Research on access control progress for online social networks

Jian Wang[1,2], Kuo-Yuan Qiao[1] and Zhi-Yong Zhang[1]
[1]*Information Engineering College, Henan University of Science & Technology, Luoyang, 471023, China*
[2]*School of Information Engineering, Zhengzhou University, Zhengzhou, 450001, China*
E-mail: wangjian_migi@sina.com
**Jian Wang*

Online social networks (OSNs) have become the most important platform for people to make friends and show themselves in nowadays, and unauthorized access and usage on people's privacy gains great social attention at the same time. Access control is a general and important way to protect user data from unauthorized sharing. This paper analyzes and compares the present main thought and schemes for access control in OSNs, and presents the existing problems and challenges to be conquered. Finally, the possible research direction and solution technologies are provided.

Keywords: Online Social Networks; Access Control; Attribute-Based Encryption; Usage Control.

1. Introduction

Online Social Networks (OSNs) provide services for people to meet new friends and share multimedia information (e.g. photos, videos, blogs, and reviews) with others. The convenience and efficiency of data dissemination and sharing based on the relationships among users make OSNs become one of the most popular Internet applications. Along with the mature development of wireless mobile communication networks and the widely use of smart terminals, people realize obtaining or sharing digital content anytime and anywhere through OSNs. Until August of 2014, the quantity of OSNs users all over the world has broken through 200 million. For example, Facebook, one of the most famous social network sites, claims that it has more than 900 million active users and over 35 billion pieces of content (web links, news stories, blog posts, notes, photo albums, etc.) shared each month [1]. OSNs have been not only an Internet Application, but also a life way for present people. However, the explosive growth of sensitive and private user data that are readily available in OSNs has raised an urgent expectation for effective method to protect these data from

unauthorized users in OSNs. Security and privacy incidents in OSNs have tremendously gained attention from media and research community [2].

A general method to protect private data from unauthorized access is access control, which is the process to grant permissions to authorized users to act upon resources in a computer-based information system, concluding subjects, objects and access control policy. And the access control system or technology for OSNs is more and more critical, as individual user security and privacy has become an issue related to social stability.

Traditional access control models can be categorized into discretionary access control (DAC) [3], mandatory access control (MAC) [3] and role-based access control (RBAC) [4]. As users in OSNs have absolute rights to decide who can access and share the private data of themselves, MAC don't suit the OSNs environment for its ownership requirements obviously. As while, RBAC is centralized access control, the roles in which are system wide groups set by a system administrator. The access rights over users' resource are allocated to a role the user has no control over, that is, users on OSNs want to set their own values for roles without reference to a central authority. So, it's difficult for users on OSNs to realize local control of relationships with generic roles defined in RBAC model. Finally, DAC driven models seem to be the only choice. However, it becomes over-complex for an OSNs with millions of users and billions of resources for mapping resources directly to subjects. The challenge of managing the access rights of so many users' contributions affects access control efficiency and processing spent unnecessarily on access control affects use factors like response delay. [5]

As a result, all of the traditional access control models for generic information system don't suit access control requirements in OSNs environment. In recent years, along with the privacy preservation being a social focus, the access control methods for OSNs obtain lots of discussion with many excellent research achievements. In this paper, we introduce and compare some representative ideas for access control in OSNs, afterwards, the problems and challenge still existing and the possible future research direction are presented.

2. Related Works

In this section, we present some typical research achievements in access control for OSNs, which is commonly classified by policy design.

2.1. *Trust-based access control*

Trust based approaches use the trust value of OSNs users as the most important parameter in control policy design to decide whether the requestor will be authorized to access the resource. D-FOAF [6] is a distributed identity management system which deploys social networks. It shows how information inherent in social networks can be utilized to provide community driven access rights delegation. And the algorithms for managing distributed identity, authorization and access rights checking are also discussed. Ali et al. [7] presented a multi-level security approach, where trust is the only parameter used to determine the security level of both users and resources. Every resource is assigned a confidence level equal to the trust level of the owner, and only users with equal or higher trust level can access it [5]. Lang [8] presented a novel algorithm that transforms a trust network to a computable expression, and then proposed a Trust Degree Based Access Control model according to the semantics of trust. It's pointed out in the paper that trust does not have only binary value (trust or distrust) but have different levels related to specific situations. Bhatia et al. [9] is intended to address the problem of enforcing privacy policies along with traditional access control policies in an integrated way in order to prevent malicious users to violate the privacy rights of the data providers, where trust threshold value is calculated and set by the data owner to decide authorization. Yan et al. [10] proposed a scheme to secure instant community data access based on trust levels, contexts and time clock in a fine-grained control manner. It permits any community member to select other members with at least a minimum level of trust for secure communications. And the members with a lower trust level cannot access the data sent from him/her in the scheme.

