Journal of Mobile Multimedia, Vol. 6, No. 2 (2010) 145–157

A FLEXIBLE AND SECURE ACCESS CONTROL SCHEME USING SOCIAL BEHAVIOR IN REAL WORLD

DEBASISH CHAKRABORTY SATOSHI OGAWA GEN KITAGATA
Research Institute of Electrical Communication, Tohoku University
2-1-1 Katahira, Aoba-ku, Sendai 980-8577, Japan
deba@shiratori.riec.tohoku.ac.jp satoshi@shiratori.riec.tohoku.ac.jp minatsu@shiratori.riec.tohoku.ac.jp

ATUSHI TAKEDA
Tohoku Bunka Gakuen University
6-45-16 Kunimi, Sendai 981-8551, Japan
atushi@shiratori.riec.tohoku.ac.jp

KAZUO HASHIMOTO
Graduate School of Information Sciences, Tohoku University
6-3-09 Aramaki-Aza-Aoba, Aoba-ku, Sendai, 980-8579, Japan
kh@aiet.ecei.tohoku.ac.jp

NORIO SHIRATORI
Research Institute of Electrical Communication, Tohoku University
2-1-1 Katahira, Aoba-ku, Sendai 980-8577, Japan
norio@shiratori.riec.tohoku.ac.jp

Received July 31, 2009
Revised January 31, 2010

A social network is viewed as a set of people or organizations connected by a set of social relationships, such as friendship or common interests. In the past people would rely on the friends or close associates for information. Today, they search in the web for such information and opinion. And access control to resources is one of the most important technologies for supporting human activities in the digital space, where confidentiality and secure data handling are two most important issues for any such social network users. To realize this control two schemes were proposed: RBAC (Role-Based Access Control) [1] and TRBAC (Temporal Role-Based Access Control) [2] by adding time constraints and role dependencies to RBAC. However, these methods are not effective for temporal activities because of high maintenance costs and inadequacy in safeness. In this paper, we focus on a flexible and secure access control in the real space, by using relations with users and situations, and propose a novel access control which is effective for temporal activities. We evaluate our proposed scheme by implementing a prototype system which shows the effectiveness of this method.

Keywords: access control, socialware, symbiotic computing, collaborative work

1 Introduction

A social network is a structure consisting of individual as well as organizations, connected through various social relationships, varies from close familiar bonds to casual acquaintance. With the proliferation of mobile computer and mobile telephone social networking becoming ever more popular, especially in Japan. A recent study shows that three quarters of Japanese

social network users access the sites only from their mobile phones.

Growth of ubiquitous computing technology makes people's activities in digital space more popular than ever. Digital space is a kind of societies where people participates and interacts. Same as in real space, people in digital space should recognize society, and be able to take actions without anxiety and discomfort. Socialware [3] is a software technology to support people's activities in digital space by enhancing social reality. Socialware has two goals: to apply existing rules and knowledge used in real space to activities in digital space, and to create new and knowledge specific rules to digital space. In social knowledge, where knowledge involved with social activities, is an important information source to enhance people's social reality in digital space. In this paper, focusing on access control to resources in digital space, which is indispensable for activities in digital space, we propose a novel access control scheme based on the concept of Socialware.

RBAC (Role-Based Access Control) [1] is one of the existing access control schemes, where users are assigned with roles, and roles with access rights. This scheme has an advantage of cost management because, roles are in general likely to be associated with positions in an organization. However, this scheme requires static configuration of acceptable roles in ACL (Access Control List). So to add, change, and delete users and their roles, it has to be done manually. Therefore, this scheme is effective where roles are semi-static. But some user's accesses should be enabled temporarily. This is because, in the latter case, administrator will be burdened by frequent manual management of ACL, and also there might be an issue of safety if administrator forgot to disable temporal access rights afterwords. TRBAC (Temporal Role-Based Access Control) [2] is an access control scheme for dynamic and temporal changes to access rights assigned to roles. TRBAC is effective for activities with clear action times, such as a task starting from a fixed time. However, TRBAC can not deal with occasional meetings and unexpected activities caused in emergency situation. Therefore, it is necessary to dynamically control access rights for activities with no clearly specified action time.

