

# Introducing Multiparty Authorization And String Search In A Parental Controlled Social Network

Anu P Salim

Dept. of Computer Science & Engg.  
Sree Buddha College of Engg.  
Alappuzha, Kerala, INDIA

Reeba R

Dept. of Computer Science & Engg.  
Sree Buddha College of Engg.  
Alappuzha, Kerala, INDIA

**Abstract**—Online social networks or simply social networks is one the important emerging service provided in the Internet. It is very popular and powerful tools for making and finding friends and for identifying other people who share similar interests. This paper introduce a new Online Social Network with two new techniques, one is for improving the performance of information collection using string transformation and enable the protection of shared data associated with multiple users in OSN. A parental control is also provided to control the activities of kids in social network.

**Keywords**—Social Networks, Multiparty Authorization, Social Search, String Transformation, Parental Control.

## I. INTRODUCTION

Online social networks (OSNs) have become a new networking platform for connecting people through a variety of mutual relationships. Social Network Services (SNS) such as Facebook, Friendster, MySpace and Orkut have established themselves as very popular and powerful tools for making and finding friends and for identifying other people who share similar interests. The dynamics and evolution of social networks are very interesting but at the same time very challenging area. In this paper the formation and growth of one of such structure.

A typical OSN provides each user with a virtual space containing profile information, a list of the user's friends, and web pages, such as Timeline in Facebook, where users and friends can post contents and leave messages. A user profile usually includes information with respect to the user's personal information. In addition, users can not only upload a content into their own or others' spaces but also tag other users who appear in the content. Each tag is an explicit reference that links to a user's space. For the protection of user data, current OSNs indirectly require users to be system and policy administrators for regulating their data, where users can restrict data sharing to a specific set of trusted users. OSNs often use user relationship and group membership to distinguish between trusted and untrusted users. Although OSNs currently provide simple access control mechanisms allowing users to govern access to information contained in their own spaces, users, unfortunately, have no control over data residing outside their spaces. To address such an issue, preliminary protection mechanisms have been offered by existing OSNs.

Search behavior of Web users often reflects that of others who have similar interests or similar information profiles in social networks. Social search or a social search engine is a type of search method that tries to determine the relevance of search results by considering interactions or contributions of users. The premise is that by collecting and analyzing information from a user's explicit or implicit social network improve the accuracy of search results. The most common social search scenario is a user in the social networking site submits a query to the search engine associated with it. Then the search engine computes ordered list of the most relevant results using a ranking algorithm. The search engine collects information that lies in the neighborhood of user and relates to the results in list. It utilize this information to reorder the list to a new list and which is presented to user. Using of string transformation for searching is a new technique in social search. String transformation is about generating one string from another string, such as "OSN" from "Online Social Network".

In this paper introducing a new OSN with multiparty authorization framework (MAF) to model and realize multiparty access control for an effective and flexible access control mechanism, accommodating the special authorization requirements coming from multiple associated users for collaboratively managing the shared data and provide string transformation for searching in OSN.

Kids can also use this OSN because a parental control is provided for them. The challenge is to help children enjoy the benefits of going online while avoiding the risks. For solving this issue we put forward a browser which helps in avoiding the inappropriate contents reaching children and to inform parents about the surfing content of children. The parent and child should be registered in the browser in order to access the features. When accessing the social networking site, the child will be under verification. The search keywords entered by the children and the search contents will be mailed to the parent email id provided while during registration. The mail consists of the time and date of accessing, the screenshot of the accessed or searched contents and keywords provided while during search. Thus it helps parents to continuously verify the internet contents browsed by the child. It also helps parent to funnel children towards child-friendly options and remove the chance of accidental exposure to inappropriate content.

The social network structure can be modeled as a graph  $G$  with individuals representing nodes and relationships among them representing edges.

