A Trust Management Model for PACS-Grid

Hyun-Sook Cho, Bong-Hwan Lee*, Kyu-Won Lee and Hyoung Lee, *Member, KIMICS*

Abstract—Grid technologies make it possible for IT resources to be shared across organizational and security domains. The traditional identity-based access control mechanisms are unscalable and difficult to manage. Thus, we propose the FAS (Federation Agent Server) model which is composed of three modules: Certificate Conversion Module (CCM), Role Decision Module (RDM), and Authorization Decision Module (ADM). The proposed FAS model is an extended Role-Based Access Control (RBAC) model which provides resource access capabilities based on roles assigned to the users. FAS can solve the problem of assigning multiple identities to a shared local name in grid-map file and mapping the remote entity's identity to a local name manually.

Index Terms— Trust Management, Grid, Security

I. INTRODUCTION

Security is crucial for the successful deployment of large distributed systems. Many of these systems provide services to people across different administrative domains. The traditional identity-based access control mechanisms are unscalable and difficult to manage. Unlike the closed systems, open systems provide services to people from different security domains. It is often impossible or unnecessary to know the identities of users in these systems. What really count are the roles or attributes of the principals. This observation directly implies a requirement for a new trust model based on the attributes or roles of entities on the distributed systems. This new scheme is called trust management systems aiming to solve the trust problems based on attributes. In these systems, strangers can gradually establish trust by iteratively exchanging information with each other. The basic functionality of these systems is to decide whether to allow or deny a resource request after a series of exchanges of credentials and policies between the service requestor and the server.

Trust management is a new research area. Trust as a concept has a variety of applications, which causes divergence in trust management terminology. Trust management research has its roots in authentication and authorization. In the context of authentication, trust is established by means of digital certificates. The certificates are proof of either identity directly or membership in a group of good reputation. Authentication-related trust is discussed in [1, 2]. Credential-based authentication and authorization systems fall into three different groups:

- Identity-based systems
- Property-based systems
- Capability-based systems

Identity-based systems such as X.509 [3, 4] authenticate using an entity's identity or name. However, identity is not a useful basis for establishing trust among strangers. Property-based credentials have emerged to manage trust in decentralized and distributed systems [5, 6]. In this scheme, the access control policy evaluation engine retrieves the certificates among multiple, distributed stakeholders to share control over access to resources. Capability-based systems manage delegation of authority for a particular application. These systems are not designed to establish trust between strangers since clients are assumed to possess credentials that represent authorization of specific actions with the application server. In the KeyNote system [7], polices delegate authority on behalf of the associated application to otherwise untrusted parties.

In this paper, we have extended the features of the KeyNote system, and applied the proposed scheme to the PACS-Grid as a target application. KeyNote credentials express delegation in terms of actions that are relevant to a given application. The proposed trust model makes use of the KeyNote's idea in the sense that authorization is directly embedded into the certificates.

The rest of this paper is organized as follows. The background and related work is summarized in Section 2. Section 3 describes implementation of the proposed a trust management model for PACS-Grid. Conclusions are presented in Section 4.

II. RELATED WORKS

A. Trust Management

Trust management was first introduced by Matt Blaze et al. in the PolicyMaker system [8] to denote a distinct component of security in network services. In PolicyMaker system, the aspects of formulating security

Manuscript received May 21, 2007.

Asterisk indicates corresponding author.

The authors are with the Department of Information and Communications Eng., Daejeon University, Daejeon, Korea (Tel: +82-42-280-2553, e-mail: blee@dju.ac.kr)

policies and security credentials are considered to determine whether particular sets of credentials satisfy the relevant policies or defer trust to third parties. Later on many researchers looked into different aspects of the problem. Different credential formats have been proposed and implemented and different policy languages have been proposed and verified in real applications. Trust negotiation theories have been developed and dozens of negotiation strategies and protocols have been proposed. Regardless of the complexity and sophistication of the system, the general structure and elements fall into the same category. The basic elements of the trust management system are described in Fig. 1.

