Context-Aware Role Based Access Control Using User Relationship

Kangsoo Jung and Seog Park

***Abstract*—Role-based access control is widely used in modern enterprise systems because it is adequate for reflecting the functional hierarchy in various organizations' for access control model. However, environmental changes, such as the increasing usage of mobile devices, make several challenges. Our research suggests a relationship-based access control model that considers the relation with surrounding users in organization. Relation is significant context information but it is not considered in existing access control models. The proposed technique is different from that in traditional research in two ways. First, we regard the relationship among employee's as contextual information. As a result, the administrator can manage fine-grained access control for cooperative work in an organization. Second, we design access control architecture using NFC technique to deal with usability and security problems. Moreover, we propose a protocol for enforcing the suggested access control model in real world. We report performance analysis and security evaluation**

***Index Terms*—Access control, context-aware, relationship-based, Security.**

I. Introduction

In the role-based access control model, the permissions to perform certain operations is assigned to specific roles instead of assigning permission to each user directly. That is why role-based access control appropriate to manage enterprise and government access control systems. Role-based access control model extends various access control models to satisfy the requirements for access control. Nowadays, context-aware access control models that take contextual information account of are researched to reflect the dynamic environment of organizations.

Context is classified into five categories. (1) Environmental context: light, people, services, etc. (2) Personal context: mental and physical information about the user, (3) Spatio-Temporal context: time, location and movement. (4) Task context: user's behavior, goal, tasks, etc. (5) Social context : social relationship of user.

Existing context-aware access control model focus on location and temporal contextual information to constraint access control. However, various types of context-aware access control models are needed to satisfy domain-specific requirement for access control.

Manuscript received October 9, 2012; revised December 17, 2012. This research was supported by the MKE(The Ministry of Knowledge Economy), Korea, under the ITRC(Information Technology Research Center) support program supervised by the NIPA(National IT Industry Promotion Agency"(NIPA-2012-(H0301-12-3004)))

Kangsoo Jung and Seog Park are with the Department of Computer Science and Engineering at Sogang University (e-mail: azure84@naver.com)

We suggest relationship-based access control model that considers the relationship among users in an organization and surrounding user identification as context information. We assume mobile office environment as our domain this paper. In mobile office, employees who use mobile device such as smartphone and tablet PC have relation with other employees for cooperative work to perform organization's task. But existing access control model do not consider relationship among employees as context information in mobile office. Proposed access control model consider relations among surrounding users for access control in mobile office systems.

The rest of paper is organized as follows. Section 2 describes the related work. Section 3 explains our research goal, proposed access control model and protocol. Section 4 discusses performance analysis and security evaluation. Section 5 concludes the paper with future works.

II. Related Works

Several extensions to the basic RBAC is proposed for addressing the access control needs of commercial organizations, and some of the researches focus on how RBAC can be extended to context-aware access control.

Generalized RBAC model (GRBAC)[1] define environmental role to control access to private information and resources in ubiquitous computing applications. Permission to assign role is associated with set of environmental role in GRBAC and environmental properties such as time and location influence to role activation. Temporal RBAC (TRBAC)[2] consider time dimension to the RBAC model. Role is activated if time constraints are satisfied in TRBAC. Generalized Temporal RBAC (GTRBAC)[3] is extended from TRBAC. In this work, role hierarchy and separation of duty is defined in terms of TRBAC. GEO-RBAC [4] is to associated spatial extents with traditional roles. In this model, role activation is based on location of the user. For example, user activate employee role only when the user's location is in the company.

There are a lot of context-aware access control model is researched, but it needs more research to deal with fine-grained and secure access control. In this paper, we introduce relationship-based access control model that is based on user's relation information that is associated with cooperative work in organization.

Recently, several relationship-based access control model [5] [6] [7] is researched, but these kind of researches have different goals with proposed access control. Because existing relationship-based access control model focuses on relationship in OSN (Online Social Network). But proposed

DOI: 10.7763/IJCTE.2013.V5.744

access control model consider user's relation for cooperation in organization

The difference between suggested access control model and existing model are as follows. First, we introduce relationship-based access control model that consider surrounding user who cooperate together, and design architecture to enforce proposed access control model. Second, we propose protocols that is based on Near Field Communication (NFC) technique for suggested access control model. NFC is an RFID-based technology that provides contactless communication between NFC enabled device. NFC has a limitation that is broadcast range is typically 10 cm in radius. But this limited range can provide evidence of the user's presence. Using NFC, we can prove that other user's existence and prevent permission abusing.