In this paper, we propose an access control scheme to control third person's access right by using social relationship. Our scheme flexibly gives access rights in response to situation of workplace and social relationship. This realizes temporal grant of access to resources for irregular activities that do not have clearly specified action times such as occasional meeting. It is to be noted that 'right' and 'authentication' has been used to represent the same meaning throughout this paper if not otherwise mentioned.

Our method is also applicable for mobile multimedia domain. When an outside user wants to access a mobile multimedia services such as video or voice conference system or multimedia storage in a laboratory from remote place, the outside user will automatically gain permission to access these multimedia system and resources only when this user has social relationship with the member of the laboratory. If the member in the laboratory is absent, the outside user will not be able to access the resources or services.

The remainder of this paper is organized as follows. In Section 2, we introduce related works on access control and issues. The proposed scheme is described in Section 3. Section 4 presents a collaborative work support system with the proposed scheme, and Section 5 presents experiments and evaluation of the system. We conclude this paper with a discussion and possible future direction in Section 6.

2 Related Works

Different aspects of social network is analyzed in [4], where social network is described as mapping and measuring of relationships and flows between people, organization and groups, as well as between computers or other information/knowledge. Here, web is also considered as a social network and a mathematical analysis is done to provide a roadmap for researchers working on different aspects of social network. Different social network sites (SNS), such as facebook, MySpace, Hi5, LinkedIn are popular and often useful as well for people to share information and keep in touch with other. But these SNSs are also can pose security threat due to unwanted disclosure of information. Because it is hard to control and monitor who is accessing which information. Though there are some access control is provided but users mostly have to rely on the provider, who may not be always trustworthy. A model is proposed in [5] by providing users with a tool to control their own data by means of encryption.

Lockr is an access control schemed proposed in [6], based on social relationship to make sharing personal content easy. They argued that even in the emergence of huge number of content sharing systems and sites, it is still difficult to share personal content, due to the fact that each of these systems have a different way of providing access control which can not be used with other systems. Moving from one system to another is a lengthy process and requires new registration and inviting friends and it becomes more complicated as the member of such social network grows. In their proposed scheme two new concepts were introduced - social attestation and social access control lists. By using them people can manage their social networks themselves in one place while letting Web sites and Internet systems be in charge of content delivery only.

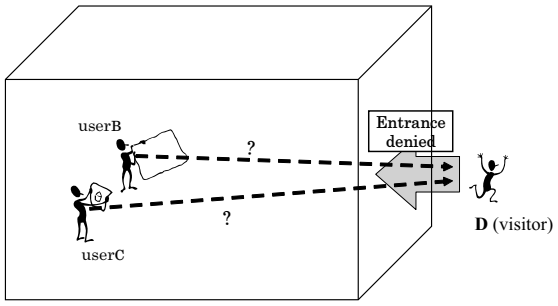
Extensive use of mobile telephones caused widespread availability of Internet applications to mobile users. However, there are certain limitation of mobile phones to render full scale of services, and making it difficult to access lengthy and media-rich information found on the web [7]. But at the same time a voice interface allows the user to speak commands and queries while receiving an audio response and a combination of mobile and voice technologies can lead to a new venues for marketing, entertainment, news and information and business locator services [8]. In [9] a multimodal social networking prototype system is proposed, which is designed for sharing of geographical bookmarks. The system is accessible via a traditional web-based interface as well as via a voice-based interface suitable for mobile phones.

