Visitor Access Control Scheme Utilizing Social Relationship in the Real World

Gen Kitagata, Debasish Chakraborty, Satoshi Ogawa, Atushi Takeda, Kazuo Hashimoto, Norio Shiratori

Visitor Access Control Scheme utilizing Social Relationship in the Real World

Gen Kitagata[1], Debasish Chakraborty[1], Satoshi Ogawa[1], Atushi Takeda[2], Kazuo Hashimoto[3], and Norio Shiratori[1]

[1] Research Institute of Electrical Communication, Tohoku University
2-1-1 Katahira, Aoba-ku, Sendai 980-8577, Japan
[2] Tohoku Bunka Gakuen University, Sendai, Japan
[3] Graduate School of Information Sciences, Tohoku University, Sendai, Japan

Abstract. Access control to resources is one of the most important technologies for supporting human activities in the digital space. To realize the control two schemes were proposed: RBAC (Role-Based Access Control) and TRBAC (Temporal Role-Based Access Control) by adding time constraints and role dependencies to RBAC. However, these methods are not effective for temporal activities such as visitor access because of maintenance costs and inadequacy in safeness. In this paper, we focus on a visitor access control in the real world, by utilizing relationship with users and situations, and propose a novel access control scheme which is effective for temporal activities.

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

1 Introduction

Growth of ubiquitous computing technology make people's activities in digital space more popular than ever. Digital space is a kind of societies where people participate 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 [1] 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) [2] 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 management cost 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 roles, it has to be done manually. Therefore, this scheme is effective where roles are

semi-static. But some users 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 afterwards. TRBAC (Temporal Role-Based Access Control) [3] 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 due to emergency situation. Therefore, it is necessary to dynamically control access rights for activities with no clear action time.

In this paper, we propose automated visitor access control scheme to control third person's access right by utilizing 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 explicit 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.

The remainder of this paper is organized as follows. In Section II, we introduce related works on access control and issues. The proposed scheme and its model are described in Section III. Section IV presents a collaborative work support system with the proposed scheme, and Section V presents experiments and discussion with the system. In Section VI, we compare our scheme with existing access control scheme utilizing social relationship. We conclude our work in Section VII.

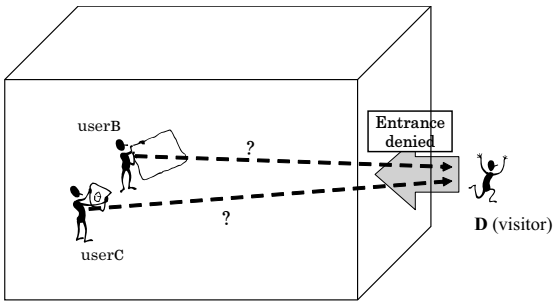
2 Related Works

TRBAC (Temporal Role-Based Access Control) [3] 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 'part-time-staff' is assigned to the 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.

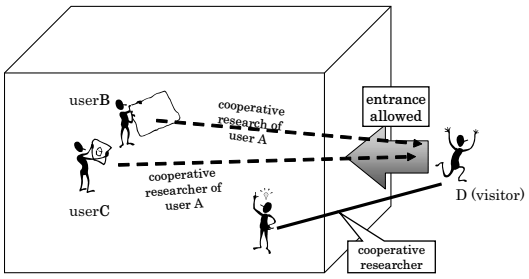
3 Access control proposal based on real space social interactions

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



(a) No member has social relationship with the visitor



(b) Person $User\ A$ has social relationship with the visitor

Fig. 1. Access control in real-space

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.

While inside the laboratory, person $User\ A$ becomes responsible of $User\ D$'s behavior. For that reason, $User\ D$ can have same or less access privileges than $User\ A$. In this 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 in the digital space the same concept regarding access control permissions 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 from inside the working place (L)
- T2 - delegation of rights based on social relationship

Based on the previous 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.

The introduction of a work place In real space, depending on the existence of a guarantor, in other words if there is no social relationship, our access to certain resources in a certain environment are limited or completely restricted. 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 III(A) 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.