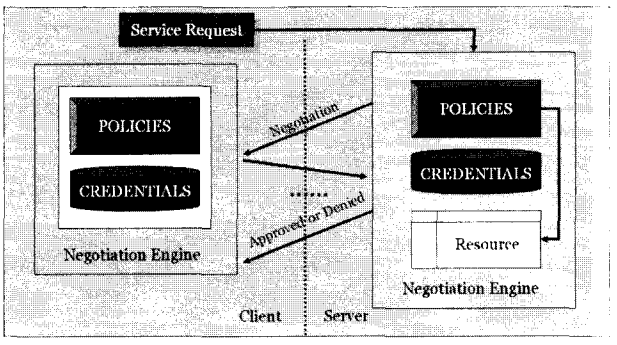


Fig. 1 Elements of the Trust Management System

The client is an entity that issues a request to access the resource on the server. The client could be any entity such as process acting on behalf of the user or a Web service itself, while the server is an entity that owns the resources. The digital credentials contain the assertions of attribute information of the entity, and generally they are certificates issued by certificates authorities describing the attributes or roles of the entity. They could also be delegated from other entities. The credentials are normally digitally signed by the certificate authority's private key and could be verified by its public key. The credentials stored in both the clients and the servers represent the attributes of the client and the server, respectively. The credentials could contain sensitive information and the owner may only want to disclose them after they trust the other party to a certain degree. The policies are defined to govern the access to the credentials in the client, and both the credentials and the resources in the server. They are specified in a policy language and a certain combination of credentials is required to access a certain resource. When the client issues a request to access resources on the server, this request is intercepted by a server module. The negotiation engine checks the request and the local policies first and returns certain policies and credentials to the client. When the client negotiation engine receives the message, it verifies the credentials, checks against the local policies, and sends another message containing the policies and a set of credentials to the server. The process repeats until the service request is approved or denied.

B. PACS-Grid

Grid is being introduced in many applications including medical applications. Introducing Grid technology in healthcare applications opens up new possibilities in the medical domain. Medical applications are of the most demanding multimedia applications which require large data storage, high processing capabilities, and strong security. Grid technology provides various features of the medical data processing including workflow, load balancing, and security policies. Grid technology can be used in medical applications such as the Picture Archive and Communication System (PACS). The application of the Grid technology to PACS gives rise to PACS-Grid system. For example, DICOM (Digital Imaging and Communications in Medicine) Services Grid software [9] which delivers image management features and performance has been introduced. Also "A Data Grid" [10] specifically designed for clinical image backup and disaster recovery has been developed at the IPI (Image Processing & Informatics) Laboratory, USC using the Globus Toolkit 4.0. This Data Grid was designed to utilize the strengths of Grid technology along with PACS/DICOM technology for storing and distributing clinical images. PACS/DICOM resources are embedded within the five layer Grid computing architecture: Fabric, Connectivity, Resource, Collective, and Applications as shown in Fig. 2.

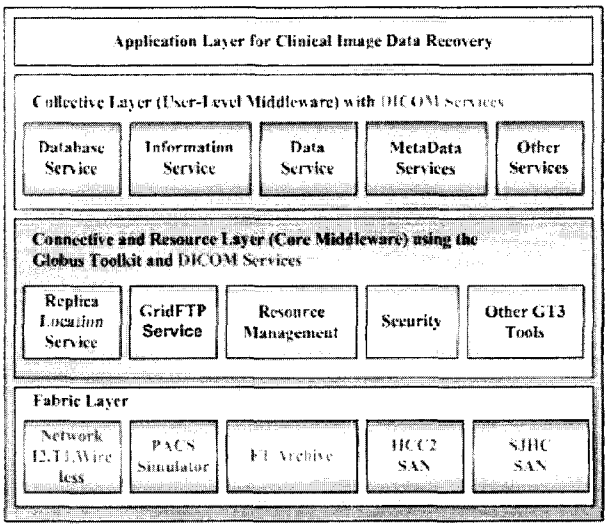


Fig. 2 Architecture of the DataGrid [10]

C. Grid Security Infrastructure (GSI)

In 1997, the Globus Project introduced an implementation of GSS-API called the Grid Security Infrastructure (GSI). This implementation uses public key protocols for use in programming Grid applications [11] such as applications run in dynamic inter-domain distributed computing environments. GSI is an implementation of the Java Generic Security Services Application Service Interface (GSS-API). GSS is used for securely exchanging messages between communicat-

ing applications, and it offers uniform access to security services on top of a variety of underlying security mechanisms such as Kerberos. It also provides single sign-on (SSO), delegation abilities for Grid users, and facilities for authentication (i.e. verifying the identity of a Grid entity) and authorization. GSI implements standards from various standards bodies and specifications from the Web services community to provide the fundamental security needs.