TRBAC (Temporal Role-Based Access Control) [2] introduces time constraint and role dependencies to its scheme, to deal with temporal roles. For example, assume that a part-time staff works with some company from 9 a.m. to 1 p.m., and a role of 'part-time-staff' is assigned to this staff. In this case, an administrator can activate the role 'part-time-staff' from 9 a.m. to 1 p.m. in order to give the staff an access right to the company's system with some time constraint. In addition, validity of a certain role can be controlled in response to the condition of other role, which is called role dependencies. For example, a role 'nurse' can be active only if a role 'doctor' is active. With time constraint and role dependencies, TRBAC effectively deal with regular activities. However, administrator has to make changes to roles for temporal or emergency activities, and higher the frequency of such activities, heavier the workload. Therefore, it is necessary to realize temporal access grant for temporal and emergency activities.

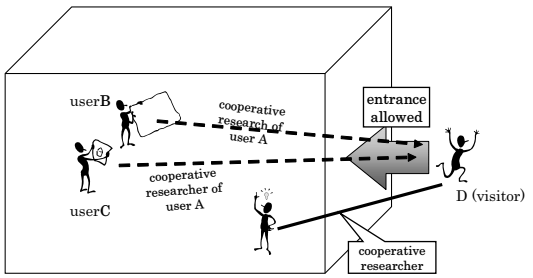
3 Access control proposal based on real space social interactions

3.1 Access control in real space

This paper introduces the notion of temporary access control based on irregular time stamps. This concept is difficult to apply in the existing TRBAC. In real world, there is a need to grant temporary access control during undetermined time stamps, as shown in Fig. 1. In this case, *user A*, *user B* and *user C* are members of the laboratory L, whereas *user D* (visitor) is not a member. However, *user D* involves in a cooperative research project with *user A*. Let us suppose *user D* is going to L. As shown in Fig. 1(a), due to the fact that *user A* is not in the laboratory, *user B* and *user C* are unable to identify *user D*. Therefore, *user D* will not be allowed inside. Since *user A* is not present, L infers that there is no cooperative project in development and so *user D* would not receive the permission to enter the laboratory. On the other hand, as shown in picture Fig. 1(b), when *user A* is in the laboratory, it creates an environment in which *user D* is authenticated as socially related with *user A*. Therefore, *user D* is allowed inside the room. In this way, rooms that normally would be out of reach for an outsider, can be accessed due to the social relationship.



(a) No member has social relationship with the visitor



(b) *user A* has social relationship with the visitor

Fig. 1. Access control in real-space

While inside the laboratory, *user A* becomes responsible of *user D*'s behavior. For that reason, *user D* can have same or less access privileges than *user A*. In similar way we introduce the term of social relationship based access control authority delegation.

3.2 Proposal

As we presented in the previous chapter, we introduce the notion of automatic temporary access control based on irregular time stamps. This concept is difficult to implement by using only TRBAC. We intend to implement the same concept regarding access control permissions in the digital space as in the real world. The spectrum of our access control permissions greatly depends on the existence of a guarantor at the location where a certain job or task is being undertaken.

Therefore, we consider the following two conditions as important:

- T1 - selection of the socially related user inside the working place (L).
- T2 - delegation of rights based on social relationship.

Based on these above two conditions, we propose the following:

- S1 - Implementation of the workplace.
- S2 - Social relationship based access control filter and delegation of rights.

We will explain in detail about S1 and S2 in the next chapters.

3.2.1 The introduction of a work place

In real space, depending on the existence of a guarantor, access to certain resources in a certain environment will be limited or completely restricted, if there is no social relationship. In order to introduce this concept into the digital world, we have to explicitly state the existence of a working place. So far, this was not considered by the existing access control models. Because of the existence of the working place we can now define the relationship between the users that activate within its boundaries. The working place in this case is what we defined in Section 3.1 as L. Inside the working place, there are several resources like printer, projector etc., which can be accessed by outsiders only with the explicit permission of an insider with the right permissions and the right social relationship.

3.2.2 Delegation of access control based on social relationship

A couple of events occur when *user A*, the user that delegates the access rights transfers its rights to *user D*, the user that receives the delegated rights.

