Single Sign-On Scheme using XML for Multimedia Device Control in Children's Game Network based on OSGi service Platform

Dongkyoo Shin and Dongil Shin

Department of Computer Engineering, Sejong University
98 Gunja-Dong, Gwangjin-Gu, Seoul 143-747, Korea
{shindk, dshin}@sejong.ac.kr

Abstract

This paper proposes a single sign-on scheme in which a user offers his credential information to children's game network running the OSGi (Open Service Gateway Initiative) service platform, to obtain user authentication and control a remote device through a mobile device using this authentication scheme, based on SAML (Security Assertion Markup Language). By defining the single sign-on profile to overcome the handicap of the low computing and memory capability of the mobile device, we provide a clue to applying automated user authentication to control a remote device using a mobile device for distributed mobile environments including children's game network based on OSGi.

Keywords: *single sign-on, SAML, home network service environment, OSGi, device control, children's game network*

1. Introduction

Children's game network is based on the home network service environment which consists of different kinds of personal equipment, wireless sensors, middlewares, services, and networked devices [1]. In this environment, middlewares such as UPnP (Universal Plug in Plug) [2], Jini [3], Havi [4], PLC (Power Line Community) [5] play an important role controlling and maintaining a variety of network component. However, middlewares are not interoperable because each one is dependent on vendors who establish middleware. OSGi (Open Service Gateway Initiative) [6] provides the key to solve such problem. By providing transparent layer on which each middleware can communicate OSGi enables middlewares to be interoperable.

In the OSGi service platform, every service bundle in the gateway operator requires user authentication. By the result, a user should complete authentication repeatedly whenever the user wants to access several number of services. This causes potential security problems as well as the difficulty of user access.

First of all, the main security problem with a home network environment including children's game network based-on the OSGi service platform is that the security infrastructure is distributed and these architectures usually require that key security features be built into all parts of the system. In addition, a user must memorize usernames and passwords for each service. Additionally, the system's administrator manages many passwords in the database and is faced with potential insecure system problems due to the frequent transmission of these passwords at the sites [7]. SSO (Single Sign-On) is a good alternative to solve these problems. SSO is a security feature that allows a user to log into the many different services offered by the distributed systems while only needing to provide authentication once, or at least always in the same way [8].

In this paper, we propose a single sign-on scheme using SAML (Security Assertion Markup Language) for home network service environment including children’s game network based on the OSGi service platform. We simulated this environment by proposing and verifying a messaging scenario through implementation, and defined a profile to implement SSO through mobile devices with small memory capacities in distributed OSGi environments, which should exchange and verify a key to authenticate a user.

2. Background

Mobile devices open up the possibility of offering home network services regardless of a user's or service provider's location. But the handicaps of mobile devices become the barriers to adopting new security technologies, such as single sign on, in mobile or home network service environments [9]. To overcome these barriers, a lightweight method to avoid key-exchange and message encrypting/decrypting must be considered for a mobile device.

A user in a wide area network can control a remote device within a home network environment via a service bundle in a gateway operator. To use the service bundle, the user's authentication is necessary. For this functionality, Release 4 of the OSGi service platform defines a "User Admin Service" but only offers authentication for each service unit [10]. For this reason, when a user wants to access various services, a home network environment using the OSGi service platform may have the same primary security problem experienced in a mobile or Web Services environment. SSO can be implemented by exchanging and reusing a user's authentication information, including the fact that the user has previously been authenticated by a specific method among different security domains. We specified the information in a uniform and unified way based on SAML.

2.1. OSGi (Open Service Gateway Initiative) framework

OSGi was developed to control and manage services and devices in homes, offices, vehicles, mobiles, and other environments via network and its final goal is to solve problems involving service distribution and the interaction between several home network middlewares [6].

The OSGi service platform is divided into two parts: the OSGi Service Framework and OSGi Service. The OSGi framework supports registry and life-cycle management for an OSGi service in Java runtime environment. As a bundle, an OSGi service such as HTTP, Logging, and Device Access Service is defined by Java Interface. A bundle is the minimum unit for managing a framework. A framework manages installing, uninstalling, resolving, stopping, starting, and active life cycle for bundle.

Figure 1 shows the OSGi framework, which connects the wide area network and the local area network. When a user wants to control a device in the local area network, he can control the device through the service being managed by the gateway operator in the wide area network. If there is a trust-relationship between the services, a user who has been authenticated from a service in the gateway operator can avoid any redundant authentication required to use other services.