III. Relationship-Based Access Control Model

A. Goals

We defined the following goals for our design. First, proposed technique provides an access control model as convenient as possible. If access control model is not convenient to use, users try to find byway of system. Proposed access control model aims to provide a maximum usability using NFC technique as an interface. Second, we consider user's relation that is associated with cooperation among employees in organization for access control. Access control for cooperation is needed because cooperative work is more general in real world. Third, we try to design our access control model as general as possible. For achieving this goal, we minimize any assumption for our access control model. It makes proposed technique can be applied to existing context-aware model easily.

Before we introduce proposed access control model, we try to define several terms that we use in proposed model to avoid confusion with existing access control model.

1) Definition 1 relationship

Relationship means that relation among users who cooperate in organization. Relationship reflects organization hierarchy and only administrator can change registered relationship.

2) Definition 2 relationship-based access control

Relationship-based access control model is access control model that consider user's relationship and surrounding user information to decide permission assignment and delegation. Role that is related with relationship is defined as follows.

For every k, i

If $\exists$ RR(k) $\in$ Relation Role, $\exists$ U(i) $\in$ Users,

Then role activation among User a, b, c are defined as follows

$$\text{Active RR}(k) = \text{U}(a) \wedge \text{U}(b) \wedge \text{U}(c)$$

That is, role activation is occurred when other users who is related for cooperative work is in surrounding area. We use NFC technique to assure other user's presence in surrounding area.

B. Architecture

Suggested access control architecture is described in Fig. 1. It consists of Certification Server, Access Control Administrator, and User. We explain each component more detailed as follow.

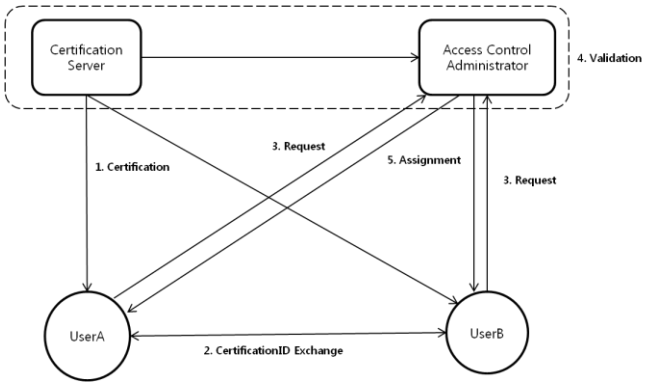

Fig. 1. Relationship-based access control architecture.

Certification Server: Certification server publish certification value to each user. Proposed access control model validate each user's identification because we use relation information as contextual information to decide permission assignment and delegation. Certification server publish certification id to each user and these certification id is also published to access control administrator to validate user's identification

Access Control Administrator: Access control administrator perform access control decision. When users request certain permission, access control administrator decide permission assignment by access control policy, user's certification id, requested permission and relationship information.

User: User requests permission assignment or delegation to access control administrator. Proposed access control model use PKI(public key infrastructure) for authentication. That is why each user should store own private key and other user's public key. We assume that user's mobile device has sufficient capability to calculate public key cryptography.

C. Protocol for Permission Assignment

Proposed access control model decides permission assignments based on relationship among users. It focuses on real world requirements that tasks in organization is carried out by cooperation. Suggested protocol is as follow. We assume that there are two users who are co-worker use proposed access control.