- The delegation of rights occurs in conformity with the social relationship between the two.
- The person that receives the rights cannot have more rights than the person that delegates the rights.

In order to meet the previous two requirements, we propose an authentication filter whose role is to delegate only the necessary rights from *user A* to *user D* . The access rights of *user D* will be the intersection between the set of rights of *user A* and the set of rights accepted by the filter. The control knowledge (access control rules) is given by the pair of social relationship and permission filter. As shown in Fig. 2, in order to delegate access control

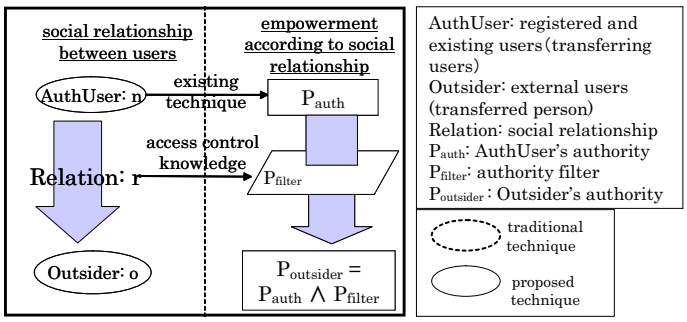


Fig. 2. Delegation of access authorization

rights based on social relationships, we need to setup the access control filter based on access control knowledge. The filter will therefore set the terms of access control rights.

If the permission delegation does not occur in a hierarchical manner, from the security point of view we do not have a trustworthy environment. Therefore, we introduce the concept of allowing rights which enables the user with access permissions to delegate his rights to others. To fulfill this we employ two types of filters:

1. Filter A - which will give right to delegate even to the outsiders if they are trustworthy.
2. Filter B - which will give only specific rights to outsiders, but not the right to delegate.

3.3 The concept in detail

3.3.1 Factors (components)

In this proposal we introduced seven components of the access control model: *resources, users, access (authority) rights, (permission) rights filter, social relationship, work place and access control knowledge.* We will explain them in detail as follows.

- Resource I: computing resources or secret information which fall into the authority of access control.
- User U: participants to different jobs/tasks which requires resource usage.
- Access authority (permission, rights) P: the set of rules against the resources utilized by users.
- Permission filter F: the set of access permissions that can be delegated.
- Social relationship R: the link between users (e.g. if there is a cooperative project under development, the participating members are bound by social links).
- Workplace W: the place where resources are located.
- Access control knowledge K: this knowledge is used to choose authority filter which is used for authority transferring utilizing social relationships among users.

3.3.2 Workplace (attribute value; property value)

In our proposal, considering the importance to retrieve information about the status of a user, we define the workplace as follows:

$w = \langle u_{list}, i_{list} \rangle$
$u_{list} = \langle u_0, u_1, ..., u_n \rangle$
$i_{list} = \langle i_0, i_i, ..., i_m \rangle$
$w \epsilon W, u_n \epsilon R, i_m \epsilon I$

In this case, the u_{list}, and i_{list} are the set of users and resources in a certain workplace. In other words, our workplace is formed of users and existing resources. The user's status with regard to the workplace might change. Therefore w changes with time. User u is defined as:

$u = \langle d_u, ru_{list}, p_{list} \rangle$
$ru_{list} = \langle ru_0, ru_1, \cdots, ru_n \rangle$
$ru_k = \langle r_k, u_k \rangle$
$p_{list} = \langle p_0, p_1, \cdots, p_n \rangle$
$r_k \in R, u_k \in U, p_k \in P$

In this case, d_u represents the user's data and ru_{list} represents the set of social relationships of the user. For example, in case of a cooperative project, we can identify it as social relationship between the coworkers.

```
authorize(uu){
   (ua, ra-u):=decideDelegater(uu, w);
   pu := delegatePermissions(uu, ra-u);
   allow(pu);
}

delegatePermissions(ua, ra-u){
   f := getPermissionFilter(ra-u);
   p := ua.plist ∧ f;
   return  p;
}
```