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 that 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 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 rights based on social relationships, we need to setup the access

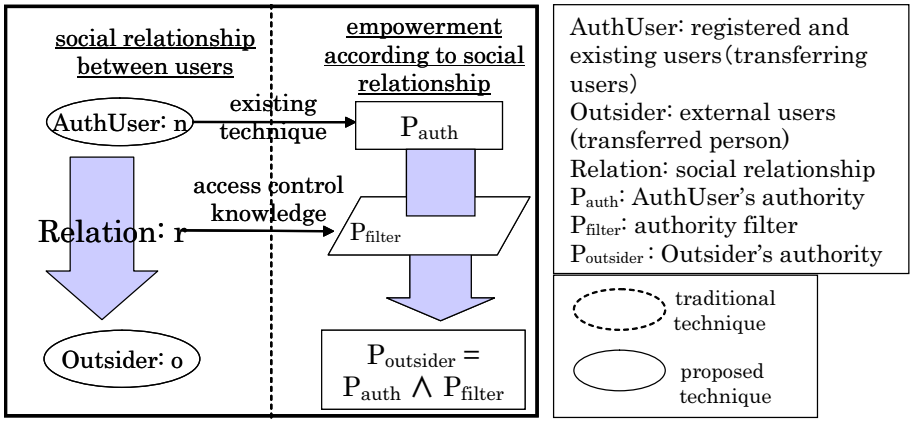


Fig. 2. Delegation of access authorization

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

Factors (components) and models In this proposal we introduced seven components of the access control model: *resources, users (visitor and member), access (authority) rights, (permission) rights filter, social relationship, work place and access control knowledge*. Fig. 3 shows our access control model. We will explain them in detail as follows.

- Resource I: computing resources or secret information which fall into the authority of access control.
- Outsider O: a visitor who wants to use resources but not having permission regularly.
- Member M: a member of organization who has regular permission for resource usage.
- Access authority (permission, rights) P: the set of rules against the resources utilized by users.

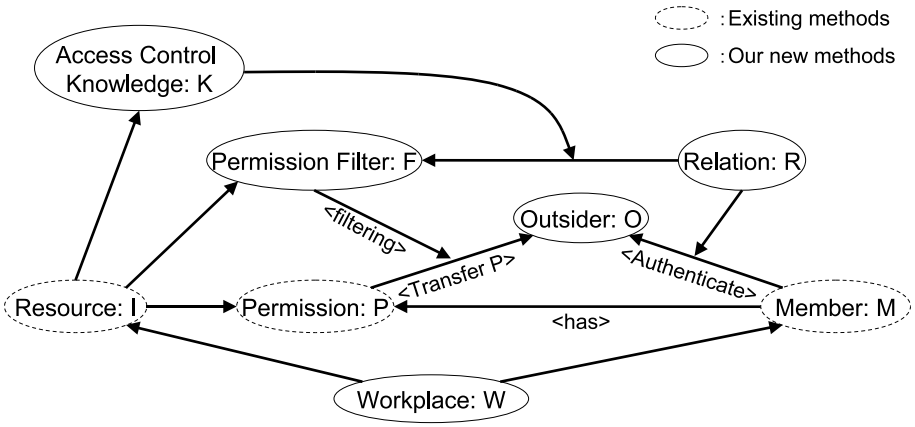


Fig. 3. Access control model of our scheme.

- 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.

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 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:

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

```
authorize(u_u){
    (u_a, r_a–u) := decideDelegater(u_u, w);
    p_u := delegatePermissions(u_a, r_a–u);
    allow(p_u);
}

delegatePermissions(u_a, r_a–u){
    f := getPermissionFilter(r_a–u);
    p := u_a.p_list ∧ f;
    return p;
}
```

Fig. 4. Algorithm for access delegation

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

Fig. 5. Access control knowledge for a laboratory

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.

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. 4. 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. 5 we show how the access knowledge works.