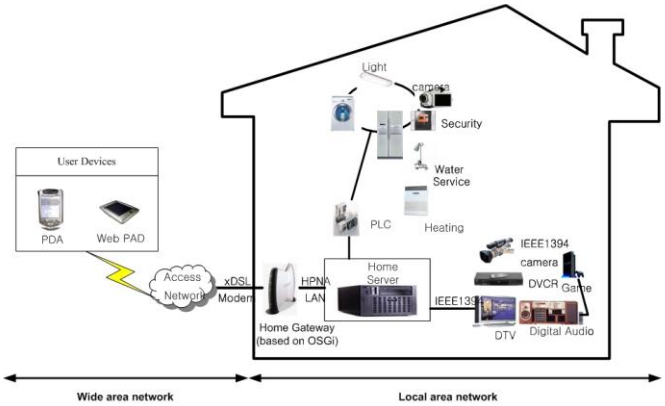


Figure 1. The OSGi Architecture

In order to apply the SSO scheme to the home network as shown in Figure 1, the services extended from core services provided by the OSGi framework should be developed and deployed onto the OSGi framework. Figure 2 shows core services provided by the OSGi framework and extended services.

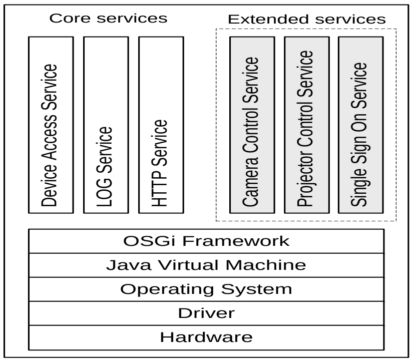


Figure 2. OSGi framework and extended services

The description for core services is as follows [11]:

- Device Access Services enables an operator to update, install, or remove device drivers.
- LOG Service gives users a general-purpose message logger for the OSGi environment.
- HTTP Service offers users' access to services on the Internet and other networks..

For experimental purposes, we implemented following extended services:

- Camera Control Service provides functionality for controlling a surveillance camera to read children’s face , such as camera view, camera on/off, and camera zoom in/out.
- Projector Control Service provides functionality for controlling a projector in a conference room or meeting room to show digital contents for children, such as projector on/off and adjusting.

- Single Sign On Service makes XML-based queries for user authentication. Also it plays the role of exchanging artifacts between the user and an Authentication Agent. After authenticating the user successfully, it leads the user to the destination service.

2.2. SAML (Security Assertion Markup Language)

Using a subset of XML, SAML defines the request-response protocol by which systems accept or reject subjects based on assertions [12]. An assertion is a declaration of a certain fact about a subject. An assertion includes the statements generated by the SAML authority, conveying them and verifying that they are true. SAML defines three types of assertions.

- AuthenticationAssertion: indicating that a subject was authenticated previously by some means, such as a password, hardware token, or X.509 public key.
- AttributeAssertion: indicating that the subject is associated with attributes.
- AuthorizationAssertion: indicating that a subject should be granted or denied resource access.

The SAML authority can be classified as authentication authorities, attribute authorities, and policy decision points according to the type of assertions included. The SAML authority can use various sources of information from external policy stores or assertions being received as the input in requests.

SAML defines an artifact mechanism when the authentication request is too long for an HTTP redirect. The artifact has the role of a token. It is created within a security domain and sent to other security domains for user authentication. To achieve single sign-on, a mobile device keeps its artifact, which verifies that the mobile user has been authenticated once by the SAML authority in the system. An artifact is a small string and keeping it in the mobile device can overcome the handicap of having low computing power and a small memory in the mobile device.

3. Single Sign-On architecture for ubiquitous home network service environment

The role of a security domain is to manage and control resources ruled by a specific access control policy. When a subject within a security domain requests resource from another security domain, the subject must be defined in the first security domain and a mutual trust-relationship must exist between the first security domain and the second security domain [13]. Specifically, OSGi recommends the HTTP service to offer users access to the services on the Internet and other networks [14]. Therefore we strongly suggest SSO as a core security scheme to improve user accessibility and security performance in home network environments exploiting the HTTP service.

Two approaches can be considered for implementing SSO [15, 16].

- The first approach is to maintain an authentication list for all users in a central repository.
- The second approach is to include authentication information for each Web service in the initial SOAP(Simple Object Access Protocol) message..