Fig. 3. Algorithm for access delegation

3.3.3 Delegation of access control

We propose a system in which a user u_u wishing to utilize a workplace w is looking for a user u_a with whom u_u has a social relationship r and it is being identified by the latter. The permission filter is based on the access control knowledge and the social relationship. As a result, the permission p_a, held by the user u_p intersected with the permission filter set f,

produces the set of permissions p_u of user u_u. The process of granting access permission p to user u_u is shown in Fig. 3.

The algorithm starts with the selection of the socially related user (*decideDelegater*) which can delegate permissions. In order to do that, the *delegatePermissions* function is applying the *getPermissionFilter* and returns the proper access control rights. In Fig. 4 we show how the access knowledge works.

```
getPermissionFilter(ra-u){
    if(ra-u == "cooperative researcher")
        return[p1, p2, p3, p4];
    elseif(ra-u == "OB")
        return[p3, p4];
    elseif(ra-u == "visiting Lab.")
        return[p4];
    else
        return[];
}
```

Fig. 4. Access control knowledge for a laboratory

3.4 The process of granting access permission

We explain the process of granting access permission with Fig. 5. In this example we portray user *user A* who does not belongs to the laboratory L but has the intention of being active for a while there. *user B* and *user C* are members of laboratory L. *user A* and *user B* are socially linked through a common (cooperative) project and the former has *rwa (read, write, allow)* rights for the resource 1. Socially linked users as co-researchers are empowered by the access control knowledge with *rw* rights for resource 1. We present the process of granting permissions to *user A* as follows:

1. *user A* asks for access permission from the workplace - in this case the laboratory L.
2. The users that have any social link with user A reply to it.
3. *user A* finds *user B* as being socially related.
4. Based on the predetermined rules, *user B* becomes the guarantor of *user A*.
5. If the authentication process is successful, *user B* requests access permissions from the resource administrator.
6. The resource administrator checks all the resource access knowledge, passes them through permission filter and intersects them with the set of *user B*'s permissions resulting in *user A*'s permissions.

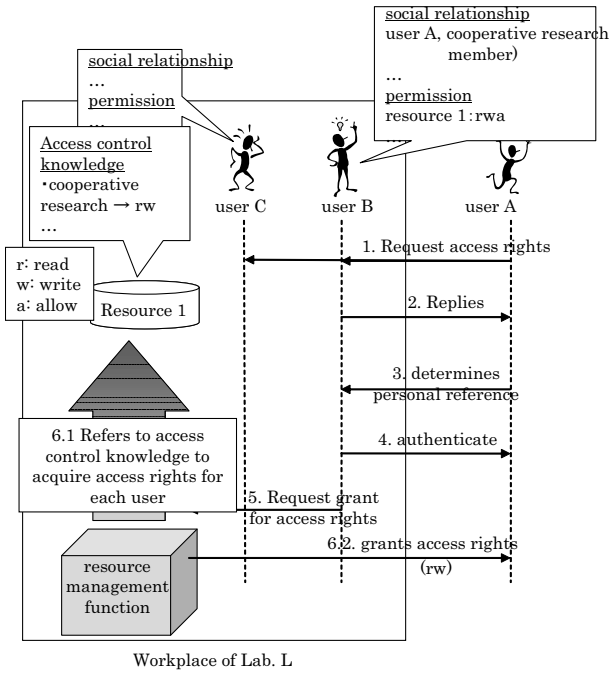


Fig. 5. Flow of access authorization

In this way, utilizing our concept, even if *user A* does not have permissions to access resources, due to the social link with *user B*, the former will be granted temporary access rights to the resources that make the object of the common goal.

