INTELLIGENT ACCESS CONTROL POLICIES FOR SOCIAL NETWORK SITE

Saung Hnin Pwint Oo

Faculty of Information and Communication Technology, University of Technology (Yatanarpon Cyber City), Pyin Oo Lwin, Myanmar
hnin.pwint172004@gmail.com

ABSTRACT

Social networking sites (SNSs) are increasingly becoming a major type of online applications that facilitate online social interactions and information sharing among a large amount of users. Furthermore, privacy protection is an important issue in social networking. Users are not able to easily specify their access control requirements through the available privacy configuration interfaces. An approach assisting online users in composing and managing their access control policies to configure their privacy setting is proposed based on Decision Tree Learning. Moreover, Ontology APIs include social network ontology (SNO) to capture the information semantics in an SNS and an access control ontology (ACO) that is used to store rules from the classifier combining with existing access control rules. Therefore, a fine-gained OSN access control model based on semantic web technologies is proposed in order to automatically construct access control rules for the users' privacy settings with the minimal effort from the user.

KEY WORDS

Access Control, Decision Tree Learning, Ontology, Privacy, Social Networking.

1. INTRODUCTION

Nowadays, people spend an unexpected amount of time on using social networking sites (SNS) and representing themselves as interacting with friends and uploading large amount of personal information on SNS. SNSs are increasingly becoming a major type of online applications that facilitate online social interactions and information sharing among a large number of users [3]. Social networking sites (e.g., Facebook, MySpace, Twitters, etc.) have attracted billions of users and the number of users is still fast increasing. When people join social networking sites, they have to create a profile first of all, and then also make connections to existing friends as well as new friends they meet through the site [18]. Therefore, Online Social Networking Sites (OSNs) are increasing large user growth with more than 350 million of active users. The wide use of SNSs causes a myriad of privacy concerns that arise between SNSs users [15].

Privacy protection is an important issue in social networking [18]. Since users represent them as profile information including private information (e.g., name, birthday, hometown, religion, ethnicity, and personal interest) on OSNs, an appropriate approach to protect on this sensitive information is needed. However, many social networking websites provide interfaces for users to configure their privacy settings. They only provide so-called access control systems by which user is able to decide on his personal information that can be accessed by other members by assigning a given item as public, private, or accessible by their direct contacts [6]. Although some online social networks enforce variants of these settings to provide more flexibility, the principle is the same. For instance, besides the basic settings, Facebook (www.facebook.com) supports

DOI : 10.5121/ijcsit.2013.5315

customizing of privacy setting rules for users of various settings (everyone, friends of friends, friends only, specific individuals). It is important to note that all these OSNs have the advantage of being easy to be implemented, but they lack flexibility. Furthermore, existing solutions are platform specific and they are hard to be implemented for various different online social networks.

Moreover, it is challenging since (1) as many users lack sufficient understanding of privacy policies, asking users to define privacy rules is difficult and (2) it is hard to define rules for the future friends, or the data contents. To address these challenges and limitations, an approach that produces intelligent access control polices and configures privacy system for social networking sites is proposed. The objectives of the approach are (i) to define security policies as rules return by the classifier, (ii) to express much more fine-grained access control policies than the existing models, (iii) to express the policies on the relations among concepts in the social network ontology, (iv) to encode social network-related information by means of an ontology, (iv) to automatically construct access control rules for the user's privacy settings with minimal effort from the user, and (v) to get a privacy configuration mechanism to allow online users not only to easily specify their access control requirements but also to control their resources from unwanted person and to avoid attacks. Therefore, a fine-grained Online Social Networks (ONS) access control model based on semantic web technologies is proposed.

The paper is organized as follows. Section 2 is the related work. Section 3 describes implementation of the system. Section 4 concludes the paper.

