscope application generates daily horoscope based on user's birthday. Furthermore, Facebook is a shared platform, used and managed by different entities (the provider, the third party application and the users). For that, users must carefully control what contents are visible to whom in order to preserve privacy. Therefore, users set their privacy preferences through an audience selector which supports only five modes (public, friends of friends, friends only, specific friends and only me). So, users cannot specify their access control on base of time, location, or under other circumstances. Therefore, the privacy sitting provided by Facebook is not expressive enough, it is limited somehow. In addition, users cannot control what others reveal about them such as tagging users in post, tag is option available in Facebook where users can simply tag other users by associating their profiles with post without their permission [11]. It should be noted that Facebook provider has full access to all user's personal data. Further, Facebook provide no privacy control against third party application. To overcome the limitations and challenges of privacy control in Facebook, the model Organization Based Access Control (OrBAC)[12] is expressive enough to specify access privacy based in various information and it supports in their policy different types of context, so OrBAC model is well suitable for Facebook [13].

III. RELATED WORK

Privacy is an emerging challenge in OSNs that caught much attention recently. There exist different research works that have examined different aspects of the privacy problem. Ajami et al. [7], it is confirmed that users have trouble with existing privacy controls, and they have difficulties to set their preferences. The traditional access controls models are not sufficiently flexible to specify the requirements of privacy management in OSNs [14]. Different access control models and mechanisms are proposed to support users when they set their privacy settings in OSNs. Abdessalem and BenDhia [15], it is proposed a reachability-based access control model that allows users to express their privacy preferences as constraints on existing links with other users. Wang et al. [16], it is developed an automated access control policy specification tool that helps ordinary users to specify who should have access to which part of their data. Oo [17], it is presented a fine-grained OSN access control model based on semantic web technologies in order to automatically construct access control rules for the user's privacy settings with the minimal effort from the user. However, many of these mechanisms provided solution for a certain privacy requirements but missed others. Ahmad and Whitworth [18], it is provided a distributed access control based on decentralised architecture for OSN instead the centralized architecture to avoid the single authority of the provider and that way, users have full control to manage their privacy control. It is good idea but it requires a lot of work. There is also considerable works [19] has been done in the area of access control in the Cloud Computing environment, which is completely challenging research problem and there is no complete solution for it.

IV. ORGANIZATION-BASED ACCESS CONTROL MODEL

The central entity in OrBAC model is the Organization. An organization may be viewed as any entity that has to manage a security policy. In our case study, Facebook itself corresponds to an organization. We can consider also user profile, fan page, group, application and event as organisations. There are always subject, object, action in access control model. In OrBAC model, a subject will be any active entity in a system that accesses objects. In Facebook, subject can be users (Alice, Bob, ...), application, etc. Object is any information or resource which can be accessed. For example, list of friends, photo, fan page, etc. Action is operations that subject are allowed to do on objects. For example, like, share, send message, etc. The idea of OrBAC model is to specify the security policy at the organizational level so instead of modeling the policy by using the concrete and implementation related concepts of subject, object and action, the OrBAC model suggests reasoning with their abstract concepts. The abstract concepts of subject, object and action are respectively role, view and activity. The concept of role in OrBAC is assigned to subjects with similar permissions. For example, in user profile, we can define admin, close friend, family, and colleague as roles.

If org is an organization, and r is a role, then Role_appropriate (org, r) means that role r is defined in organization org.

Role_Appropriate (user_profile, admin)

Role_Appropriate (user profile, colleague)

The concepts of view and activity are in the same way used in OrBAC model to respectively group objects and actions which similar permissions apply to, for example, the objects in user profile can be grouped in the following views: public data, limited data, and private data and for activity, we can define publishing as abstract of actions post, share, comment, and tag in Facebook.

If org is an organization, v is a view, then view_ appropriate (org, v) means that view v is defined in organization org.

View_Appropriate(user_profile, limited_data)

If org is an organization, a is an activity, then Activity_Appropriate (org, a) means that activity a is defined in organization org.