The primary motivations behind GSI are:

- The need for secure communication between elements of a Grid.
- The need to support security across organizational boundaries, thus prohibiting a centrally-managed security system.
- The need to support "single sign-on" for users of the Grid, including delegation of credentials for computations that involve multiple re-sources and/or sites.

The GSI process can be divided into two different steps: authentication and authorization. These two actions are often lumped together, but understanding the difference is at the heart of the GSI. Fig. 3 shows the GSI authentication and authorization processes. The authorization needs to be modified to apply for the PACS-Grid system.

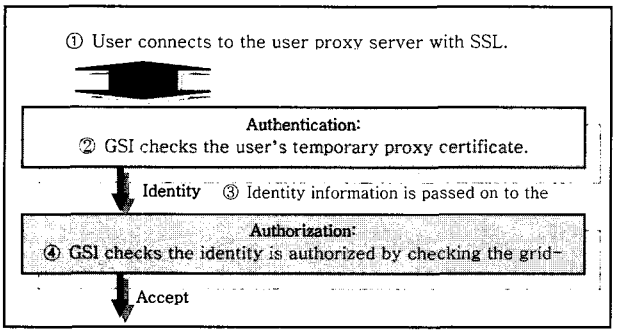


Fig. 3 GSI authentication and authorization process

Authentication is an act of one party proving its identity to another. In GSI this is accomplished using the SSL protocol with mutual authentication, where both sides prove their identity to the other. Note that a user authentication to a resource doesn't grant them any access. After a user is authenticated, the GSI then checks to verify the user for the authorization to use the resource. The SSL protocol enforces a simple trust management scheme in that only users whose X.509 certificates are signed by the known CA's are allowed to connect via the SSL protocol. GSI expands this idea by adding a CA signing policy file for each CA that specifies the namespace in which it may issue names. In GSI the only Grid level authorization rules are in the "grid map" file [12], which maps a Grid DN to a local user account.

III. TRUST MANAGEMENT MODEL FOR PACS-GRID

A. Problem of grid-map file

Once users have been authenticated to a system and proven their GSI identity to the system, they must be authorized before gaining any access to the resources. Authorization is the act of deciding if the authenticated party is allowed to access a resource. The grid-map file is a plain text file containing a list of authorized GSI identities and mappings from GSI identities to local user identities. Thus it is both an access control list and a mapping mechanism. Entries are added to the grid-map file by the local system administrator when a user who presents his or her GSI identity to the administrator. The administrator then determines what the local account name is for the user and adds this mapping to the grid-map file. In other words, the system administrators must manage the updating of each node's grid-map file to stay current with local Grid user. The grid-map file first checks to see if the user's Grid identity is listed in the grid-map file. If a user is not listed, he or she is denied to access to the resource. If a user is listed in the grid-map file, the GSI gets the name of the local user account from the grid-map file, changes incoming user's identity to the local identity and then runs the task requested by the user. Each subject name in the grid-map file must be listed only once. However, multiple identities can be mapped to a single shared local name.

The "Community Authorization Server" (CAS) [13, 14] is a system developed by the Globus Project to allow virtual organizations to flexibly authorize access to resources and data in large distributed Grids. Even in CAS system, multiple identities can be mapped to a shared local name. This is a critical problem in PACS-Grid domain because if a user has a strong access authority, he or she can modify or delete the resources. In that case, the administrator has to analyze the system and find who has committed the undesirable action. Moreover, the grid-map file doesn't have any mechanism for roles, groups and any other user peculiarity supported.

Therefore, we propose the FAS (Federation Agent Server) model to solve the problems of the grid map-files described above. The identified problems can be categorized into three parts: allocating multiple identities to a shared local name, mapping by the administrator manually, user's properties and roles problem.

B. Federation Agent Server (FAS) Model

As discussed above, authorization in GSI is commonly based on identity credentials and access control lists (i.e. grid-map files). However, recent work applied authorization credentials and authorization policy management techniques to Grid computing [13, 14, 15, 16]. CAS and Shibboleth [15] uses the idea of federation for group objects with similar properties (e.g. roles). The concept of federation can be applied to identification and authorization to solve a wider range of security issues. It may be useful to define a Grid under these circumstances as a temporary binding between a federation of users and

one or more federations of resource providers to deliver an agreed set of services.