2. RELATED WORK

The development of usable tools for protecting personal data in social media is an emerging problem that caught much attention recently [8, 1, 2, 7, 10, 11 and 14]. In 2006, Kruk et al. proposed the D-FOAF system [11], a Friend of a Friend (FOAF) ontology-based distributed identity management system for social networks, where access rights and trust delegation management are provided. In 2006, Choi et al. proposed another D-FOAF-related paper [8] in which they denote authorized users in terms of the minimum trust level and maximum length of the paths between the requester and the resource owner. Ali et al. proposed a social access control (SAC) strategy based on multi-level security model [4]. They adopt a multi-level security approach, where trust is the only parameter used to determine the security level of both users and resources [4]. In 2009, Carminati et al. proposed a discretionary access control model for online social networks [5]. The model allows the specification of access rules for online resources, where authorized users are denoted in terms of the relationship type, depth, and trust level existing between nodes in the network. Carminati et al. designed an access control system that uses semantic web technologies to represent much richer forms of relationships among users, resources and actions [6]. For example, by using OWL reasoning tools, a “very close” friend will be inferred as a “friend”; thus anything that is accessible by friends could be also accessible by a “close friend. In 2010, Masoumzadeh et al. proposed an access control ontology to capture the information semantics in asocial network site. The access control policies are defined as rules and enforced based on the access control ontology [3]. In the work by Fang et al. [12], they proposed a tool that can infer the model of users' privacy preference by using machine learning techniques on users' specified input of some of their privacy preference. The preference model will then be used to configure the user's privacy settings automatically. In 2011, Qingrui et al. proposed the semantics-enhanced privacy recommendation for social network sites [18] inferring user's privacy preference models. In addition, the work considered rich semantics in users’ profiles, and integrate the semantics into model inference. The work assumes the user-specified access control rules are not sufficient to address users' privacy requirements, thus they consider to infer hidden rules and perform automatic predictions based on users' access control history.

The works related to the proposed system are [18] and [12]. According to these work, users need to be trained in order to have a better understanding the privacy protection. However, it is difficult to predict how many a particular user will provide the amount of input and more user efforts are needed to implement better privacy settings. This work shares the same goal of inferring user's privacy preference models. The differences between the proposed system and the above systems are taken into account. First of all, instead of asking the user to decide for each of her friends who to give access or not, the proposed approach provides options (e.g., by age) to the user for setting access rights on his friends. From the minimal effort of user, the classifier decides on the access control policy settings for his friends. Secondly, ontology APIs are considered which include social network ontology (SNO) to capture the information semantics in an SNS and an access control ontology (ACO) that is used to store rules from the classifier combining with existing access control rules. Finally, the system can automatically construct access control rules for the user's privacy settings combining with existing privacy setting history.

3. DESIGN

The section is divided into five subsections, namely: the proposed system, how to extract features, system design how to predict user to get access photo and finally the advantages of the approach.

3.1. The proposed system

The system is intended to express and enforce access control policies for social network sites based on semantic web technologies (e.g. OWL). Moreover, the system is able to express much more fine-gained access control policies on social network knowledge based than the existing models. The main objective of the system can automatically construct access control rules for the user's privacy settings combining with existing privacy setting history by using a Decision Tree Classification method on users' profile.

3.1.1. The preliminaries

Firstly, some preliminaries of the system are introduced before the detail of the system is represented. They are:

1. User profiles - Every online user has a user profile which is a list of identifying information such as name, birthday, hometown, etc.
2. Data items - Data items in social networks can be of various types; including user profile information (e.g., age and gender), photo images, blog entries and so on.
3. Privacy settings - A user’s privacy setting represents his/her requirement to share data items with each of his/her friends. Assume a particular user has friend set F, and let I denote her data items. The users privacy settings can be expressed as a $|F|\times|I|$ matrix, where each entry is valued “permit” or “deny”, corresponding to the setting as allowing and denying the access. Table 1 shows an example of user De De privacy settings.
4. Ontology APIs - That include two knowledge bases;
   i. Social network ontology (SNO) is to capture the information semantics in an SNS.
   ii. An access control ontology (ACO) is used to model and store any knowledge solely needed for access control purpose including inferences based on access control policy rules.
5. Access control rules - The proposed access control rules are shown in following subsection.

Table 1. An example of privacy setting.

Friends	Data Items			
	Date of Birth	**Diving Video**	**Blog Entry**	…
Aye Aye	Permit	Deny	Deny	…
Bo Bo	Deny	Permit	Deny	…

3.1.2. Proposed access control rules

Studies have found that users have a difficult time completing basic access control management tasks, including determining who has access to which resources, and making changes to an existing policy [19, 20 and 13]. Therefore, some of access control rules are proposed to use in the system so as to configure users' privacy settings. The following access control rules are considered.