2.2. *Relationship-based access control*

Relationship-based access control takes into account the existence of a particular relationship or a particular sequence of relationships between users and expresses access control policies in terms of relationships between entities (users, resources, etc.) in OSNs. Fong [11] presented a formal model for access control in Facebook-like systems, which divided the access control process into two stages, which are reaching the search listing of the resource owner and accessing the resource, respectively. Although this model allows expression of arbitrary topology-based properties, such as "k-common friends" and "k-clique", it still can't support directed relationships, multiple relationship types and trust metric of relationships. Based on [11], Fong et al. [12] proposed a formal model for

social computing applications, which supports not only “k-common friends” and “k-clique” policies, but also multiple relationship types and directional relationships. Bruns et al. [13] improved [12] by using hybrid logic to enable better efficiency in policy evaluation and greater flexibility of atomic formulas. Nasim et al. [14] presented a XACML-based access control structure for distributed online social networks, whose access privileges mostly depend on “relation type” of U2U (friend, family, colleague, etc.). In the proposal, user profiles are divided into two categories including resources and relations. The category resources is also divided into groups based on types, while the relations of a user are divided into groups based on the relation-type attribute and are stored under the category relations. Cheng et al. [15] integrated attribute-based policies into relationship-based access control and proposed attribute-aware relationship-based access control method to enhance access control capability and support finer-grained controls. Pang et al. [16] proposed a new relationship-based access control scheme, which treats public information existing as a new dimension for users to regulate access to their resources, to solve the problem that the resource owner cannot exploit any other information but user relationships between him and the requester when defining access control policies in general relationship-based schemes.

2.3. *Semantic-based access control*

The semantic web is a concept created by Tim Berners-Lee in 1998, which is an extension of the Web through standards by the World Wide Web Consortium (W3C) to provide a common framework that allows data to be shared and reused across application, enterprise, and community boundaries. Carminati et al. [17] proposed an extensible, fine-grained OSN access control model based on semantic web technologies. In the proposal, the social network related information, including user’s profile, relationships among users, resources, relationships between users and resources, and actions, is encoded by means of semantic web ontologies. Masoumzadeh et al. [18] proposed an Ontology-based Social Network Access Control model using an access control ontology and access control policy rules, which supports both user defined authorization rules and system-level authority policy. Paradesi et al. [19] presented a framework based on user generated policies to control access of social network data. The framework utilizes the DBpedia Lookup service2 to accept the input keywords from the users in the form of Linked Data terms as semantically enhanced keywords, which is stored as policies. And the experiments suggest that such a

framework can help ease privacy concerns while posting and sharing social network content.

2.4. *ABE (Attribute-Based Encryption) based access control*

Recent years, the attribute-based encryption (ABE) scheme [20] provides a new way for privacy protection in distributed resource sharing and has got a lot of researches in access control for OSNs. ABE scheme takes attributes as the public key and associates the cipher text and user's secret key with attributes, so that it can support not only encrypted storage but also expressive access control policies. Sonia et al. [21] presented an access control architecture for OSNs, named EASiER that supports efficient revocation in ABE. Zheng et al. [22] utilized two dimensions of trust levels to control pervasive social networking data access in a heterogeneous manner on the basis of ABE. Huang et al. [23] proposed a secure data sharing scheme in OSNs based on ciphertext-policy attribute-based proxy re-encryption and secret sharing. Guo et al. [24] proposed a privacy-preserving content dissemination scheme in mobile OSNs based on ABE. Shuai et al. [25] proposed a novel access control mechanism called Masque employing ABE, as a hierarchical solution for interactive sharing of encrypted data in OSNs.