Activity_Appropriate(user_profile, publishing)

In OrBAC, specification of a security rule is not restricted to permissions, but also includes the possibility to specify prohibitions, obligations and recommendations. As we have mentioned before, Security rules in OrBAC model are specified with abstract entities as follows:

If org is an organization, r is a role, v is a view, a is an activity and c is a context then Permission(org, r, v, a, c) (resp. Prohibition(org, r, v, a, c), Obligation(org, r, v, a, c) or Recommendation (org, r, v, a, c)) means that organization org grants role r permission (resp. prohibition, obligation or dispensation) to perform activity a on view v within context c.

For instance, *Permission(Facebook, member, public_data, consulting, Default)*: "Facebook grants member permission to consult public data within the Default context". The Default context represents a condition which is always true.

To activate a given security rule, the subject, the object and the action must separately satisfy some conditions, these conditions are that the subject must be assigned to a given role, the object must be used in a given view and the action implements some given activity. This is represented by the following OrBAC relationships:

If org is an organization, s is a subject and r is a role, then Employ (org, s, r) means that org employs subject s in role r.

Employ (Facebook, Alice, member): "the role member is assigned to the user profile Alice in the Social Network Facebook".

Employ (Alice_Profile, Alice, admin): "Alice is admin in her own profile".

If org is an organization, o is an object and v is a view, then Use(org, o, v) means that org uses object o in view v.

Use (Fashion_Page, Pub.mp4, public_data): "the Page fan Fashion uses the video Pub.mp4 as a public data".

Use(Private_Group, Team.png ,limited_data): "the group Facebook Private uses photo Team.png as a limited data"

If org is an organization, α is an action and a is an activity, then Consider(org, α, a) means that org considers that action α implements the activity a.

Consider(Fcaebook, read, consulting): "in Facebook, we consider read as a consulting"

Consider(Alice_Profile, add_photo, publishing): "in Profile Alice, we consider add photo as a publishing"

Besides these conditions, there are extra conditions that must be satisfied to activate a security rule. These extra conditions may be related to very different notions, such as temporal or spatial requirements. We call context such extra conditions.

If org is an organization, s is a subject, o is an object, α is an action and c is a context, then Define(org, s, o, α, c) means that within organization org, context c is true between subject s, object o and action α. This issue will be detailed in section VII.

For Concrete level, security rules are specified with concrete entities as follows:

If s is a subject, o is an object and α is an action then Is_permitted(s, o, α) (resp. Is_prohibited(s, o, α), Is_obliged(s, o, α) and Is_recommended(s, o, α)) means that subject s is permitted (resp. prohibited, obliged, recommended) to perform action α on object o.

For instance, *Is_permitted(Alice, Pub.mp4, read)*: "Alice is permitted to read video Pub.mp4".

V. Temporal Logic of Actions Overview

Generally, the choice of a formal language for specifying a security policy is based on the capabilities and richness of this language, and on the requirements of the targeted application. The Temporal Logic of Actions (TLA) is a powerful tool to specify systems and their properties, especially for interactive and concurrent systems. TLA combines two logics: a logic of actions and a standard temporal logic [20]. Variables, values, states, functions, predicate and actions are basic concepts in TLA. Values are elements of a data type. A variable has a name like *x* and *y*, and can be assigned a value. A constant is a variable that is assigned a fixed value. A state is characterized by assignment of a value *s[[x]]* to each variable *x*. A function is a nonboolean expression built from variables, operator symbols, and constants, such as $x^2 + y - 3$. The semantics *[[f]]* of a function f is a mapping from states to values. For example, $[[x^2 + y - 3]]$ is the mapping that assigns to the state s the value $s[[x]]^2+s[[y]]-3$, where *s[[x]]* and *s[[y]]* denote the values that *s* assigns to *x* and *y*. Generally, *s[[f]]* ≡ *f(∀ 'v': s[[v]]/v)* where f*(∀'v': s[[v]]/v)* is the value obtained by substituting *s[[v]]* for each variable *v* in the expression. Semantically, a variable is also a function that assigns the value *s[[x]]* to the state *s*. A predicate is a boolean expression built from variables, operator symbols, and constants, such as *x = y+1*. The semantics *[[P]]* of a predicate *P* is a mapping from states to booleans. A state *s* satisfies a predicate *P* iff *s[[P]]*, the value of *[[P]]* in *s*, equals true. An action is a boolean valued expression formed from variables, primed variables, operator symbols, and constants. Formally, an action represents a relation between old states and new states, where unprimed variables refer to the old state and the primed variables refer to the new state. Formally, an action *A* is a function assigning a boolean *s[[A]]t* to a pair of states (*s*, *t*) , where *s* is the old state with unprimed variables, and *t* is the new state with primed variables. For example, *x' = y + 1* has the boolean value of *t[[x]] = s[[y]] + 1*. We say that *(s, t)* is an *A* step if *s[[A]]t* equals true. Generally, *s[[A]]t ≡ A(∀ 'v': s[[v]]/v, t[[v]]/v')*. Since a predicate *P* is a boolean expression built from variables and constants, it is regarded as a special action without primed variables. A pair *(s,t)* is a *P* step iff *s[[P]]* is true. The basic temporal operator is □ (always). The semantics of a temporal action is defined using the concept of behavior. A behavior σ in TLA is an infinite sequence of states $< s_0, s1, s_2, ... >$ (a finite set of states can be regarded as infinite with identical repeating states).