1. When Bo Bo invites Aye Aye to add as a friend but Aye Aye cannot read Bo Bo's profile, community structure will be extracted to check whether a subset of Bo Bo's friends is from Aye Aye's friends or not. If so, Aye Aye will accept Bo Bo as a friend. Otherwise Aye Aye will deny Bo Bo's invitation.
2. Based on relationship, specific data items can be controlled for specific groups. When Bo Bo wants to show his age for only his family and closed friends, friends' profile information has to be extracted.
3. In sharing information with each other, individuals can automatically remove unwanted sharing from an untrusted person. Both community structure and friends' profile information are required for this rule.
4. Bo Bo wants to show a photo based on the age of their friends like showing this photo to subset of his friends with between age of 20 and age of 28 by friends' profile information.
5. If Bo Bo requested Aye Aye for a access to use/share her resource, Aye Aye could decide on his request based on community structure, common friends and group in which Bo Bo exist whether she couldn't know Bo Bo's private information or not.

3.2. How to extract features

In order to build a better classifier which can accurately classify a user's unlabeled friends and to predict future friends, the better set of features is necessary to be selected. For this purpose, the following two main types of features are considered.

1. Community Structure: Community structure takes place a crucial role for understanding the relationships between participants in social network [17]. For example, extracted community structure is shown in figure1. The community structure between participants is used to be an effective feature for classifying social connections in SNS. The hierarchical community discovery approach [12] which is based on the edge between algorithm [16] is used to extract communities.
2. Friends' profile information: Other friends' profile features such as age, gender, location, etc. are collected because they may be related to hidden rules of a user's privacy setting shown in table 2. For example a user wants to show a photo based on the age of his/her friends like showing this photo to subset of his friends with between age of 20 and age of 28.

Table 2. An example of friends list with extracted features and class labels for item "Show Photo" of a user.

Friends	Features					Class Label
	Community	Age	Gender	Location	…	(Show Photo)
Aye Aye	C01	20	F	Yangon	…	Permit
Bo Bo	C201	23	M	Mandalay	…	Permit
Chit Chit	C1	30	F	Saging	…	Deny
De De	C21	50	M	Mdy	…	?

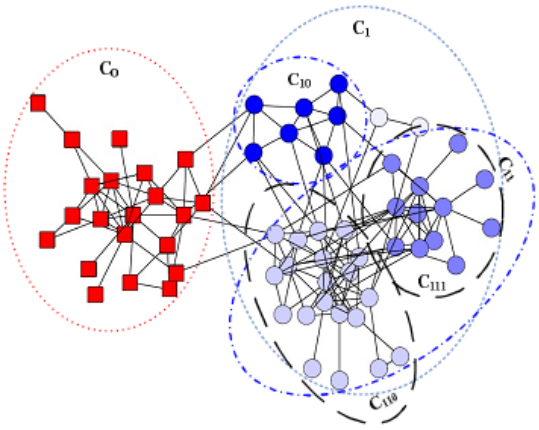

Figure1. Example of extracted hierarchical community structure of user's friend neighborhood.

3.3. System design

The community structures are fundamentally important for understanding the social relationships between social network participants. The community feature is extracted by employing the implementation of iGraph library [21] based on edge betweeness algorithm. The example of extracted community structure is shown in figure1. Extracted features are classified by Decision tree Classifier because (i) decision tree can easily be converted into rules which is stored in ACO ontology combining with existing access control rules and (ii) the resulting search of decision tree classifier is much less sensitive to error in training examples. Thereafter, rules from the classifier and from existing access control rules are produced and stored Knowledge base ACO. So, user has access control on his data items while sharing them with his friends. The user request processor accepts the requests from a user, and passes it to the query modifier module. The query that has been modified is then sent to the SPARQL engine. The SPARQL engine then interacts with the SNO and ACO to retrieve the query results. The system extracts rules from the knowledge based. Finally, the authorized query results to determine which friends can get access to a given item are returned to the user request processor. The design of the system is represented in figure 2.

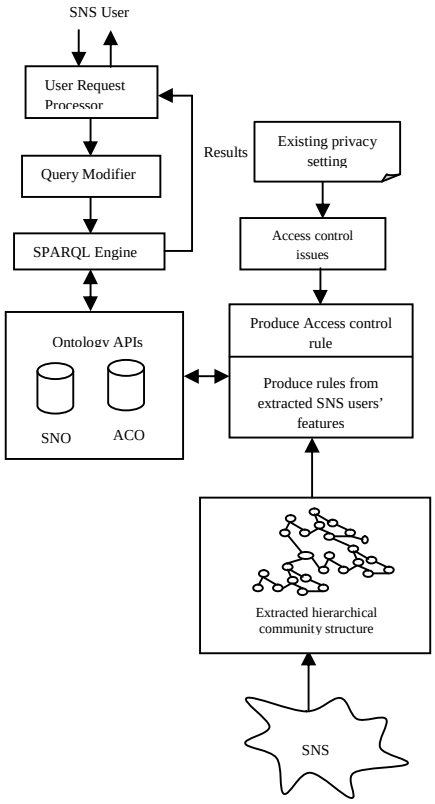

Figure2. System Overflow

3.4. How to predict to get access photo

Table 3. Prediction users to access photo.