3. Open Issue and Challenge

Access control is a mature technology for traditional information systems; however, it is a new field to OSNs for the access control in the OSNs environment has three characteristics: (1) greater demands for privacy preserving and information security are placed on access control; (2) the policy of access control need to reflect more subjectivity for the data authorization being mainly according to the owners' trust and preference; (3) the topology of relationships among OSNs users is more complicated. As a result, the access control in OSNs still faces some problems and challenges.

(1) How to ensure privacy security when realizing fine-grained access control policies

There are many access control methods (trust-based methods, relationship-based methods, semantic-based methods, etc.) being better to realize the fine-grained access than access control list (ACL), but the users' private data is usually stored in plaintext on the social network server. However, the OSNs service provider is only a semi-trusted server who might collect the users' data and share them with others for benefits without users' knowledge or consent [26]. Besides, once the server is attacked, the confidentiality of the user data will

be threatened, too. To realize the encrypted storage, there are also some achievements. Sun et al. [27] presented an identity based encryption method, and Luo et al. [28] presented a data protection structure named FaceCloak. These researches ensure the data confidentiality, but limit the feasibility of the user access, which are not suitable for OSNs. At present, ABE-based access control scheme [21-25] is a good way to support not only encrypted storage but also expressive access control policies; however, they are still not perfect and facing many difficulties in OSNs applications. The main problems existing are:

(a) To express fine-grained control policies, users need define enough attributes subjectively, which leads it difficult to design access structures.

(b) For social groups are dynamic and user attributes may change over time, frequent attributes revocation and alteration lead to too large computational cost for re-encryption and also too large communication cost for key re-distribution, especially to mobile terminals.

(2) How to implement control policies when re-distribution

All the access control schemes above can protect data from unauthorized access at the time of initial release, but they will lose effect after the data got by the authorized users. Actually, users in OSNs have become more aware of the risk of unauthorized re-distribution and usage of their private data through social network sites. Usage Control (UCON) [29] deals with the verification process which ensures that organizations only use personal data in a way compliant with the promises made to the users, and it can enable richer, finer and persistent controls on digital resources. Recent years, there have been many achievements about UCON for data sharing in distributed environment [30-33], mostly used in cloud computing and DRM (Digital Rights Management) system, but the discussion for its application in OSNs is still few. The problem for usage control methods used in OSNs is that the policy can only help users to express which is permitted for limited times or which is prohibited absolutely rather than vague request. It's not suitable for social networks environment for the famous "privacy paradox" [34], that is, people in social networks expect both show themselves to get more attention and protect privacy from unauthorized access or use.

(3) How to compute the trust between users in OSNs accurately

Though different access control schemes adopt different authorization criteria (e.g. Trust, relationship, semantic), they all try to make the control decision maximally according with what users themselves will do in reality. In fact, trust is usually the most important and direct element, according to which users in OSNs decide whether to share their private data with others. However, it is very difficult to accurately compute trust in OSNs for its subjectivity and

complexity. It's always related to many elements including relationship, reputation, historical activity, similarity, etc., even just evaluator's private interest. Oliver et al. [35] researched trust propagation route, and computed trust value using Dijkstra algorithm. Qiao et al. [36] presented a trust calculating algorithm according to the social networks users' context. Liu et al. [37] computed trust between strangers using friends' recommendation value in a P2P social network. Zhang et al. [38] proposed a multimedia social networks trust model based on small world theory, including a direct trust calculation window mechanism, recommended path finding algorithm, and multiple recommendation trust synthetic strategy. Sun et al. [39] used adjacent matrix to represent trust relationships among users, and got trust value through computing inner products of corresponding vectors. However, most of the present methods choose a single dimension (e.g. historical activity, others' commendation, relationship attributes) as the criteria to evaluate trust and got the value through the statistic about the static historical data related to this dimension. As a result, the value computed in this way can't embody the subjectivity, complexity, and variability of the trust among users in a real OSN.

(4) How to avoid privacy disclosure when implementing access control

When making access control decisions or computing trust values, the OSNs server need obtain some users' private information mentioned above, which leads to the privacy disclosure. How to preserve privacy for users during the access control process is still a serious challenge.