In the first approach, all the old IDs for users are removed and then new IDs are assigned from the central repository [15]. To access services, a user must use a new ID. This approach is suitable for a single organization with many branches, each branches may lose its control for the administration because all the users' information is stored into the central repository. This approach may not be appropriate for distributed environments made up of Web services, which are a set of domain-specific services.

In the second approach, all users can use the existing ID to access different domains without needing a new ID [15, 16]. This approach is suitable for a distributed environment that is a set of domain-dependent distributed services, as illustrated in Figure 3. In this environment, when a user wants a number of domains, each domain requests the user to provide authentication. Then the user is authenticated by a domain and his authentication information is attached to a message to be transferred to other domains. Using this approach, attaching authentication information to the message and transferring the message to other domains, none of the organizations need to change their peculiar authentication scheme in order to communicate with other organizations.

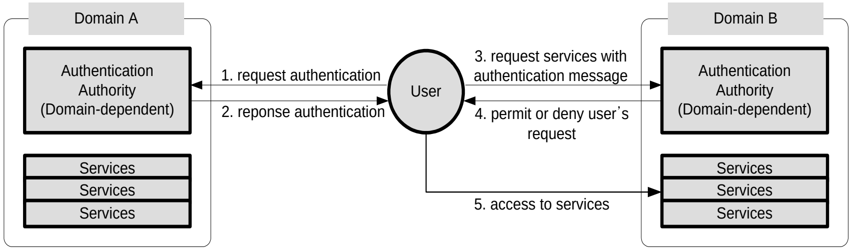

Domain A
Authentication Authority (Domain-dependent)
Services
Services
Services
1. request authentication
2. reponse authentication
User
3. request services with authentication message
4. permit or deny user`s request
5. access to services
Domain B
Authentication Authority (Domain-dependent)
Services
Services
Services

Figure 3. An approach to implementing Single Sign-On using attached authentication message

The second approach is more appropriate for a home network service environment in which all services require user authentication.

The concept of the proposed Single Sign-On architecture is shown in Fig. 4, in which the OSGi delivers certain services offered by service providers to the end user regardless of the system environments. In our implementation, a mobile user gains access to services being managed by a gateway operator with the SAML-based information related to his own authentication in order to control a remote camera and projector. A mobile user keys in his username and password to a mobile device in order to access the Camera Control Service in the gateway operator of the Wide Area Network. This user credential information is transferred to the SSO Service through the gateway operator, which connects the mobile device and Wide Area Network.

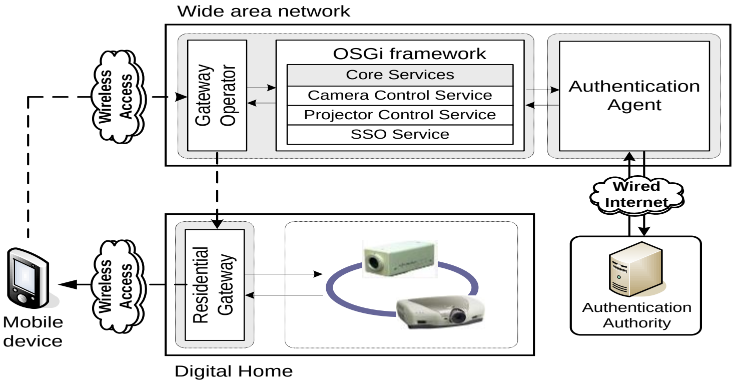


Figure 4. Proposed Single Sign-On Scheme

The user authentication procedure for the architecture is presented in the form of a sequence diagram in Figure 5, where each box in the diagram denotes an entity involved in this process. Figure 5 explains the messages between entities applying a user's single sign-on among services, in which there are mutual trust relationships.