CAS and Virtual Organization Membership Service (VOMS) [16] each embed authorization credentials in GSI proxy credentials to enable transport of authorization credentials in existing GSI authentication protocols. CAS embeds signed SAML policy assertions in GSI proxy credentials, encoding specific rights such as read and/or write access to files served by a GridFTP server. VOMS also embeds attribute certificates in GSI proxy credentials that specify group and virtual organization membership for access to community resources. However, CAS uses whole new proxy certificates with the CAS server Distinguish Name as the subject. This means that existing services in Globus-based Grids would need to be modified to use a CAS certificate. In CAS, both groups and roles are not considered, but only permissions. VOMS has been developed on a completely new basis to sustain the burden of a potentially high number of complex queries. However, PACS-Grid system doesn't require the whole features of CAS and VOMS. Thus, we have proposed a Federation Agent Server (FAS) model that embeds authorization in GSI proxy credentials using three modules: CCM, RDM, and ADM. The FAS is based on a very simple policy and makes use of a user-Group table connecting to grid-map file.

The proposed FAS model is an extended version of the Role-Based Access Control (RBAC) model, in which resource access is associated with roles and roles are assigned to the users. The existing authentication scheme described in Section 2.2 related to the first step of GSI has been used. In order to solve the authorization problem the FAS model is proposed in this paper. The FAS model is composed of three different modules:

- Certificates Conversion Module (CCM): converts proxy certificate to XML format.
- Role Decision Module (RDM): decides roles and capabilities of the user based on the proxy credential and local site policy.
- Authorization Decision Module (ADM): decides authorization of user who requests a specific local PACS resource and attaches user's authorization to CCM.

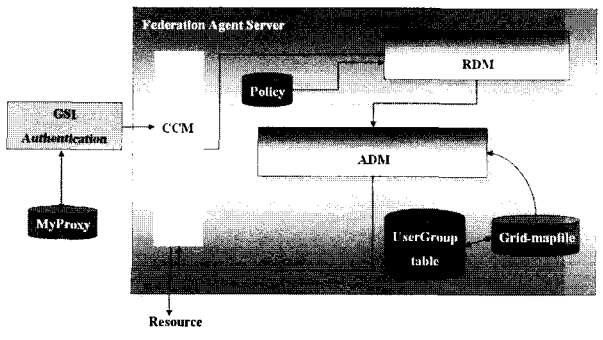


Fig. 4 Structure of the Federation Agent Server

Once the FAS model is executed, user's proxy credential contains user's authorization based on role and converted into the XML format. Then user can access to re-sources with an associated specific role in PACS-Grid. Figure 4 shows the overall architecture of the FAS.

We use the MyProxy [17] as a user Proxy which provides a centralized certificate repository with advanced features such as certificate renewal. The detailed features of the three modules are described as follows:

1) Certificates Conversion Module (CCM)

The first step of FAS is to convert user proxy certificates into XML format. The CCM allows user to easily operate Globus or Web services commands. The policy provides the rules for mapping an entity to a group. It also provides the rules that determine whether or not a certificate owner is a member of a certain group. In PACS, supposed that a user belongs to a specific hospital group and doctor group. Then the user can be recognized as a member of the doctor group if he or she has a certificate from the hospital. The policy would be written in XML format. The policy maps entities to groups or roles and defines the rules for each group.

2) Role Decision Module (RDM)

The RDM decides the users' roles based on their certificates and a local PACS-Grid policy. It extends traditional RBAC systems by adding authorization and mapping function of the certificate owner to a role. RDM does not provide the actual access control decision, but rather decides who belongs to which groups. The current version of RDM implements three roles and will be extended to provide more specific roles.

- *public role*: allows a limited level of access to PACS resources. (it can be a "patient" role)
- *user role*: allows regular level of access to all services of PACS.(it can be a "nurse" role)
- *superUser role*: allows advanced level of access to all services of PACS. Additionally it has additional computational or data management capabilities.(it can be a "doctor" role)

RDM is based on the role of the user, not the user itself. Thus, grid map-files update is not needed anymore in order to add or delete users.