Step 1: Certification server publish Certification ID to each user. [Cetification Server->$\text{Cert}_{\text{User}}$]

Step 2: UserA and UserB encrypt their own Certification ID by their own public key. And then, they exchange encrypted Certification ID using NFC. [UserA: $E_{pub\_A}(\text{Cert}_A)$->UserB, UserB: $E_{pub\_B}(\text{Cert}_B)$:->UserA]

Step 3: UserA,B encrypt their own Certification ID, Timestamp T, request role RR_k,and encrypted other user's Certification ID. And then send these encrypted message to Access Control Administrator. User can add other contextual information such as time and location to apply other context-aware access control model. [User_A:$E_{pub\_A}(\text{Cert}_A,T_A,RR_K,E_{pub\_B}(\text{Cert}_B))$-> Access Control Administrator, User_B:$E_{pub\_B}(\text{Cert}_B, T_B,RR_K,E_{pub\_B}(\text{Cert}_A))$->

Access Control Administrator]

Step 4: Access Control Administrator decrypt encrypted message using stored each user's private key and validate user's identification. After then, Access control administrator decide to allow permission comparing user's relationship with access control policy. At this time, UserA and UserB's timestamp's time and request time difference is under threshold value to prevent abusing. Protocols

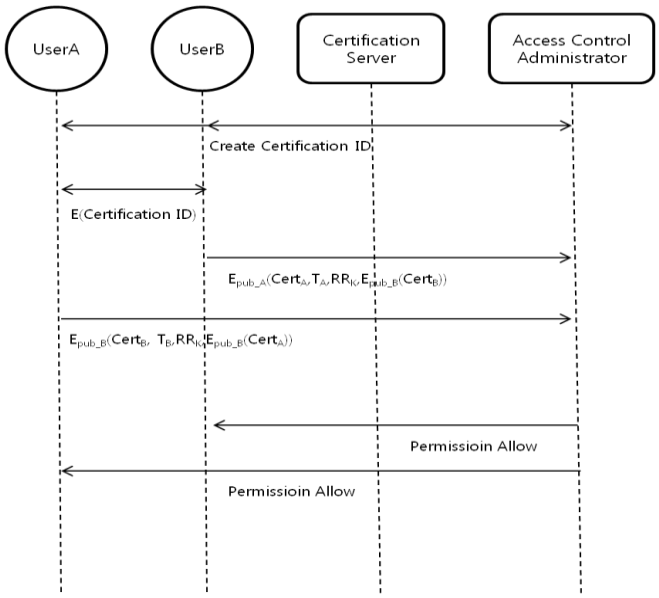

Fig. 2. Protocol for permission assignment

D. Protocol for Permission Delegation

In real world situation, delegation is occurred to give permissions to other user. There are several requirements for secure delegation. First, user can delegate permissions to other user in user-level. Second, delegation carries out after security administrator approve it within restrict scope. Third, delegation should prevent security problem such as separation of duty and information disclosure caused by user-level delegation.

We suggest delegation protocol that prevent security problem using NFC technique. NFC technique has limited broad cast range, but this can ensure other users presence in surrounding area. Proposed protocol is as follows.

Step 1: This step is as same as protocol assignment

Step 2: UserB encrypt his own Certification ID and request role R_N by his private key. And then, they send it to User A who have right to delegate permission [$User_B$: $E_{pri\_B}(Cert_B,R_N)$]->$User_A$]

Step 3: UserA decrypt encrypted message using userB's public key and validate user's identification.

Step 4: User A encrypt his own Certification ID, delegation role R_N,Timestamp T_A, delegation time $Time_R$ using his private key. And then, UserA send this encrypted message to UserB

Step 5: UserB encrypte his own Certification ID, Timestamp T_B including encrypted message that is sent from UserA. After then, UserB send this encrypted message to Access Control Administrator.

Step 6: Access Control Administrator decrypt encrypted message using stored each user's private key and validate user's identification. After then, Access control administrator decide to allow delegation by access control policy. Delegation is valid during delegation time that is defined in $Time_R$.