Friends	**Features**				**Class Label (Acces Photo)**
	Community	**Age**	**Gender**	**Location**	
Sandar Win	C01	25	F	Singapore	Permit
Khant Zaw Htet	C11	26	M	Pyin Oo Lwin	Deny
Mya Pwint Cho	C11	26	F	Pyin Oo Lwin	Permit
Swe Swe Yee	C01	25	M	Mandalay	Permit
Sar Kuyar	C02	32	F	Mandalay	Permit
Kyaw Zin Oo	C01	25	M	Mandalay	Permit
Khine Swe Win	C12	29	F	Pyin Oo Lwin	Deny
Khin Win	C12	26	F	Pyin Oo Lwin	Permit
May Su Mon	C21	26	F	Singapore	Deny
Tun Aung Kyaw	C21	26	M	Singapore	Deny
Pyay Khaing	C2	26	M	Singapore	Deny
San Min	C2	25	M	Australia	Deny
Areal Thu	C01	26	F	Mandalay	?
Zin Aung Lin	C11	26	M	Mandalay	?
Daw Tin Lay	C02	54	F	Mandalay	?

By using a Decision Learning Classifier, the system can automatically extract users' features and label them shown in table 3 for access control rule (5). Thereafter, results from the classifier which is shown in figure3 can be stored in access control ontology combining with the existing access control rules. New user can be predicted based on rules from the ontology. Therefore, the system can automatically construct access control rules for the user's privacy settings. Finally, the performance of the system tends to be compared with existing systems and to be calculated by the accuracy of the system. Therefore, the system may be a privacy configuration mechanism to allow online users not only to easily specify their access control requirements but also to control their resources from unwanted person and to avoid attacks.

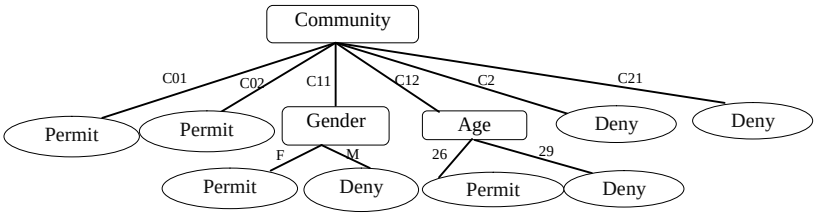

Figure3. Decision tree for table 3.

The rules generated by the decision tree classifier are:

1. IF Community = "C01" THEN AccessPhoto = "Permit" OR
2. IF Community = "C11" AND Gender = "M" THEN AccessPhoto = "Deny" OR
3. IF Community ="C12" AND Age ="26" THEN AccessPhoto = "Permit" OR ….

According to the rules generated by the decision tree classifier, Aeral Thu and Daw Tin Lay can access the photo but Zin Aung Lin cannot access it.

3.5. The advantages of the approach

Since predicting the amount of input from a user being willing to provide is difficult, the approach provides some forms of indicating who will be able to get access right to his/her resources for example photo, profiles and so on, according to the access control rules represented in procedure 3.1.2. Instead of asking the user to decide for each of his/her friends who to give access or not, the proposed approach provides options (e.g.,by age) to the user for setting access rights on his friends. By semantically capturing the social information stored in SNO ontology such as that "Mandalay" and "Mdy" has a same meaning in location and combining with ACO ontology that stores the results from the classifier as rules, the approach can correctly predict setting for access right on a user's friends. Therefore, the approach is able to understand human expression through language and automatically construct access control rules for the user's privacy settings at the end.

4. CONCLUSION

Privacy is an important emerging problem in online social network sites. While these sites are growing rapidly in popularity, existing policy configuration tools are difficult for average users to understand and use. In order to have a better understanding the privacy protection, users need to be trained. It is difficult to predict how many a particular user will provide the amount of input and more user efforts are needed to implement better privacy settings. In the system using a Decision Tree Classification method, it can automatically extract users' features and label them. Results from the classifier can be stored in ACO ontology combining with the existing access control rules. New user can be predicted based on rules from the ontology. The system can automatically construct access control rules for the user's privacy settings. The system may be a privacy configuration mechanism to allow online users not only to easily specify their access

control requirements but also to control their resources from unwanted person and to avoid attacks.