4. Development Trend and Research Direction

Our research in this paper provides interesting patterns relating access control in social networks. It highlights some problems with the current access control models and provides various new directions for future access controls. Following are the most noticeable elements to be researched:

4.1. *A trust evaluating scheme based on Information fusion*

As the most essential criteria to make a sharing decision, the trust among OSNs users should fit in with users' considerations at utmost. In reality, there are many factors related to the trust between person and person, including subjective ones and objective ones. So, looking for a way fusing both subjective evidence and objective evidences to evaluate the trust will be a necessary research direction. Multi-Source Information Fusion (MSIF) [40] technology may be the key to this problem.

4.2.*An security architecture based on ABE-based access control and UCON theory*

In the present access control methods for OSNs, the ABE-based schemes can realize both encrypted storage and fine-grained control policies; however, it can't ensure the secure data usage after the data is transferred away from the control domain of the owner. On the contrary, the UCON theory presents the way to preserve the data security when re-distribution; nevertheless, its policy is difficult to reach fine-grained and flexible control. How to combine the ABE-based access control with the UCON theory to design the privacy preserving architecture will be a significant research point.

4.3.*An security strengthened implementation for access control based on trusted computing technology*

OSNs is a typical distributed network, consisted of large amount of nodes and complicated relations. The security of data sharing among these nodes relies heavily on the dependability and security of them. Whether the control policy will be performed honestly in the node platform or whether the sharing node is malicious is important and should be considered, especially in the mobile social networks, where the wireless network environment and mobile terminals face more security risks. The remote attestation in trusted computing can protect data from being shared with malicious nodes, meanwhile, the sealing scheme can ensure the storage and usage security of the data and control policy file. How to use trusted computing technology to implement control policies credibly and consistently is valuable to research.

4.4.*A feasible way to assess the access control for OSNs*

There are many various schemes and models of access control designed for OSNs, all of which are claimed to be effective. Then, scalability is one of the major concerns for access control in social networks. How to build a estimate system with respect to scalability and efficiency of a access control scheme for OSNs can be a valuable contribution.

5. Conclusion and Future Work

This paper has presented an analysis and comparison of access control models for social networks depending on various properties. It's observed that these models are not completed confronted to the security requirements of OSNs. Afterwards, the existing problems and challenges for access control are listed,

and meanwhile, the possible solution and research direction are provided. This study then becomes a basis towards the identification of a perfect access control model for OSNs.

Future work would be the trust evaluation in social networks and a feasible access control model supporting user data encrypted storage, fine-grained control policy, and persistent control without complicated key management.

Acknowledgments

The work was sponsored by National Natural Science Foundation of China Grant No.61370220, Program for Innovative Research Team (in Science and Technology) in University of Henan Province Grant No.15IRTSTHN010,Program for Henan Province Science and Technology Grant No.142102210425, Key Program for Basic Research of The Education Department of Henan Province Grant No.14A520048.

References

1. Arjunagari Yugandhar and Orvakanti Devakiran, *Multi Party Authorization Framework for Data Sharing in Online Social Networks*, in *International Journal of Scientific Engineering and Technology Research*, Vol. 36(March, 2014), pp. 7186-7190.
2. H. Gao, J. Hu, T. Huang, J. Wang, and Y. Chen, *Security issues in online social networks*, in *Internet Computing*, Vol. 15(IEEE Computer Society,2011), pp. 56-63.
3. TCSEC, *Trusted Computer Security Evaluation Criteria (TCSEC)*, DOD 5200.28-STD, Department of Defense, 1985.
4. R. Sandhu, E. Coyne, H. Feinstein, and C. Youman, *Role-Based Access Control Models*, in *IEEE Computer*, Vol.29(IEEE Computer Society,1996), pp. 554-563.
5. A. Ahmad, B. Whitworth, *Distributed access control for social networks*, in *Proc. 7th International Conference on Information Assurance and Security*, (Melaka, Malaysia, 2011).
6. S. R. Kruk, S. Grzonkowski, H. C. Choi, T. Woroniecki, and A. Gzella, *D-FOAF: Distributed identity management with access rights delegation*, in *Proc. the 1st Asian Semantic Web Conference (ASWC'06)*, (Beijing, China, 2006).
7. Ali, B., Villegas, W., and Maheswaran, M., *A trust based approach for protecting user data in social networks*, in *Proc. Conference of the Center for Advanced Studies on Collaborative research (CASCON'07)*, (Ontario,