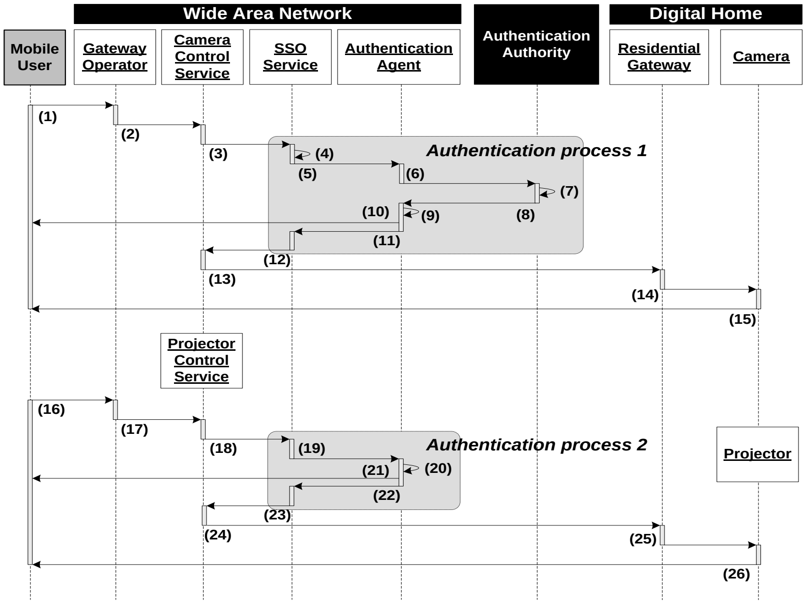


Figure 5. Sequence Diagram of the Proposed Single Sign-on Architecture

A description of each step is as follows:

(1) The mobile user keys his name and password into his mobile device in order to access the Camera Control Service via the gateway operator.

(2) The gateway operator transfers the user's credential information to the Camera Control Service. When the user's password is transmitted, the password must be encrypted.

(3) The Camera Control Service requests user authentication from the SSO Service, providing the user's credential information.

(4) The SSO Service makes a SAML-based authentication query and signs it digitally to be trusted by the Authentication Authority.

(5) The SSO Service sends the signed authentication query to the Authentication Agent.

(6) The Authentication Agent requests user authentication from the Authentication Authority.

(7) The Authentication Authority verifies the signed authentication query, decrypts the user's password, authenticates the user, makes an authentication assertion, and signs it digitally.

(8) The Authentication Authority sends this signed authentication assertion to the Authentication Agent.

(9) The Authentication Agent verifies the signed authentication assertion, evaluates it, and signs the evaluated result digitally. If the result is valid, the Authentication Agent generates an artifact for the mobile user.

(10) The artifact is assigned to the mobile user who wants to access the Camera Control Service.

(11) The Authentication Agent returns the evaluated result to the SSO Service.

(12) The SSO Service leads the mobile user to the Camera Control Service.

(13), (14), and, (15) The Camera Control Service controls the Camera via the Residential gateway in the Digital Home. Before granting access to the Camera, the Residential Gateway must verify the signed result.

(16) The mobile user who wants to access the Projector Control Service via the gateway operator provides the artifact received from the SSO Service (refers to step (10)).

(17) The gateway operator transfers the artifact to the Projector Control Service.

(18) The Projector Control Service requests user authentication from the SSO Service, providing the artifact instead of the user's name and password.

(19) The SSO Service sends the artifact to the Authentication Agent. The SSO Service no longer makes an authentication query.

(20) The Authentication Agent compares the artifact received from the SSO Service (refers to step (10)) with the original artifact (refers to step (9)). If the result is valid, the Authentication Agent removes the original artifact and generates a new artifact for the mobile user.

(21) The new artifact is assigned to the mobile user who wants to access the Projector Control Service.

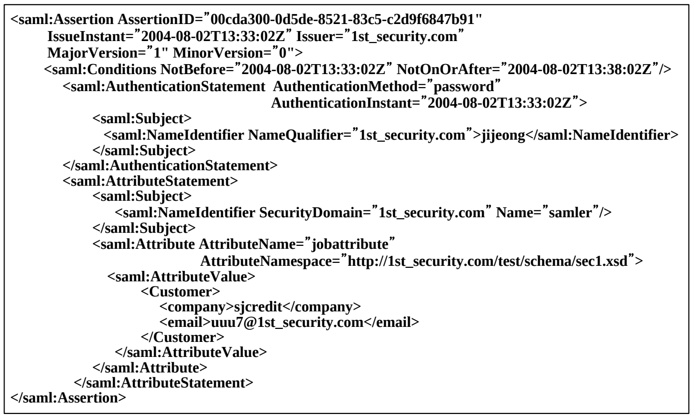
(22) The Authentication Agent returns the signed evaluated result to the SSO Service.

(23) The SSO Service leads the mobile user to the Projector Control Service.

(24), (25), and (26) The Projector Control Service controls the Projector via the Residential gateway in the Digital Home. Before granting access to the Projector, the Residential Gateway must verify the signed result.