3)Authorization Decision Module (ADM)

Once the specific role is decided in RDM, the ADM checks the grid-map file and assigns the local user identity to associated role in user group table. To select a local user identity not assigned to anyone, if a local user identity is assigned to a remote user, ADM removes the local user identity from the userGroup table. In this case the grid-map file does not need to be updated and the Globus container also doesn't need to be restarted. On the other hand, if all user identities are assigned already,

ADM creates a new identity with a proper authority. In this case, the grid-map file and Globus container should be updated, respectively.

Figure 5 illustrates how user/requestor can get authorization of PACS-Grid using FAS model.

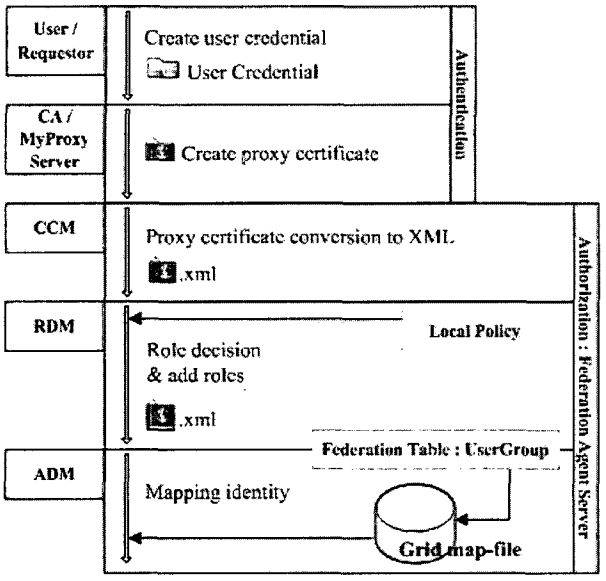


Fig. 5 The process of the FAS model

The FAS model works in automatic fashion. Thus, PACS-Grid user doesn't need to understand GSI architecture, look up grid-map file, and allocate role to access Grid resources.

IV. CONCLUSIONS

For regional or national health systems, Grid technology opens up the possibility of building extremely scalable and affordable shared storage infrastructures for managing huge volumes of medical information. The current GSI model does not provide a complete security process for authentication and authorization in an end-to-end fashion. Moreover, the current Grid security model requires the user to handle GSI components, which may vary between administrative domains.

We proposed a FAS model which composed of three modules: Certificate Conversion Module (CCM), Role Decision Module (RDM), and ADM (Authorization Decision Module). The FAS leverages MyProxy for the certificate storage and grid-map file for mapping users. The FAS model provides automatic execution for assigning authorization to users who do not understand what exactly GSI works. In addition, the FAS can assign roles to users using one-to-one mapping procedure for local PACS-Grid.

ACKNOWLEDGMENT

This research was supported by Korea Industrial Technology Foundation (KOTEF) through the Human Resource Training Project for Regional Innovation. It was also supported in part by the MIC(Ministry of Information and Communication), Korea, under the ITRC support program supervised by the IITA(Institute of Information Technology Advancement)" (IITA-2006-(C1090-0603-0014)).

REFERENCES

[1] Djordjevic, I., Dimitrakos, T., "Towards dynamic security perimeters for virtual collaborative networks," In: Trust Management: Second International Conference, iTrust, Oxford, UK, March 29–April 1, 2004.

[2] Winsborough, W.H., Seamons, K.E., Jones, V.E., "Automated trust negotiation," In DARPA Information Survivability Conference and Exposition, 2000, DISCEX Proceedings, Volume 1, IEEE, pages 88–102, 2000.

[3] Tuecke, S., et al., "Internet X.509 Public Key Infrastructure Proxy Certificate Pro-file", IETF, 2003.

[4] Sean Turner, Alfred Arsenault, "X.509 Public Key Infrastructure," IETF 2002.

[5] Hertzberg, A., Mihaeli. J., Mass,Y., Naor,D., and David, Y., "Access Control Meets Public Key Infrastructure, Or "Assigning Roles to Strangers," In IEEE Symposium on Security and Privacy, Oakland, CA, 2000.

[6] Johnson, W., Mudumbai,S., and Thompson, M, "Authorization and Attribute Certificates for Widely Distributed Access Control," In IEEE International Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises, 1998.

[7] Blaze, M., FEIGENBAUM, J., and KEROMYTIS, A. D. "KeyNote: Trust Management for Public-Key Infrastructures," In Security Protocols Workshop, Cam-bridge, UK, 1998.