4 Cooperative Work Support System

4.1 Summary of the System

To confirm the effectiveness of our proposal, we design a cooperative work support system. This system realizes access control for resources owned by organizations, and can also be applied for temporal activities of users by utilizing social relationships.

Fig. 6 shows summary of the system. As it is shown in this figure, there are two organizations, X and Y. These organizations proceed cooperative project. Social relationship such as "cooperative project member" are constructed among users who has joined to the project. Due to this social relationship, users belonging to organization Y, and has joined to the project can use resource in organization X. Whereas, users belonging to organization Y but are not joined to the project and has no relationship with member of organization X cannot use the resource in organization X. Also a visitor who does not belong to either organization X and Y, and has no relationship with the member of organization X cannot use the resource in organization X.

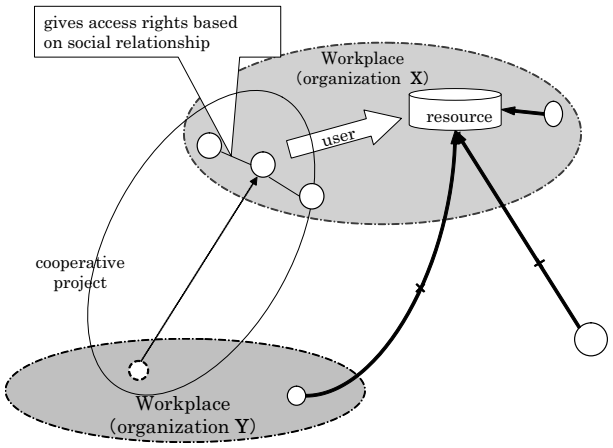


Fig. 6. Cooperative work support system

4.2 Agent composition

We design the system based on agent-oriented computing and introduce the following three agents:

1. User Agent: This agent is a delegate of a user in digital space. This agent uses resources instead of real user according to the user's request.

2. Resource Agent: This agent agentificates resources and has access control knowledge and an authority filter. For instance, we designed a printer agent ($printerAg$) and a projector agent ($projectorAg$).

3. Workplace Agent: This agent administrates user agents and resource agents in workplace. It delegate access authority to a user according to social relationships by referring access control knowledge held in resource agent.

Fig. 7 shows agent composition of our system. $userAg1$ to $userAg3$ represents user agents, $printerAg$ and $projectorAg$ are resource agents, and $workplaceAg$ is a workplace agent. Workplace in Fig. 7 represents the space where user works. The field is administrated by $workplaceAg$. Here, presence of a user is expressed as presence of a user agent in workplace. For example, when a user sends a request for authority delegation but no response is returned by any user agents, it implies that there are no member who has social relationship with the user, and as a result access to the requested resource is denied.

4.3 Environment of Implementation

We implemented the system by using DASH [11] system, a rule-based agent framework, and IDEA [12] which is an integrated design environment for DASH. We used Java language to implement base processes controlled by DASH agents.