$$< s_0, s_1, s_2, ... > [[A]] \equiv s_0 [[A]] s_1$$

$$< s_0, s_1, s_2, ... > [[\Box A]] \equiv \forall n \geq 0: s_n [[A]] s_{n+1}$$

The same semantics can be defined for predicates since a predicate is a special form of action.

In TLA, a formula is built from predicates and actions with logical connectors and temporal operators.

VI. A SECURITY POLICY FOR ONLINE SOCIAL NETWORK SITE USING ORGANIZATION BASED ACCESS CONTROL MODEL

In this section, we present a logical approach for formalizing OrBAC adopted for Facebook. First we describe the basic components, and then we define the logic model of OrBAC with these components. A system state is a set of assignments of values to variables. In OrBAC, there are eight different kinds of entities, organization, subject, object, action, role, view, activity, and context. Each entity is specified by a finite set of attributes. We require that each entity has at least one attribute for identity, which is unique and cannot be changed. An attribute of an entity is denoted as **ent.att** where **ent** is the entity's identity and **att** is the attribute name. Hereafter, we assume that an entity name without any attribute specified denotes its identity. An attribute is a variable of a specific datatype, which includes a set of possible values, i.e., domain and operators to manipulate them. For example, the domain of attribute "gender" of entity "user profile" is {male, female}. The assignment of a value to an attribute is denoted by ent.att = value. We use *ent.att* to denote an attribute value. The constants correspond to the instances of the entities. A function is an expression built from one or more attributes and constants. For example, Alice_profile.age= Alice_profile .currentDate - Alice_profile.birthday. The variables, the functions, and the constants comprise the basic terms of our logical model. A predicate is a boolean expression built from variables, functions, and constants. A predicate can be defined with a number of attributes from a single entity, or two entities, or the system. In our model, predicate correspond to the relationships of OrBAC presented in Section IV and for the concrete permissions, prohibitions, obligations and recommendations that apply to subjects, objects and actions are represented as follows:

$$
\begin{aligned}
&\forall s\, \forall o\, \forall \alpha\, \forall r\, \forall v\, \forall a\, \forall c\\
&\mathit{Permission}(org, r, v, a, c) \wedge\\
&\mathit{Employ}(org, s, r) \wedge\\
&\mathit{Use}(org, o, v) \wedge\\
&\mathit{Consider}(org, \alpha, a) \wedge\\
&\mathit{Define}(org, s, o, \alpha, c) \rightarrow \mathit{Is\_permitted}(s, o, \alpha).
\end{aligned}
$$

If organization *org*, within the context *c*, grants role *r* permission to perform activity *a* on view *v*, if *org* employs subject *s* in role *r*, if *org* uses object *o* in view *v*, if *org* considers that action *α* implements the activity *a* and if, within *org*, the context *c* is true between *s*, *o* and *α* then *s* has permission to perform *α* on *o*.

VII. SPECIFYING CONTEXT IN ONLINE SOCIAL NETWORK

Different contexts may be expressed within OrBAC model [21]. In order to show the expressiveness of our proposed model, we design several scenarios and give their corresponding formulas in our logic.