Canada, 2007).
8. Bo Lang, *Trust degree based access control for social networks*, in *Proc. 2010 International conference on Security and Cryptography*, (Athens, Greece, 2010).
9. Bekha Bhatia, Manpreet Singh, *Trust Based Privacy Preserving Access Control In Web Services Paradigm*, in *Proc. 2013 Second International Conference on Advanced Computing, Networking and Security*, (Mangalore, India, 2013).
10. Zheng Yan, Mingjun Wang, Peng Zhang, *A Scheme to Secure Instant Community Data Access Based on Trust and Contexts*, in *Proc. IEEE International Conference on Computer and Information Technology*, (Xi'an, China,2014), pp. 646-651.
11. P. W. Fong, M. Anwar, and Z. Zhao. *A privacy preservation model for facebook-style social network systems,* in *Proc. Computer Security–ESORICS*, (Berlin, Germany, 2009), pp. 303–320.
12. P. W. Fong and I. Siahaan, *Relationship-based access control policies and their policy languages*, in *Proc. The 16th SACMAT*, (Innsbruck, Austria, 2011), pp.51–60.
13. G. Bruns, P. W. Fong, I. Siahaan, and M. Huth, *Relationship based access control: its expression and enforcement through hybrid logic*, in *Proc. The second CODASPY*, (San Antonio, Texas, USA, 2012), pp. 117–124.
14. Robayet Nasim, Sonja Buchegger, *XACML-Based Access Control for Decentralized Online Social Networks*, in *Proc. IEEE/ACM 7th International Conference on Utility and Cloud Computing*, (London, Britain, 2014), pp. 671-676.
15. Y. Cheng, J. Park, and R. Sandhu, *Relationship-based access control for online social networks: Beyond user-to-user relationships*, in *Proc. PASSAT 2012*, (Amsterdam, Netherlands, 2012), pp. 646–655.
16. Jun Pang, Yang Zhang, *A New Access Control Scheme for Facebook-style Social Networks*, in *Proc. The 9th International Conference on Availability, Reliability and Security*, (Fribourg, Swiss, 2014), pp.1-10.
17. Carminati B, Ferrari E, Heatherly R, et al, *A semantic web based framework for social network access control*, in *Proc. The 14th ACM Symposium on Access Control Models and Technologies*, (Stresa, Italy, 2009), pp. 177-186.
18. Masoumzadeh A, Joshi J., *OSNAC: an ontology-based access control model for social networking systems*, in *Proc. The 2010 IEEE Second International Conference on Social Computing*, (Washington DC, USA, 2010), *IEEE Computer Society*, pp. 751-759.
19. Sharon Paradesi, Ilaria Liccardi, lalana Kagal, Joseph Pato, *A Semantic*

Framework for Content-based Access Controls, in *Proc. International Conference on Social Computing*, (Washington, United states, 2013), pp.624-629.