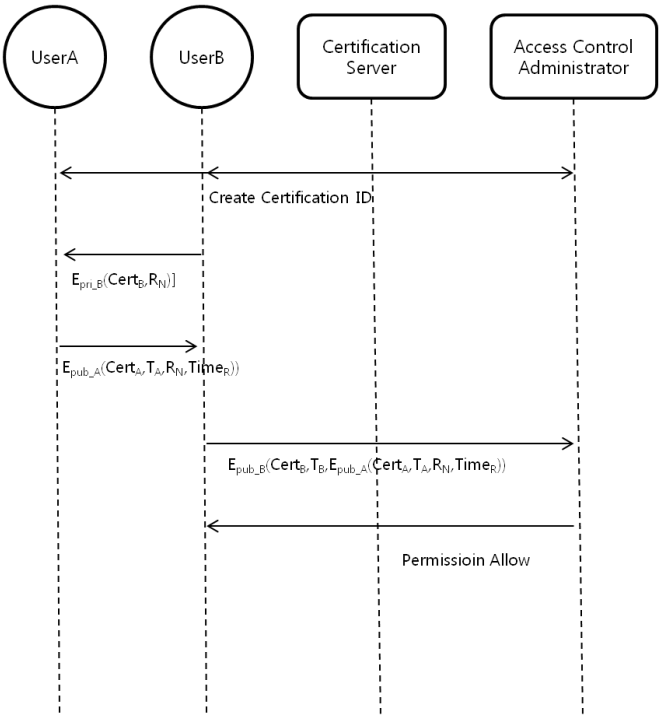

Fig. 3. Protocol for permission delegation

IV. Scenario

A. Permission Assignment in Hospital

Tom and Mike is a resident in hospital. They manage their own patients, but sometime they are cooperative to care certain patients. In this case, access request for that patient's information doesn't allow individually because patient's private information might be abused by Tom or Mike although they don't have authority about that. Using proposed access control model, we can control this situation. Tom and Mike exchange their Certification ID, and send request at the same time. Proposed access control model enforce to allow permission only related user's request is receive in access control administrator at the same time. If Tom and Mike's request is allowed, they can access patient's information during threshold time. Of course proposed access control cannot prevent security violation by conspiracy, but we assume that individual is more vulnerable than cooperative work.

B. Permission Delegation in Company

Alice is an employee in certain company and Ben is Alice's senior. Ben and Alice are cooperative for their task, and sometimes, Ben needs to delegate his permission to Alice. In this case, Ben should withdraw delegated permission after Alice complete her task that delegated permission is needed. If they don't do that, Alice might use her delegated permission maliciously. Existing access control model provide several way to manage this kind of problem, but it is inconvenient to use in real world. Proposed technique

improved usability and security. Alice request delegation to Ben and Ben delegate his permission using his NFC-enabled device. It is convenient to use because Ben can delegate his permission by touching his NFC-enabled device to Alice's NFC-enabled device. And NFC's limited bandwidth give a way to ensure other user presence in surrounding area. If Ben wants to withdraw his delegated permission, he touch again to Alice's device.

V. Analysis

A. Requirements Analysis

Existing context-aware access control model didn't consider relationship. Proposed access control model consider relationship among users as a context constraint. Our access control technique can satisfy real world organization's access control requirements, especially mobile office environment. We compare our access control model with existing RBAC and context-based access control model. Table I shows each access control technique's functionality evaluation measure. Our estimation is based on security measurements in [8]. As result shows that suggested technique can satisfy access control requirements including relationship based access control model.

TABLE I: Comparison of Existing Access Control Model

	RBAC	Context-aware RBAC	Relationship-based RBAC
Role-based permission assignment	O	O	O
Least privilege	O	O	O
Role hierarchy	O	O	O
Flexible permission assignment	X	O	O
Relation based access control	X	X	O
Group-level access control	X	X	O

B. Performance Analysis

If We assume that number of role is m, possible combination of role is m^n(n=number of combination). If m is huge or number of combination is increased, our access control model makes a burden to manage role and permission in organization. In addition to that, users have to contain other user's public key to authenticate other user's identification in proposed access control protocol. It also makes a cost to key management. That is why try to minimize this kind of side effect considering real world environment.

Fig. 4 is our access control model that extend traditional role-based access control model. In proposed technique, role is not directly mapped to permission. Role is mapped to task that consists of several roles. Task represents real world work and permission is mapped to task, and task share their permission with roles that has same tasks. As a result, role combination is occurred in task area. If we represent number of entire task is T and number of role that is included in task is R_t, possible number of role combinitaion is $T * R_t^{Rt}$. This is reasonable number of roles. And also, this modified access control model gives a way to manage partial delegation by role assignment to task.