## II. RELATED WORKS

### A. Access Control in OSN

Access control for OSNs is still a relatively new research area. Several access control models for OSNs have been introduced. Early access control solutions for OSNs introduced trust-based access control inspired by the developments of trust and reputation computation in OSNs. The D-FOAF system [16] is primarily a Friend of a Friend (FOAF) ontology-based distributed identity management system for OSNs, where relationships are associated with a trust level, which indicates the level of friendship between the users participating in a given relationship. Carminati et al. [15] introduced a conceptually-similar but more comprehensive trust-based access control model. This 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 between users in OSNs. They further presented a semi-decentralized discretionary access control model and a related enforcement mechanism for controlled sharing of information in OSNs [7]. Fong et al. [14] proposed an access control model that formalizes and generalizes the access control mechanism implemented in Facebook, admitting arbitrary policy vocabularies that are based on theoretical graph properties. Gates [8] described relationship-based access control as one of new security paradigms that addresses unique requirements of Web 2.0. Then, Fong [13] recently formulated this paradigm called a Relationship-Based Access Control (ReBAC) model that bases authorization decisions on the relationships between the resource owner and the resource accessor in an OSN. However, none of these existing work could model and analyze access control requirements with respect to collaborative authorization management of shared data in OSNs.

### B. Social Search Technique

There are many social search techniques. Most of the searching is based on the relationship between the nodes in the graph. The retrieved information is ranked on the basis of relationship between the nodes. If the nodes are strong then the result is ranked as one. This paper propose a social search based on the string transformation and the relationship. Some of the existing techniques are described in the following section.

- Search Based on Relationship

This is the common technique for the social search. The concept of “strong link” [1] is introduced. If two nodes are communicated regularly then a strong link is formed between them. Similarities between articles and keywords are measured and rank the search result based on it. It also combine keyword density and

social relations as a value which is called social ranking value.

- Hybrid Social Search

Hybrid social search model, which harnesses the user’s social relation to generate the satisfying results [2]. Upon receiving a user’s query, the search engine aims to return a list of ranked answers who might give the correct answer to that query. Topic Relevance Rank (TRR) algorithm is used to evaluates user’s professional score on the relevant topics. Social Relation Rank (SRR) algorithm is used to capture the social strength between users.

- SMART Finder

Social search behavior of a user often reflects that of who have similar interest or similar information profiles in the network. Therefore if we locate users interested in certain topics or areas and then keep track of their preference in terms of search result. SMART Finder [3] is an efficient search to pinpoint relevant and reliable information about these people. The search results for locating people whose social relationships are highly ranked according to specific topics. It can also identify people who are highly associated with each other with regard to search topic.

- Agent-Based Mining

Developed an agent-based framework that mines the social network of a user to improve search result [4]. Agent in the system utilize the connections of a user in the social network to facilitate the search for items of interest. Agent observes the user activity such as rating and comments and agents retrieve such users those who are comment, tagged by user to the searcher.

- Search Based on Framework

The HTML framework or template is extracted from the social networks [5] and this information is used for searching. Similarity between the frameworks of users is the key for searching. Such type of users has some relations so it is used for ranking.

### C. Parental Control

The recent software for parental control are Qustodio and Avira. Qustodio is parental control designed for today’s busy, web-savvy parents. No hardware, no complicated setup—just a simple, web-based dashboard that gives the information. Whether your kids use the family computer, personal laptop, tablet, or mobile phone, Qustodio is there to set limits, block questionable sites, and keep kids safe. The parents get the details only if it is installed. Avira is social network protection. In it the parent register in the site and get kid’s browsing details in a mail.

## III. SOCIAL NETWORK STRUCTURE

The social network structure can be modeled as a graph  $G$  with individuals representing nodes and relationships among them representing edges. The label associated with each edge indicates the type of the relationship. Edge

direction denotes that the initial node of an edge establishes the relationship and the terminal node of the edge accepts the relationship. The number and type of supported relationships rely on the specific OSNs and its purposes.

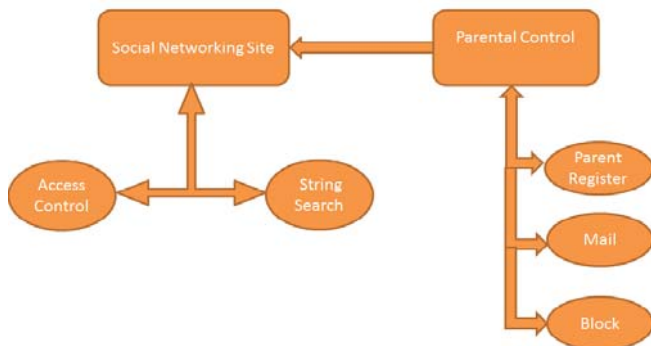


Fig .1. Social Network Design

### A. Multiparty Authorization

To enable a collaborative authorization management of data sharing in OSNs, it is essential for multiparty access control policies to be in place to regulate access over shared data, representing authorization requirements from multiple associated users. A flexible access control mechanism in a multi-user environment like OSNs is necessary to allow multiple controllers associated with the shared data item to specify access control policies. For a specific data there is an owner and controllers including the contributor, stakeholder and disseminator of data, also desire to regulate access to the shared data. Define these controllers as follows:

- **Owner:** In Owner module let  $d$  be a data item in the space  $m$  of a user  $u$  in the social network. The user  $u$  is called the owner of  $d$ . The user  $u$  is called the contributor of  $d$ . We specifically analyze three scenarios—profile sharing, relationship sharing and content sharing—to understand the risks posted by the lack of collaborative control in OSNs. In this the owner and the disseminator can specify access control policies to restrict the sharing of profile attributes. Thus, it enables the owner to discover potential malicious activities in collaborative control. The detection of collusion behaviors in collaborative systems has been addressed by the recent work.
- **Contributor:** In Contributor module let  $d$  be a data item published by a user  $u$  in someone else's space in the social network. The contributor publishes content to other's space and the content may also have multiple stakeholders (e.g., tagged users). The memory space for the user will be allotted according to user request for content sharing. A shared content is published by a contributor.
- **Stakeholder:** In Stakeholder module let  $d$  be a data item in the space of a user in the social network. Let  $T$  be the set of tagged users associated with  $d$ . A user  $u$  is called a stakeholder of  $d$ , if  $u \in T$  who has a relationship with another user called stakeholder, shares the relationship with an accessor. In this scenario, authorization requirements from both the

owner and the stakeholder should be considered. Otherwise, the stakeholder's privacy concern may be violated. A shared content has multiple stakeholders.

- **Disseminator:** In Disseminator module let  $d$  be a data item shared by a user  $u$  from someone else's space to his/her space in the social network. The user  $u$  is called a disseminator of  $d$ . A content sharing pattern where the sharing starts with an originator (owner or contributor who uploads the content) publishing the content, and then a disseminator views and shares the content. All access control policies defined by associated users should be enforced to regulate access of the content in disseminator's space. For a more complicated case, the disseminated content may be further re-disseminated by disseminator's friends, where effective access control mechanisms should be applied in each procedure to regulate sharing behaviors. Especially, regardless of how many steps the content has been re-disseminated, the original access control policies should be always enforced to protect further dissemination of the content.
- **MPAC Module:** MPAC is used to prove if our proposed access control model is valid. To enable a collaborative authorization management of data sharing in OSNs, it is essential for multiparty access control policies to be in place to regulate access over shared data, representing authorization requirements from multiple associated users. Our policy specification scheme is built upon the proposed MPAC model. **Accessor Specification:** Accessors are a set of users who are granted to access the shared data. Accessors can be represented with a set of user names, asset of relationship names or a set of group names in OSNs.

### B. String Search

There are two possible settings for string transformation. One is to generate strings within a dictionary, and the other is to do so without a dictionary. In the former, string transformation becomes approximate string search, which is the problem of identifying strings in a given dictionary that are similar to an input string. In approximate string search, it is usually assumed that the model (similarity or distance) is fixed and the objective is to efficiently find all the strings in the dictionary. Most existing methods attempt to find all the candidates within a fixed range and employ  $n$ -gram based algorithms or trie based algorithm. There are also methods for finding the top  $k$  candidates by using  $n$ -grams. Efficiency is the major focus for these methods and the similarity functions in them are predefined.

### C. Parental Control

The parent needs to register in this site along with the child details. The parent needs to specify the parent username and password along with the child username and password. Using this browser the child needs to login and can access the social networking site. The search keywords provided by the child will be monitored by the browser. The search keywords provided by the child and the search

content screenshot will be mailed to the parent mail id provided during registration. Thus it helps parent to funnel children towards child-friendly options and remove the chance of accidental exposure to inappropriate content.

#### IV. CONCLUSION

The concepts introduced in this paper such as multiparty authorization, string search and parental control improves the efficiency of a social network. Multiparty authorization provide a better security. String search is a new concept in social network. It improves the searching effect. The surfed content of a kid can be verify by a parent using the parental control in the online social network.