The steps in Authentication process 2 are similar to those in Authentication process 1, since the Authentication Authority when accessing a certain service issues an artifact regarding user authentication. The user authentication scheme in each service may differ depending on the characteristics of each service. To transfer a security token, regarding a user's authentication, which was generated from a different user authentication scheme among the various services, a framework that does not restrict the representation of security information is needed.

Figure 6 is an assertion statement issued by the SAML authority (refers to step (7) of Figure 5; its signed information is removed). This message was verified by a simulation where two services were constructed with a mutual trust relationship using the SAML libraries revised and extended from the previous work [17].



```
<saml:Assertion AssertionID=”00cda300-0d5de-8521-83c5-c2d9f6847b91"
      IssueInstant=”2004-08-02T13:33:02Z” Issuer=”1st_security.com”
      MajorVersion=”1" MinorVersion=”0">
     <saml:Conditions NotBefore=”2004-08-02T13:33:02Z” NotOnOrAfter=”2004-08-02T13:38:02Z”/>
        <saml:AuthenticationStatement  AuthenticationMethod=”password”
                                       AuthenticationInstant=”2004-08-02T13:33:02Z”>
             <saml:Subject>
               <saml:NameIdentifier NameQualifier=”1st_security.com”>jijeong</saml:NameIdentifier>
             </saml:Subject>
        </saml:AuthenticationStatement>
        <saml:AttributeStatement>
             <saml:Subject>
                 <saml:NameIdentifier SecurityDomain=”1st_security.com” Name=”samler”/>
             </saml:Subject>
             <saml:Attribute AttributeName=”jobattribute”
                                   AttributeNamespace=”http://1st_security.com/test/schema/sec1.xsd”>
                <saml:AttributeValue>
                     <Customer>
                        <company>sjcredit</company>
                        <email>uuu7@1st_security.com</email>
                     </Customer>
                  </saml:AttributeValue>
             </saml:Attribute>
          </saml:AttributeStatement>
</saml:Assertion>
```

Figure 6. Assertion with Authentication and Attribute Statement

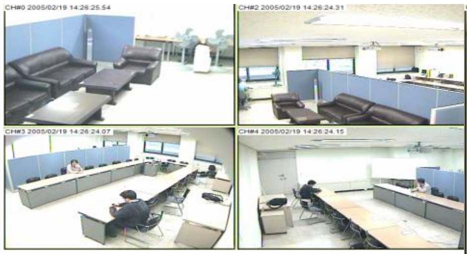


Figure 7. Rooms viewed by the Camera Control Service

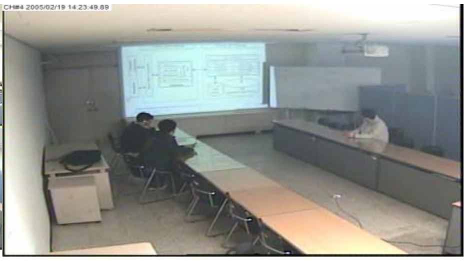


Figure 8. Meeting room where the projector is on

Figure 7 shows the views of rooms from the Camera Control Service. In Figure 7, CH#1 and CH#2 show living room and CH#3 and CH#4 show the meeting room. The mobile user can view each room to select a room for a meeting and then turn on the projector of the selected room using the Projector Control Service before the meeting. Figure 8 shows the room where the projector is on for the meeting.

4. Conclusion

In home network service environment including children’s game network based on the OSGi framework, there are some barriers to distributing automated user authentication due to the limited capabilities of mobile devices. To overcome these problems, we propose a security scheme to exchange user authentication information based on SAML under an OSGi-based network service environment including children’s game network. This scheme supports the efficient and secure transfer of a user's credential information between a mobile device and children’s game network running multimedia devices, and offers access to related domains without the burden of a repeated log-in process.

Since the proposed Single Sign-On scheme is designed to recognize the individual authentication scheme in each domain, the OSGi framework-based systems in a domain can have the right of self-government as well as extensibility.

Acknowledgements

This research is supported by Ministry of Culture, Sports and Tourism(MCST) and Korea Creative Content Agency(KOCCA) in the Culture Technology(CT) Research & Development Program 2011.

References

[1] I. -k. Hwang, D. -s. Lee and J. -w. Baek, "Home network configuring scheme for all electric appliances using ZigBee-based integrated remote controller", IEEE Transactions on Consumer Electronics, vol. 55, Issue 3, **(2009)**, pp. 1300-1307.

[2] H. Y. Lee and J. W. Kim, "An Approach for Content Sharing among UPnP Devices in Different Home Networks", IEEE Transactions on Consumer Electronics, vol. 53, Issue 4, **(2007)**, pp. 1419-1326.