20. Su Jinshu, Cao Dan, Wang Xianfeng, Sun Yipin, Hu Qiaolin, *Attribute-based Encryption Schemes,* in *Journal of Software,* Vol. 22, pp. 1299-1315.
21. Sonia Jahid, Prateek Mittal and Mikita Borisov, *EASiER: Encryption-based Access Control in Social Networks with Efficient Revocation*, in *Proc. The ASIACCS*, (Hong Kong, China, 2011), pp. 411-415.
22. Zheng Yan, Mingjun Wang, Niemi and V. Kantola, R., *Secure pervasive social networking based on multi-dimensional trust levels*, in *Proc. IEEE Conference on Communications and Network Security*, (Washington, United states, 2013), pp. 100-108.
23. Huang Qinlong, Ma Zhaofeng, Yang Yixian, Niu Xinxin and Fu Jingyi, *Improving security and efficiency for encrypted data sharing in online social networks*, in *China Communications*, Vol. 11, (China Communications,March 2014), pp. 104-117.
24. Guo Linke, Zhang Chi, Yue Hao, et al., *A privacy preserving social-assisted mobile content sissemination scheme in DTNs*, in *Proc. The IEEE INFOCOM*, (Turin, Itay, 2013), pp. 2301-2309.
25. Shuai Huimin, Zhu Wentao and Liu Xin, *Publishing and Sharing Encrypted Data with Potential Friends in Online Social Networks*, in *Security and Communication Networks*, vol. 7, (Security & Communication Networks, February 2014), pp. 409-421.
26. RAJI F, MIRI A, JAZI M., *CP2: Cryptographic privacy protection framework for online social networks*, in *Computers and Electrical Engineering*, Vol.39, (Elsevier,2013), pp. 2282-2298.
27. Sun Jinyuan, Zhu Xiaoyan, Fang Yuguang, *A privacy-preserving scheme for online social networks with efficient revocation*, in *Proc. The IEEE International Conference on Computer Communications*, (San Diego, United states, 2010), pp. 1-9.
28. Luo Wanying, Xie Qi, Urs Hengartner, *Facecloak: an architecture for user privacy on social networking sites*, in *Proc. The International Conference on Computational Science & Engineering*, (Vancouver, Canada, 2009), pp. 26-33.
29. Debmalya Biswas, Nikolai Nefedov and Valtteri Niemi, *Distributed Usage Control*, in *Proc. The 8th International Conference on Mobile Web Information Systems*, (Niagara Falls, Canada, 2011), pp. 562-569.
30. Georgios Karopoulos, Paolo Mori and Fabio Martinelli, *Usage control in SIP-based multimedia delivery*, in *Computers & Security*, Vol. 39, (Elsevier,

March 2013), pp. 406-418.
31. Leanid Krautsevich, Aliaksandr Lazouski, Fabio Martinelli, and Artsiom Yautsiukhin, *Cost-Effective Enforcement of Access and Usage Control Policies Under Uncertainties*, in *IEEE Systems Journal*, Vol. 7, (Institute of Electrical and Electronics Engineers Inc March 2013), pp. 223-235.
32. Anastasi G.F., Carlini E., Coppola M., Dazzi P., et al., *Usage Control in Cloud Federations*, in *Proc. IEEE International Conference on Cloud Engineering*, (Boston, United states, 2014), pp. 141-146.
33. Huang Qinlong, Ma Zhaofeng, Yang Yixian, Niu Xinxin and Fu Jingyi, *Attribute based DRM scheme with dynamic usage control in cloud computing*, in *China Communications*, Vol. 11, (China Communications, April 2014), pp. 50-63.
34. Acquisti A and Grossklags J., *Privacy and Rationality in Individual Decision Making*, in *Security & Privacy*, Vol. 3, (January 2005), pp. 26-33.
35. Richters O, Peixoto T P, *Trust transitivity in social networks*, in (PloSone, 2011), Vol. 6, pp. 1-14.
36. Qiao Xiuquan, Yang Chun, Li Xiaofeng, Chen Juliang, *A Trust Calculating Algorithm Based on Social Networking Service Users' Context*, in *Chinese Journal of Computers*, (Science Press,2011), Vol. 34, pp. 2403-2413.
37. Liu W, Ren P, Sun D, et al., *TrustP2PNet: P2P Social Network with Admission Control Model based on Trust*, in *AASRI Procedia*,(Aasri Procedia, 2013),Vol. 5, pp. 281-286.
38. Zhang Zhiyong, Wang Kanliang, *A Trust Model for Multimedia Social Networks*, in *Social Networks Analysis and Mining*, (Springer, 2013), Vol. 3(4), pp. 969-979.
39. Sun Shuhuan, Zhao Changwei, Zhang Zhiyong, *A Matrix Factorization based Trust Factors Model*, in *Proc. 2015 IEEE International Conference on Information and Automation*, (Yunnan, China, 2015), pp. 803-808.
40. Han Chongzhao, Zhu Hongyan, *Multi-sensor Information Fusion and Automation*, in *Acta Automatica Sinica*,(Sichuan University of Science & Technology, 2002), Vol. 28(1), pp. 117-123.