[8] Matt Blaze, Joan Feigenbaum, Jack Lacy, "Decentralized Trust Management," In IEEE conference on Security and Privacy, Oakland, CA, May 1998.

[9] http://www.acuotech.com/home.html

[10] Huang HK, Brent J, Liu, Zheng Zhou, Jorge Documet, "A Data Grid Model for Combining Teleradiology and PACS Operations," In Med Imag Tech, 2006.

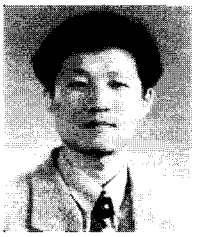
[11] Foster, I., C. Kesselman, and S. Tuecke, "The Anatomy of the Grid: Enabling Scalable Virtual Organizations," International Journal of Supercomputer Applications, 2001.

[12] The Globus Security Team, "Globus Toolkit Version 4 Grid Security Infrastructure: A Standards Perspective," September 12, 2005.

[13] L. Pearlman, C. Kesselman, V.Welch, I. Foster, and S. Tuecke, "The community authorization service: Status and future," In Proceedings of the Conference for Computing in High Energy and Nuclear Physics, La Jolla, California, USA, Mar. 2003.
[14] L Pearlman, et al., "A Community Authorization Service for Group Collaboration," In Proceedings of the IEEE 3rd International Workshop on Policies for Distributed Systems and Networks, 2002.
[15] M Erdos and S Cantor, "Shibboleth Architecture," Internet2, October 8, 2001.
[16] R. Alfieri, R. Cecchini, V. Ciaschini, L. dell'Agnello, A. Frohner, A. Gianoli, K. L'orentey, and F. Spataro, "Voms: An authorization system for virtual organizations," In Proceedings of the 1st European across Grids Conference, Santiago de Compostela, Feb., 2003.
[17] Novotny, J., S. Tuecke, and V. Welch., "An Online Credential Repository for the Grid: MyProxy," In High Performance Distributed Computing (HPDC), 2001.

Hyun-Sook Cho
received a BS degree in mathematics in 1995, an MS degree in information and communications engineering from Daejeon University, Dejeon, Korea, in 2001, respectively. She is currently a Ph.D. candidate in Department of information and communications engineering of Daejeon University. Since 2006 she has been with Center of Education Development of Daejeon University as a fulltime instructor. Her research interests include Trust management, Grid middleware, Web Services, and network security.

Bong-Hwan Lee
received a BS degree in electronics engineering from Sogang University, Seoul, Korea, in 1985, an MS degree in electronics engineering from Yonsei University, Seoul, Korea, in 1987. He also received a Ph.D. degree in electrical engineering from Texas A&M University, USA, in 1993. From 1993 to 1995 he was with Korea Telecom (KT) as a research engineer in the broadband networks group and engaged in research on multimedia services. Since 1995 he has been a professor at Daejeon University, Daejeon, Korea. His current research interests include Grid middleware, Web Services, and network security.



Kyu-Won Lee
received the B.S. M.S and Ph.D degrees in electronics engineering from Yonsei University, Seoul, Korea, in 1986, 1988 and 1998, respectively. From 1988 to 1989, he was with LG Industrial System Laboratory, Anyang, Korea, where he was involved in development of vision inspection system. He joined ETRI (Electronics and Telecommunications Research Institute), Daejeon, Korea, in 1989 and was involved in development of the Packet Exchange System and MPEG-7 technologies. Especially, he contributed many proposals on video motion analysis to MPEG-7. Since 2000, he has been with Daejeon University, Daejeon, Korea, where he is currently Associate Professor of Information and Communications Eng. Department. His research interests include active vision, motion analysis, image processing, multimedia, 3-D computer vision and content-based image and video searching.

Hyoung Lee
received a BS degree in mathematics from Seoul National University, Seoul, Korea, in 1964, an MS degree in electrical engineering from Sungkyunkwan University, Seoul, Korea, in 1971. He also received a Ph.D. degree in electrical engineering from Chosun University, Korea, in 1992. Since 2001 he has been serving as a president of the Korea Society of Information Technology Applications (KITA). Currently he is with Department of Information and Communications Engineering of Daejeon University, Daejeon, Korea, as a professor. His current research interests include trust management, computer graphics, and image processing.