[3] R. Gupta, S. Talwar and D. P. Agrawal, "Jini home networking: a step toward pervasive computing", Computer, vol. 35, Issue 8, **(2002)**, pp. 34-40.

[4] M. P. Bodlaender and R. G. Wendorf, "Adding full Internet protocol functionality to HAVi", IEEE Transactions on Consumer Electronics, vol. 48, Issue 4, **(2002)**, pp. 946-953.

[5] J. Cheng and T. Kunz, "Smart home networking: Combining wireless and powerline networking", In 7th International Wireless Communications and Mobile Computing Conference (IWCMC), **(2011)**, pp. 1276-1281.

[6] R. P. D. Redondo, A. F. Vilas, M. R. Cabrer, J. J. P. Arias, J. G. Duque and A. G. Solla, "Enhancing Residential Gateways: A Semantic OSGi Platform, IEEE Intelligent Systems", vol. 23, Issue 1, **(2008)**, pp. 32-40.

[7] A. Volchkov, "Revisiting single sign-on: a pragmatic approach in a new context", IT Professional, vol. 3, Issue 1, **(2001)** January/February, pp. 39-45.

[8] J. Yang, "An Improved Scheme of Single Sign-on Protocol", In Fifth International Conference on Information Assurance and Security (IAS '09), **(2009)**, pp. 495-498.

[9] W. -G. Lee, C. -J. Chae, S. -K. Kim, M. -Y. Kang and J. -K. Lee, "A Security Framework for Secure Home Networking in Ubiquitous Computing", In 2007 International Conference on Intelligent Pervasive Computing, **(2007)**, pp. 394-397.

[10] I. Kim, D. Lee, J. Lee and K. Rim, "Extended Authorization Mechanism in OSGi", 2010 International Conference on Information Science and Applications (ICISA), **(2010)**, pp. 1-7.

[11] OSGi Alliance Std., OSGi Service Platform Release 4.3, OSGi Alliance, **(2011)**.

[12] OASIS Committee Specification, Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML) V2.0, **(2005)**.

[13] A. Singhal, T. Winograd and K. Scarfone, "Guide to Secure Web Services", NIST (National Institute of Standards and Technology) Special Publication 800-95, **(2007)**.

[14] OSGi Alliance Std., Secure Provisioning Data Transport using Http, RFC36, **(2002)**.

[15] Z. A. Khattak, S. Sulaiman and J. A. Manan, "A study on threat model for federated identities in federated identity management system", In 2010 International Symposium in Information Technology (ITSim), **(2010)**, pp. 618-623.

[16] W. Huang and J. Xu, "An authentication agent for web-based system", In 2009 IEEE International Conference on Network Infrastructure and Digital Content (IC-NIDC 2009), **(2009)**, pp. 596-599.

[17] J. Jeong, D. Shin and D. Shin, "An XML-based single sign-on scheme supporting mobile and home network service environments", IEEE Transactions on Consumer Electronics, vol. 50, Issue 4, **(2004)**, pp. 10810-1086.

Authors

Dongkyoo Shin received a B.S. in Computer Science & Statistics from Seoul National University, Korea, in 1986, an M.S. in Computer Science from Illinois Institute of Technology, Chicago, Illinois, in 1992, and a Ph.D. in Computer Science from Texas A&M University, College Station, Texas, in 1997. He is currently a Professor in the Department of Computer Science & Engineering at Sejong University in Korea. From 1986 to 1991, he worked in Korea Institute of Defense Analyses, where he developed database application software. From 1997 to 1998, he worked in the Multimedia Research Institute of Hyundai Electronics Co., Korea as a Principal Researcher. His research interests include XML Security, XML based middleware, multimedia application, biological database, mobile Internet and ubiquitous computing.

Dongil Shin received a B.S. in Computer Science from Yonsei University, Seoul, Korea, in 1988. He received an M.S. in Computer Science from Washington State University, Pullman, Washington, U.S.A., in 1993, and a Ph.D. from University of North Texas, Denton Texas, U.S.A., in 1997. He was a senior researcher at System Engineering Research Institute, Deajun, Korea, in 1997. Since 1998, he has been with the Department of Computer Science & Engineering at Sejong University in Korea where he is currently a Professor. His research interests include Mobile Internet, Computer Supported Cooperative Work, Object-Oriented Database, Distributed Database, Data Mining and Machine Learning.