The temporal context depends on the time at which the subject is requesting for an access to the system, it should be possible to express that a given action made by a given user on a given object is authorized only at a given time/date, after or before a given time/date, or during a given time interval. To validate a given request for an access, it is necessary to be able to evaluate the current time/date, we suppose each organization have a clock. For example, the admin of group Library create new poll to choose best author for 2013.The pool is open to only members of group until 20/12/2013.

$$
\mathit{Define}(\mathit{Library\_Group}, s, \mathit{Best\_Author\_2013}, \mathit{select}, \mathit{Before\_date\_31/01/2014}) \rightarrow \mathit{Employ}(\mathit{Library\_Group}, s, \mathit{member}) \wedge \mathit{Library\_Group.currentTime} <= 20/12/2013.
$$

The spatial context depends on the subject location. Knowing the location from where the user makes the request can be useful to specify the access control policy. We can distinguish two different types of spatial context. The physical spatial context and the logical spatial context. The first one corresponds to the physical location of the user, namely his or her office, a security area, a specific building, the country, etc. The logical spatial context corresponds to the logical location he or she stands in. For example, it can be the computer, the network or the sub-network, the smartphone, etc. In some cases, physical and logical spatial contexts are highly correlated. The network IP address from which a user is connected probably corresponds to a specific physical place such as a department area. For example, we can specify that the participation in Marathon event is allowed only to users who are connected from the same country where the Marathon will be held.

$$
\mathit{Define}(\mathit{Marathon\_Event}, s, \mathit{Page\_Event}, \mathit{join}, \mathit{connected\_country}) \rightarrow s.\mathit{connected\_country} = \mathit{Marathon\_Event.country}.
$$

The prerequisite context, the permission is granted to a subject, only if some specific conditions are satisfied. For example, Bob want to share his video "How to root Samsung Galaxy S3" with other members who are not necessarily their friends but they search how to root Samsung smartphone.

$$
\mathit{Define}(\mathit{Bob\_Profile}, s, \mathit{How\_to\_root\_Samsung\_Galaxy\_S3.mp4}, \mathit{share}, \mathit{Hashtag\_Video}) \rightarrow s.\mathit{search} \in (\mathit{rootsamsung}, \mathit{rootsmartphone}, \mathit{samsungGalaxyS3}).
$$

The provisional context depends on previous actions the subject has performed in the system. For example, Alice wants to specify that when she adds new friend, this latter is permitted to consult her Timeline from the moment that became her friend.

$$
\mathit{Define}(\mathit{Alice\_Profile}, s, \mathit{Timeline}, \mathit{read}, \mathit{Adding\_New\_Freind}) \rightarrow \mathit{Alice\_Profile.currentTime} >= \mathit{Alice\_Profile.dateBeFreindWith}(s)
$$

VIII. EXAMPLE OF A SECURITY POLICY IN FACEBOOK

In this section, we show how security policy of profile user in Facebook can be expressed and deducing in our formalism. Alice in her profile Facebook defines Mary as close friend, John as member of family, Elena, Mike,Paul as friends and she specifies that her friends who work at the same work place as her, they have colleague as role in her profile. She likes page fan Zinedine Zidane, she joins group Photoshop Club, and she adds Puzzle Game as application. In our formalism, this is represented by the following instances:

- Subjects and Roles

Role_appropriate (Alice_Profile, family)
Role_appropriate (Alice_Profile, close_friend)
Role_appropriate (Alice_Profile, colleague)
Role_appropriate (Alice_Profile, friend)
Employ(Alice_Profile, s, colleague) →
Employ(Alice_Profile, s, friend) ∧
Alice_Profile.workplace=s. workplace.
Employ(Alice_Profile, John, family)
Employ(Alice_Profile,Mary, close_friend)
Employ(Alice_Profile, Elena, friend)
Employ(Alice_Profile, Mike, friend)
Employ(Alice_Profile,Zinedine_Zidane,page)
Employ(Alice_Profile, Photoshop_Club,group)
Employ(Alice_Profile,Puzzle_Game, application)