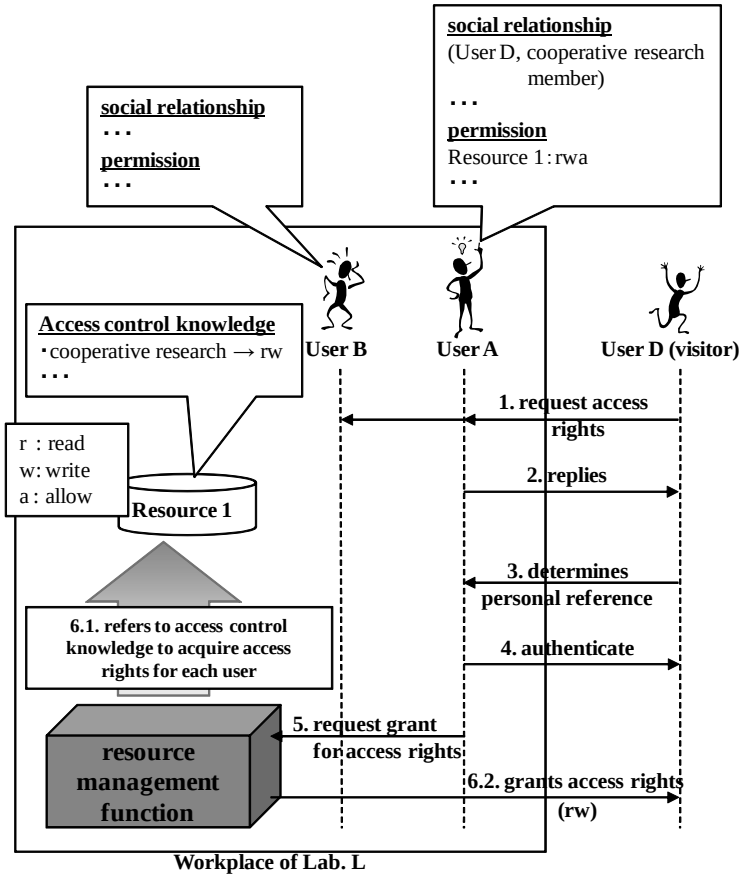


Fig. 6. Flow of access authorization

3.4 The process of granting access permission

We explain the process of granting access permission with Fig. 6. In this example we portray user *UserD* who is not a part of the laboratory L but has the intent of activating for a while there. The users *UserA* and *UserB* are members of laboratory L. *UserD* and *UserA* 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 *UserD* as follows:

1. *UserD* asks for access permission from the workplace - in this case the laboratory L.
2. The users that have any social link with *UserD* reply to it.
3. *UserD* finds *UserA* as being socially related.

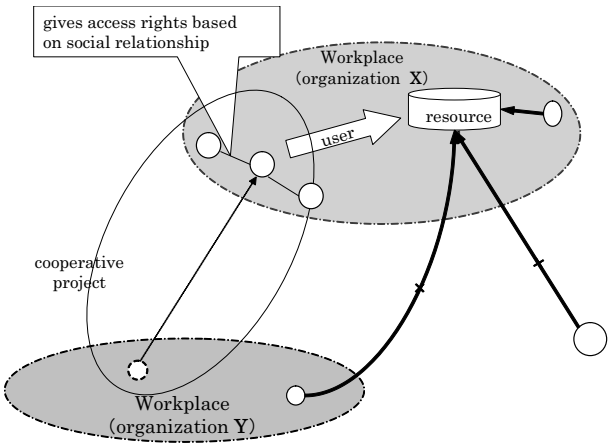


Fig. 7. Cooperative work support system

4. Based on the predetermined rules, *UserA* becomes the guarantor of *UserD* .
5. If the authentication process is successful, *UserA* requests access permissions from the resource administrator.
6. The resource administrator checks all the resource access knowledges, passes them through permission filter and intersects them with the set of *UserA* 's permissions resulting in *UserD* 's permissions.

In this way, utilizing our concept, even if *UserD* does not have permissions to access resources, due to the social link with *UserA* , 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 effectiveness of our proposal, we design a cooperative work support system. This system realizes access control for resources owned by organizations, and also the system can be applied for temporal activities of users by utilizing social relationships. Fig. 7 shows summary of the system. In Fig. 7, there are two organization X and Y. These organizations proceed cooperative project. Social relationship such as "cooperative project member" are constructed among users who are joined the project. Due to this social relationship, users belonging to organization Y and are joined the project can use resource in organization X. By contrast, users belonging to organization Y but are not joined 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 both organization X and Y, and has no relationship with member of organization X cannot use the resource in organization X.