ACKNOWLEDGEMENTS

I would like to show my appreciation and thanks to my supervisor Dr. Zar Zar Wint, Associate Professor, Faculty of Information and Communication Technology, University of Technology (Yatanarpon Cyber City), Mandalay, Myanmar, for her invaluable recommendations, patient supervision, encouragement and guidance during the period of this thesis.

REFERENCES

[1] A. Acquisti and R. Gross, "Imagined communities: Awareness, information sharing and privacy on the facebook," in the 6th Workshop on Privacy Enhancing Technologies, 2006.

[2] A. Carreras, E. Rodriguez, and J. Delgado, "Using xacml for access control in social networks," in W3C workshop on access control application scenarios, 2009.

[3] A. Masoumzadeh and J. Joshi, "Osnac: An ontology-based access control model for social networking systems," in IEEE Second International Conference on Social Computing, 2010, pp. 751 – 759.

[4] Ali B, Villegas W, Maheswaran M. A trust based approach for protecting user data in social networks. In: Lyons KA, Couturier C, editors. CASCON. IBM; 2007. p. 288e93.

[5] B. Carminati, E. Ferrari, and A. Perego, "Enforcing access control in web-based social networks," ACM Trans. Inf. Syst. Secur., vol. 13, pp. 6:1–6:38, November 2009.

[6] Barbara Carminati, Elena Ferrari, Raymond Heatherly*, Murat Kantarcioglu, Bhavani Thuraisinghamb, "Semantic web-based social network access control".

[7] C. Gates, "Access control requirements for web 2.0 security and privacy," in Web 2.0 Security and Privacy Workshop, 2007.

[8] Choi HC, Kruk SR, Grzonkowski S, Stankiewicz K, Davids B, Breslin JG. "Trust models for community-aware identity management"; 2006. IRW2006/WWW2006 Workshop.

[9] J. Chen, O. R. Zaiane, and R. Goebel, "Detecting communities in social networks using max-min modularity," SDM, 2009.

[10] K. Gollu, S. Saroiu, and A.Wolman, "A social networking-based access control scheme for personal content," in The 21st ACM Symposium on Operating Systems Principles (SOSP), 2007.

[11] Kruk SR, Grzonkowski S, Gzella A, Woroniecki T, Choi HC. D-FOAF: distributed identity management with access rights delegation. In: Mizoguchi R, Shi Z, Giunchiglia F, editors. ASWC. Lecture notes in Computer Science, vol. 4185.Springer;2006.p.140e54.

[12] L. Fang and K. LeFevre, "Privacy wizards for social networking sites," in Proc. of the 19th international conference on World wide web, 2010.

[13] Lipford, H. R., Besmer, A., and Watson, J. Understanding privacy settings in Facebook with an audience view. In UPSEC'08: Proceedings of the 1st Conference on Usability, Psychology, and Security (Berkeley, CA, USA, 2008), pp. 1-8.

[14] M. Hart, R. Johnson, and A. Stent, "More content – less control: Access control in the web 2.0," In Web 2.0 Security and Privacy , 2007.

[15] M. Madejski, M. Johnson, and S. M. Bellovin. A study of privacy settings errors in an online social network. In Proceedings of the 4th IEEE International Workshop on Security and Social Networking, SESOC '12, 2012.

[16] M. Newman and M. Girvan. Finding and evaluating community structure in networks. Physical Review, 69(2), 2004.

[17] M. Newman. Modularity and community structure in networks. ProcNatl Acad Sci USA, 103:8577–82, 2006.

[18] Qingrui Li1, Juan Li1, Hui (Wendy) Wang2, Ashok Ginjala1,"Semantic-enhanced privacy recommendation for social networking sites".

[19] Reeder, R. W., and Maxion, R. A. User interface dependability through goal-error prevention. International Conference on Dependable Systems and Networks (2005), 60-69.

[20] Reeder, R. W., Kelley, P. G., McDonald, A. M., and Cranor, L. F. A user study of the expandable grid applied to P3P privacy policy visualization. In WPES '08: Proceedings of the 7th ACM Workshop on Privacy in the Electronic Society (New York, NY, USA, 2008), ACM, pp. 45-54.

[21] The igraph software package for complex network research. InterJournal Complex System, 2006.