- Objects and Views

Alice defines the following views and objects in her profile:
View_appropriate(Alice_Profile, limited_data)
View_appropriate(Alice_Profile, private_data)
View_appropriate(Alice_Profile, public_data)
Use(Alice_Profile, List_of_ friends , private_data)
Use(Alice_Profile, Birthday, private_data)
Use(Alice_Profile, Joke , limited_data)
Use(Alice_Profile,Gender, public_data)

- Actions and Activities

Alice defines the following actions and activities in her profile:
Activity_appropriate(Alice_Profile, publishing),
Activity_appropriate(Alice_Profile, adding_friend),
Activity_appropriate(Alice_Profile, consulting),
Consider(Alice_Profile, post,publishing),
Consider(Alice_Profile, send_invitation ,adding_friend),
Consider(Alice_Profile,read, consulting).

- Hierarchies

In OrBAC, organizations, roles, views, activities can be organized hierarchically. *Sub_Role(Profile, family , friend).* The role family inherits the permissions from the role friend.

- Context

Alice wants to share joke with her *colleagues* but only with women.

Define(Alice_Profile, s, Joke, read,
Only_Women_Colleague) → Employ(Alice_Profile, s,
colleague) ∧ s.Gender=Female.

- Security policy

Alice specifies the following permissions:

Permission(Alice_Profile, friend, limited_data, consulting ,
Only_Women_Colleague)
Prohibition (Alice_Profile, friend, public_data, tagging ,
Default): Alice don't want to be tagged in public post.

Elena and Mike work at the same company as Alice and they want to access to joke posted by Alice. On the basis of the specified access policies defined by Alice, the system determines whether access should be granted or denied. First for Elena, we have:

Permission(Alice_Profile, friend, limited_data, consulting ,
Only_Women_Colleague) ∧
Employ(Alice_Profile, Elena, friend) ∧
Alice_Profile.workplace= Elena. workplace ∧
Employ(Alice_Profile, Elena, colleague) ∧
Use(Alice_Profile, Joke , limited_data) ∧
Consider(Alice_Profile, read, consulting) ∧
Elena.Gender=Female ∧
Define(Alice_Profile, Elena, Joke, read,
Only_Women_Colleague) → Is_permitted(Elena, Joke, read).

So Elena is permitted to read Alice's joke.

For Mike, we have:

Permission(Alice_Profile, friend, limited_data, consulting ,
Only_Women_Colleague) ∧
Employ(Alice_Profile, Mike, friend) ∧
Alice_Profile.workplace= Mike. workplace ∧
Employ(Alice_Profile, Mike, colleague) ∧
Use(Alice_Profile, Joke , limited_data) ∧
Consider(Alice_Profile, read, consulting) ∧
Mike.Gender=Female !

The context (Only_Women_Colleague) is not satisfied for Mike so Mike is not permitted to read Alice's joke.

IX. Conclusion and Future Work

In this paper, we have proposed a contextual access control model for users to manage access to their data in Facebook with a flexible and effective way. Using our model, users can specify their privacy sittings based in various information and they can configure access control to users, as well as applications so, it give more control to the users. We have also developed a logic specification of OrBAC for Facebook with Temporal Logic of Actions. We are currently working in developing our solution to perform a user study in order to analyse the decidability and the performance of our model in real case and we will plane to develop configuration interface for users to easily specify their privacy preferences based on our proposed model.

References

[1] M. S. Ezaleila and H. Azizah, "Online social networking: a new virtual playground", International Proceedings of Economics Development & Research, 2011, vol. 5, issue 2, pp. 314-318.

[2] J. Becker and H. Chen, "Measuring privacy risk in online social networks", Web 2.0 Security and Privacy Workshop, 2009.

[3] P. Dudi, "Cloud computing and social networks: a comparison study of myspace and facebook", Journal of Global Research in Computer Science, March 2013, vol. 4, no. 3, pp. 51-54.

[4] B. Yang, W. Tsai, A. Chen, and S. Ramandeep,“ Cloud computing architecture for social computing - a comparison study of Facebook and Google", International Conference on Advances in Social Networks Analysis and Mining, Kaohsiung, 2011, pp. 741–745.