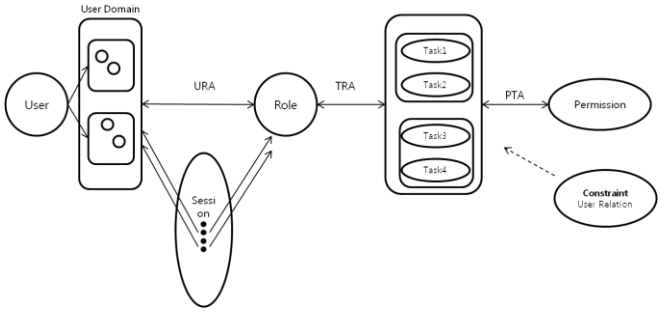

Fig. 4. Proposed access control model

And user is categorized by user domain that is defined by organization's department. Therefore user don't need to store whole user's public key. User just store other user's who is in the same department public key. It can reduce key management cost.

VI. Conclusion

In this paper, we propose a relationship-based access control model that consider relations among users as context information. Proposed technique can provide fine-grained and secure access control for cooperative work in mobile office environment. And also, we use NFC technique to improve usability and security. Proposed technique makes an additional cost to manage user's relationship. We try to reduce additional burden by classifying user group and task.

In the future, we implement prototype of our access control model and establish security measurements. And also we extend our access control model to distributed user-level access control model.

Acknowledgment

This research was supported by the MKE(The Ministry of Knowledge Economy), Korea, under the ITRC(Information Technology Research Center) support program supervised by the NIPA(National IT Industry Promotion Agency"(NIPA-2012-(H0301-12-3004)))

References

[1] M. J. Covington, W. D. Long, S. Srinivasan, A. Dey, M. Ahamad, and G. Abowd, "Securing context-aware applications using environment roles," in *Proc. 6th ACM Symposium on Access Control Models and Technologies*, Chantilly, VA, USA, pp. 10-20, 2001.

[2] E. Bertino, P. A. Bonatti, and E. Ferrari, "TRBAC: a temporal role-based access control model," in *Proc. 5th ACM Workshop on Role-Based Access Control*, Berlin, Germany, pp. 21-30, 2000.

[3] J. B. D. Joshi, E. Bertino, U. Latif, and A. Ghafoor, "A generalized temporal role-based access control model," *IEEE Trans. on Knowledge and Data Engineering*, vol.17, pp.4-23, January 2005.

[4] E. Bertino, B. Catania, M. L. Damiani, and P. Perlasca, "GEO-RBAC: A spatially aware RBAC," in *Proc. 10th ACM Symposium on Access Control Models and Technologies*, Stockholm, Sweden, pp. 29-37, 2005.
[5] P. Fong, M. Anwar, and Z. Zhao, "A privacy preservation model for Facebook-style social network systems," in *Proc. 14th European Symposium on Research in Computer Security*, Saint Malo, France, pp. 303-320, 2009.
[6] P. W. Fong, "Relationship-based access control: protection model and policy language," in *Proc. 3rd ACM Conference on Data and Application Security and Privacy*, San Antonio, TX, USA, pp.191-202, 2011.
[7] B. Carminati, E. Ferrari, R. Heatherly, M. Kantarcioglu, and B. Thuraisingham, "Semantic web-based social network access control," *The Trans. Computers and Security*, vol. 30, pp. 108-115, March 2011.
[8] S. Oh and S. Park, "Task-role-based access control model," *The Trans. on Information System*s, vol. 28, pp. 533-562, September 2003.

Kangsoo Jung is a Ph. D candidate of Department of Computer Science and Engineering at Sogang University from 2009. He received the M. S. degree in Computer Science and Engineering from Sogang University, Seoul, Korea in 2007 and 2009. His major research areas are role-based access control model, privacy.

Seog Park is a Professor of Computer Science and Engineering at Sogang University. He received the B.S. degree in Computer Science from Seoul National University in 1978, the M.S. and the Ph.D. degrees in Computer Science from Korea Advanced Institute of Science and Technology (KAIST) in 1980 and 1983, respectively. Since 1983, he has been working in the Department of Computer Science and Engineering, Sogang University. His major research areas are database security, real-time systems, data warehouse,digital library, multimedia database systems, role-based access control and web database. He is a member of the IEEE Computer Society, ACM and the Korean Institute of Information Scientists and Engineers (KIISE).