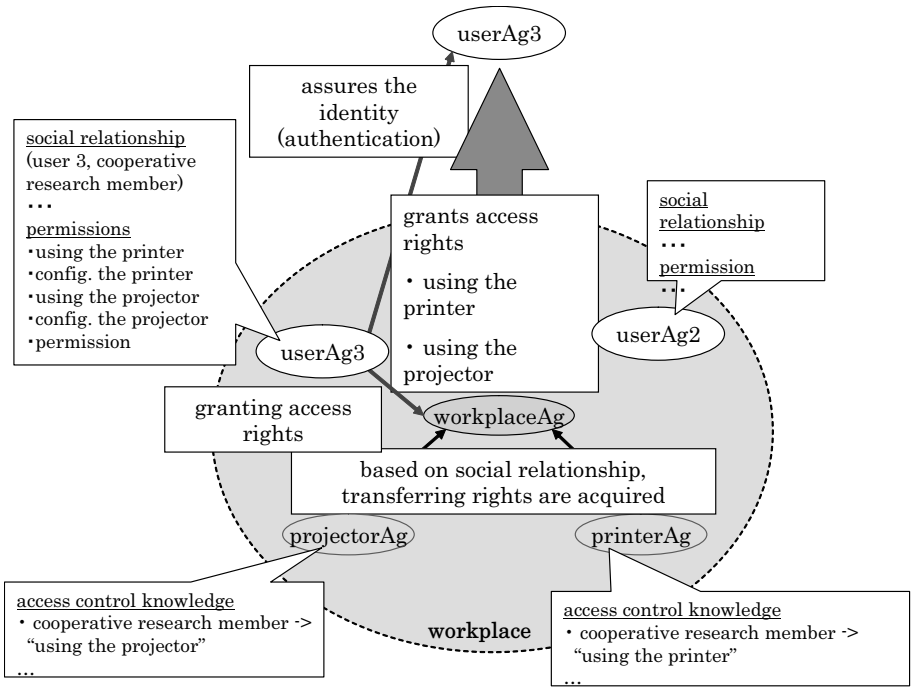


Fig. 8. Agent composition

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. 8 shows agent composition of our system. $userAg1$ to $userAg3$ represents user agents; $printerAg$ and $projectorAg$ are resource agents. And $workplaceAg$ is a workplace agent. And workplace in Fig. 8 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

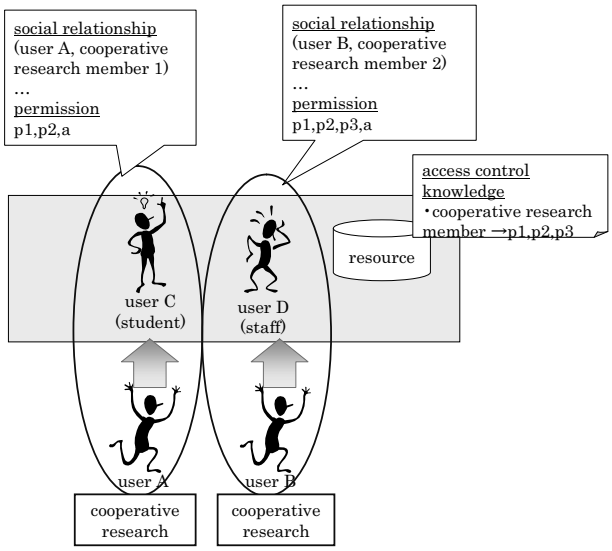


Fig. 9. Precondition of operation scenario

are no member who has social relationship with the user, and as a result access for requested resource is denied.

4.3 Environment of Implementation

We implemented the system by using DASH [5] system which is rule-based agent framework, and IDEA [6] which is an integrated design environment for DASH. We used Java language to implement base processes controlled by DASH agents.

5 Experiment and Evaluation

To evaluate our proposal, we conducted experiments with some scenarios under certain conditions depicted in Fig. 9. $User\ C$ and $User\ D$ are member of laboratory, and $User\ A$ and $User\ B$ are visitors. $User\ C$ proceeds a cooperative research with $User\ A$. $User\ D$ also does 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 much authority than $User\ C$. We assume situations that a visitor, $User\ A$ and $User\ B$, comes to laboratory's workplace to proceed cooperative research. Here, we conducted 4 experiments as following 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. 10 shows experimental results. We confirmed that both $User\ A$ and $User\ B$ got access authority by social relationship as "cooperative research member", but the

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. 10. Evaluation results

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 identity of the visitor, and no authority is delegated. In other words, absent of $User\ C$ means that cooperative work of $User\ A$ and $User\ C$ are not proceeded. Therefore $User\ A$ cannot get authority while $User\ C$ is absent.

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

6 Discussion

Visitor access control schemes utilizing social relationship was proposed in previous works [4]. 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 to the right of who offer 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.

7 Conclusion

In this paper, we proposed a novel access control scheme to automatically grant accesses for irregular activities such as resource usage of visitor which TRBAC cannot deal with. This scheme achieves to control access rights in digital space as in real space.

Acknowledgement

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

References

1. 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.
2. 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.
3. 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.
4. 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.
5. 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.
6. 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.