[5] R. Iannella and A. Finden, "A privacy awareness: icons and expression for social networks", in 8th International Workshop for Technical, Economic and Legal Aspects of

Business Models for Virtual Goods Incorporating the 6th International ODRL Workshop, Namur, Belgium, 2010.

[6] Y. Liu , K. P. Gummadi, B. Krishnamurthy, and A. Mislove, “Analyzing facebook privacy settings:user expectations vs. reality”, Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference IMC’11, Berlin, Germany, November 2-4, 2011, pp. 61-70.

[7] R. Ajami, N. Ramadan, N. Mohamed, and J. Al-Jaroodi, “Security challenges and approaches in online social networks: a survey”, International Journal of Computer Science and Network Security IJCSNS, August 2011, vol. 11, no. 8, pp. 1-12.

[8] M. Beye, A. Jeckmans, Z. Erkin, P. Hartel, R. Lagendijk, and Q. Tang, “ Literature overview - privacy in online social networks”. Technical report, Centre for Telematics and Information Technology, 2010.

[9] J. Pang and Y. Zhang, “A new access control scheme for facebook-style social networks”, 2013.

[10] K. Singh , S. Bhola , and W. Lee, “xBook: redesigning privacy control in social networking platforms”, Proceedings of the 18th conference on USENIX security symposium, Montreal, Canada, August 10-14, 2009, pp. 249-266.

[11] M. Madejski, M. Johnson, and S. M. Bellovin. “The failure of online social network privacy settings”. Technical Report CUCS-010-11, Columbia University, Feb. 2011.

[12] A. Abou El Kalam, R. El Baida, P. Balbiani, S. Benferhat, F. Cuppens, Y. Deswarte,A. Miège, C. Saurel, and G. Trouessin. “Organization Based Access Control”. In 8th IEEE International Workshop on Policies for Distributed Systems and Networks (POLICY 2003), Lake Como, Italy, June 2003.

[13] F. Cuppens,N. Cuppens-Boulahia, and E. P. Vina, “Adaptive access control enforcement in social network using aspect weaving”, Proceedings,17th International Conference, DASFAA 2012, International Workshops: FlashDB, ITEMS, SNSM, SIM3, DQDI, Busan, South Korea, April 15-19, 2012, pp. 154-167.

[14] A. Ahmad and B. Whitworth, “Future directions in access control for online social networks”, International Conference on Networks and Information ICNI, Bangkok, Thailand. November 24-25, 2012.

[15] T. Abdessalem and I. BenDhia. “a Reachability-Based Access Control Model for Online Social Networks”. In Proceedings of the First ACM SIGMOD Workshop on Databases and Social Networks, DBSocial' 11, Athens, Greece, June 12-16, 2011, pp. 31-36.

[16] T. Wang , M. Srivatsa , and L. Liu, “Fine-grained access control of personal data”, Proceedings of the 17th ACM symposium on Access Control Models and Technologies, Newark, New Jersey, USA, June 20-22, 2012, pp. 145-156.

[17] S. H. P. Oo, “Intelligent access control policies for social network site”, International Journal of Computer Science & Information Technology (IJCSIT), June 2013, vol. 5, no. 3, pp. 183-190.

[18] A. Ahmad and B. Whitworth, “Distributed access control for social newtorks”, in 7th International Conference on Information Assurance And Security, Malaysia, 2011, pp. 68-73.

[19] J.M.A. Calero, N. Edwards, J. Kirschnick, L. Wilcock, and M. Wray, “Toward a Multi-Tenancy Authorization System for Cloud Services”, Security & Privacy, IEEE, Nov. 2010, vol. 8 , issue 6, pp. 48-55.

[20] X. Zhang , J. Park , F. Parisi-Presicce ,and R. Sandhu, “A logical specification for usage control”, Proceedings of the ninth ACM symposium on Access control models and technologies, Yorktown Heights, New York, USA, June 02-04, 2004, pp. 1-10.

[21] F. Cuppens and N. Cuppens-Boulahia “Modelling Contextual Security Policies”,International Journal of Information Security, 2008, vol. 7, issue 4 , pp. 285-305.