#### REFERENCES

- [1] Hsiao-Hsuan Lu, I-Hsien Ting and Shyue-Liang Wang, "A Novel Search Engine Based on Social Relationships in Online Social Networking Website", *Advances in Social Networks Analysis and Mining (ASONAM)*, 2012 IEEE/ACM International Conference, 2012.
- [2] Guo, Liang , Que, Xirong ,Cui, Yidong , Wang, Wendong , Cheng and Shiduan, "A hybrid social search model based on the user's online social networks", *Cloud Computing and Intelligent Systems (CCIS)*, 2012 IEEE 2nd International Conference, 10.1109/CCIS.2012.6664235, 2012.
- [3] Park, GunWoo ; Lee, SooJin ; Lee, SangHoon, "To Enhance Web Search Based on Topic Sensitive\_Social Relationship Ranking Algorithm in Social Networks", *Web Intelligence and Intelligent Agent Technologies*, 2009. WI-IAT '09. IEEE/WIC/ACM International Joint Conference, 10.1109/WI-IAT.2009.322, 2009.
- [4] Anil Gursel and Sandip Sen, "Improving Search In Social Networks by Agent Based Mining\*", 2008.
- [5] Shen Yang ; Liu Zi-tao ; Luo Cheng ; Li Ye, "Research on Social Network Based on Meta-search Engine", *Web Information Systems and Applications Conference*, 2009. WISA 2009.
- [6] Wang, Z. ; Xu, G. ; Li, H. ; Zhang, M. , "A Probabilistic Approach to String Transformation", *Knowledge and Data Engineering, IEEE Transactions*, 2013.
- [7] Carminati, B., Ferrari, E., Perego, A.: Enforcing access control in web-based social networks. *ACM Transactions on Information and System Security (TISSEC)* 13(1), 1–38 (2009)
- [8] Carrie, E.: Access Control Requirements for Web 2.0 Security and Privacy. In: *Proc. of Workshop on Web 2.0 Security & Privacy (W2SP)*, Citeseer (2007)
- [9] Choi, J., De Neve, W., Plataniotis, K., Ro, Y., Lee, S., Sohn, H., Yoo, H., Neve, W., Kim, C., Ro, Y., et al.: Collaborative Face Recognition for Improved Face Annotation in Personal Photo Collections Shared on Online Social Networks. *IEEE Transactions on Multimedia*, 1–14 (2010)
- [10] Elahi, N., Chowdhury, M., Noll, J.: Semantic Access Control in Web Based Communities. In: *Proceedings of the Third International Multi-Conference on Computing in the Global Information Technology*, pp. 131–136. IEEE, Los Alamitos (2008) Multiparty Authorization Framework for Data Sharing in Online Social Networks 43
- [11] Fang, L., LeFevre, K.: Privacy wizards for social networking sites. In: *Proceedings of the 19th International Conference on World Wide Web*, pp. 351–360. ACM, New York (2010)
- [12] Fislser, K., Krishnamurthi, S., Meyerovich, L.A., Tschantz, M.C.: Verification and change impact analysis of access-control policies. In: *ICSE 2005: Proceedings of the 27th International Conference on Software Engineering*, pp. 196–205. ACM, New York (2005)
- [13] Fong, P.: Relationship-Based Access Control: Protection Model and Policy Language. In: *Proceedings of the First ACM Conference on Data and Application Security and Privacy*. ACM, New York (2011)
- [14] Fong, P., Anwar, M., Zhao, Z.: A privacy preservation model for facebook-style social network systems. In: Backes, M., Ning, P. (eds.) *ESORICS 2009*. LNCS, vol. 5789, pp. 303– 320. Springer, Heidelberg (2009)
- [15] Carminati, B., Ferrari, E., Perego, A.: Rule-based access control for social networks. In: Meersman, R., Tari, Z., Herrero, P. (eds.) *OTM2006 Workshops*. LNCS, vol. 4278, pp. 1734–1744. Springer, Heidelberg (2006)
- [16] Kruk, S., Grzonkowski, S., Gzella, A., Woroniecki, T., Choi, H.: D-FOAF: Distributed identity management with access rights delegation. In: Mizoguchi, R., Shi, Z.-Z., Giunchiglia, F. (eds.) *ASWC 2006*. LNCS, vol. 4185, pp. 140–154. Springer, Heidelberg (2006)