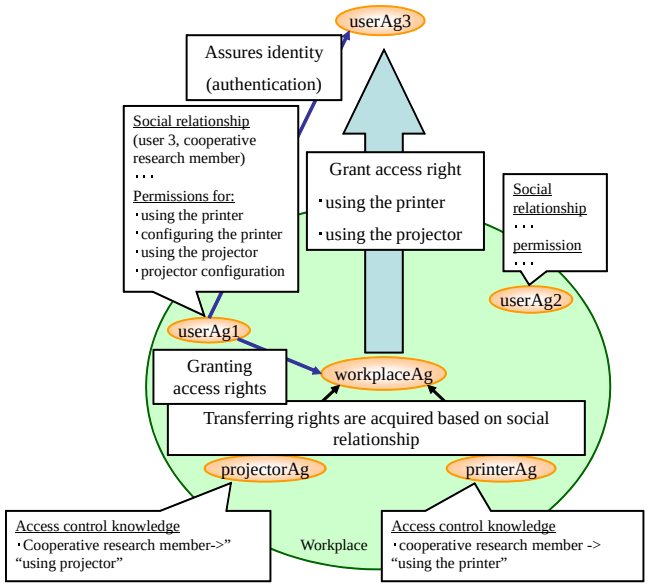


Fig. 7. Agent composition

5 Experiment and Evaluation

To evaluate our proposal, we conducted experiments with some scenarios under certain conditions depicted in Fig. 8. *user C* and *user D* are member of the laboratory, and *user A* and *user B* are visitors. *user C* involves in a cooperative research with *user A*. *user D* also relates to another cooperative research with *user B*. So there are social relationships according to these cooperative researches. In addition, *user C* is a student and *user D* is a staff, so *user D* has more authority than *user C*. We assume situations where a visitor, *user A* and *user B*, come to laboratory's workplace to proceed cooperative research. Here, we conducted experiments with the following four scenarios: (1) no one is in the laboratory, (2) only *user C* is present, (3) only *user D* is present, (4) both *user C* and *user D* are present.

Fig. 9 shows the experimental results. We confirmed that both *user A* and *user B* got access authority by social relationship as "cooperative research member", but the authorities of *user A* and *user B* are not same. This is because they are delegated authorities by different user. Also in some scenarios, we found cases when authority is not delegated. In these scenarios, because a member who has social relationship with the visitor, *user A* or *user B*, is absent and the system cannot verify the identity of the visitor, and no authority is delegated. In other words, absence of *user C* means that cooperative work of *user A* and *user C* are not proceeded. Therefore, *user A* cannot get authority when *user C* is absent.

¿From the above results, we confirmed that our system is useful to delegate authority for temporal activities by utilizing social relationship of users presented in the field of activity.

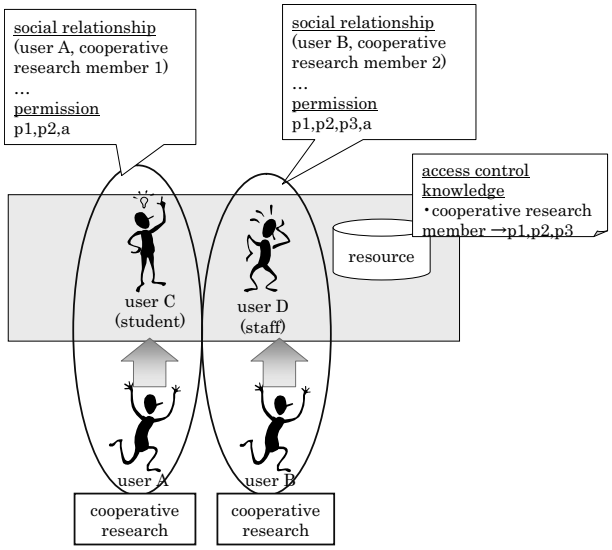


Fig. 8. Precondition of operation scenario

Cases (Users in Workplace) \ scenario	User A requests access rights	User B requests access rights
(1) None	X	X
(2) User C	p1, p2	X
(3) User D	X	p1, p2, p3
(4) User C & D	p1, p2, p3	p1, p2, p3

X: no access right is granted due to lack of personal reference

Fig. 9. Evaluation results

6 Discussion and Conclusion

Access control schemes using social relationship was proposed by Nagao et al. [10]. In this access control scheme, access rights are statically configured based on social relationship. Because of static configuration, administrator has to configure multiple access rules for each social relationships. For example, necessary rules for a relationship of 'co-researcher' are professor, associate professor, student and so on. In contrast, the proposed scheme gives an access right to a user by applying authentication filter the right to those who offers the user's personal reference. Therefore, administrator only needs to configure authentication filter and access control rules for each relationship. For example, one set of them for the 'co-researcher' relationship. In addition, existing scheme uses social relationship of all users regardless of existence of them. This can realize temporal access grant with time constraint for regular activities, but unable to deal with irregular ones. In contrast, proposed scheme can effectively control access rights even if temporal grant of access is necessary.

In this paper, we proposed a novel access control scheme to automatically grant accesses

for irregular activities which TRBAC cannot deal with. This scheme achieves to control access rights in digital space as in real space. Through this cooperative work support system a temporary access can be obtained even when the user does not have direct permission to access the resources. As our system can be used in digital space, this method can be used in mobile environment as well. Such as, synchronize login state and members' presence in a laboratory automatically, investigate the effective method for monitoring any outside user to prevent the person if he/she is behaving in an inappropriate way while using laboratory resources. These are the possible extensions we are considering as our future goal.

Acknowledgment

This work is partially supported by the Research and Development of Dynamic Network Technology program of NiCT.

References

1. R.S. Sandhu, E.J. Coyne, H.L. Feinstein, and C.E. Youman, "Role-Based Access Control Model", Computer, vol. 29, no. 2, pp. 38-47, 1996.
2. E. Bertino, P.A. Bonatti, and E. Ferrari, "TRBAC: A Temporal Role-Based Access Control Model", ACM Trans. Information and System Security, vol. 4, no. 3, pp. 191-233, Aug. 2001.
3. Tetsuo Kinoshita, Susumo Konno, Gen Kitagata, Takahiro Uchiya, Hideki Hara, "Symbiotic System: Co-existence and Mutual Respect of Human, Society, Environment, and Information System, Forward: Socialware", IPSJ, Vol.47, No.8, pp.817-824, 2006.
4. Mohsen Jamali, Hassan Abolhassani, "Different Aspects of Social Network Analysis", Proceedings of the 2006 IEEE/WIC/ACM International Conference on Web Intelligence, Dec. 2006, pp. 66-72.
5. Filipe Beato, Karkulf Kohlweiss, and Karel Wouters, "Enforcing Access Control in Social Network Sites", The 9th Privacy Enhancing Technologies (PETA 2009), Aug. 5-7, 2009. Seattle, WA, USA.
6. Amin Tootoonchian, Kiran K. Gollu, Stefan Saroiu, Yashar Ganjali, Alec Wolman, "Lockr: Social Access Control for Web 2.0", WOSN'08, Seattle, Washington, USA, August 18, 2008.
7. S.E.Chang, M.S.H. Heng, "An Empirical Study on Voice Enabled Web Applications", IEEE Pervasive Computing, IEEE, Jul.-Sept. 2006, pp. 76-81.
8. J.A.Q. Ruiz, J.R.M. Sanchez, "Design of a VoiceXML Gateway", Proc. 2003 4th Mexican International Conference on Computer Science, IEEE CS, Sept. 2003, pp. 49-53.
9. Stan Kurkovsky, David Strimple, Eric Nuzzi, Kerry Verdecchia, "Mobile Voice Access in Social Networking Systems", 5th International Conference on Information Technology - New Generations, Las Vegas, Nevada, April 7-9, 2008.
10. Masahiro Nagao, Glenn Mansfield Keeni, Masahiro Ishigaki, Atsushi Togashi, Shoichi Noguchi, "A Secure Distributed Database System with Time-series Data and Social-Relation Based Information Access Control", IEICE Technical Report, Vol.107, No.6, pp.55-60,2007.
11. S. Fujita, H. Hara, K. Sugawara, T. Kinoshita, and N. Shiratori, "Agent-based design model of adaptive distributed systems", The International Journal of Artificial Intelligence, Neural Networks and Complex Problem-Solving Technologies, Vol. 9, No. 1, pp. 57-70, 1998.
12. Takahiro Uchiya, Takahide Maemura, Kenji Sugawara, Tetsuo Kinoshita, "Interactive Design Environment for Agent-Based System", Transaction of the Institute of Electronics, Information and Communication Engineers. D-I, Vol.J88-D-I, No.9, pp. 1344-1355.