Security Management of a Cloud-based U-City Management System

Sung Min Kim, Jun Oh Kim, Chang Ho Yun,
Jong Won Park, Yong Woo LEE (Corresponding Author)
School of Electrical & Computer Engineering
University of Seoul, Ubiquitous-City (Smart City) Consortium
Seoul, Korea
{smkim, kjo, touch011, comics77, ywlee}@uos.ac.kr

Hae Sun Jung
Ubiquitous-City (Smart City) Consortium
Seoul, Korea
holylife7@hotmail.com

***Abstract*— In this paper, we introduce a user authentication methodology for a cloud-based U-City management system to manage the U-City which includes ubiquitous resources and cloud computing resources. Cloud computing enables the integrated urban operation center of the U-City to provide limitless computing power without having its own computing center. However, because huge number of services and users use the U-City service and the cloud computing power and they should be carefully screened, we need a specially designed security management to protect the U-City and its facilities. For it, we propose the cloud-based U-City management system, UTOPIA which uses SAML-based Single-Sign-On (SSO) authentication for the security management to do user authentication and privilege management for the cloud computing in the U-City.**

Keywords-U-City; Cloud Computing; SAML; U-City Security Management; Single-Sign On.

I. INTRODUCTION

With ubiquitous computing, we are seeking the way to satisfy human beings' desire to enjoy IT services with any device, anytime and anywhere. In U-City, every possible information system such as residential, environmental, medical, business, governmental, social and the like is linked through ubiquitous computing technologies and the whole U-City acts as virtually one system or a global system which works for human beings and takes care of them.

U-City is usually centrally managed by the central operation center which processes the huge amount of the data and often needs huge computing power. The irregularity of need in computing power makes it very attractive that the U-City uses cloud computing since the cloud computing obviously save the cost of computing power [1].

Cloud computing is defined as "a style of computing where scalable and elastic IT-related capabilities are provided as a service to customers using Internet technologies." [2]. To use cloud service requires generally better security than to use private system. In order to include cloud computing in U-City, we should keep it in mind. As well-publicized cases of cloud computing vulnerability, we can think Amazon S3 malfunction over seven-hour on July 20, 2008 [3], Gmail outage over one-day in mid-October 2008 [4] and Google Docs vulnerabilities [5].

Security issues such as user authentication, information protection and access control should be carefully solved in order that we provide U-City services using the cloud computing to users. For it, we propose a U-City Management System named UTOPIA, which uses SSO authentication technology based SAML as a part of the security management [6]. Users who use the U-City Management System do not need to be bothered to login again and again whenever they use difference service of UTOPIA but login just once.

This paper is organized as follows. Section 2 briefly introduces related works and confirms that this work is the first and only work till now. Section 3 outlines our U-City management system, UTOPIA, which is composed of the three tiers. Sections 4 explains our SAML based SSO user authentication as a part of our security management. Section 5 describes the implementation of the SAML based SSO user authentication into UTOPIA. Finally, Section 6 gives conclusions and explains future works.

II. RELATED WORK

A. U-City Management

U-City management system enables citizens to easily use U-City services. There are many U-Cities in Korea as shown in Table 1.

Seoul Metropolitan Government Information Agency, Seoul in Korea has been building many U-Towns based on U-Seoul Master Plan which aims U-Care, U-Fun, U-Green, U-transport, U-Business and U-Government [7]. They have central operation centers, which use their own U-City management systems but they are different from UTOPIA which uses the three tier U-City Management System Paradigm based on U-City middleware and U-City portal. They have various kinds of user services, but they are not integrated together and do not provide SSO based user authentication.

U-Dongtan U-City provides many kinds of public services such as surveillance of public areas, environment pollution information, water leakage management, media board, traffic information and so on. It uses user authentication with just identity and password and does not use SSO authentication [8]. The U-city has central operation center which use a platform but does not use U-City middleware. Like these, we are the only U-City management system which uses three tier U-City paradigm, U-City middleware and the U-City

 ISBN: 978-1-61208-153-3

portal and uses SSO authentication. That is, currently, there is no U-City which is based on our concept.

TABLE I. SOME MAJOR U-CITY PROJECTS IN KOREA

U-city Project Name	*Period*	*Goal*
Digital Media City	2001~2010	The world best IT town. Northeast Asian IT hub.
U-Gangnam	2004~2007	Seamless Connectivity. Mobile Environment. Teleportation & Telework.
U-cheonggyecheon	2007	3D-based GIS. A U-City testbed.
U-Myengdong/ U-Ljiro	2007~2010	Digital media plaza. Digital media stree, Digital media gallery.
Eunpyeong New Town	2006~2011	A ubiquitous new-town.
U-Busan	2004~2010	The World first u-city. U-port, U-Traffic, U-convention.
U-Gwangju	2004~2012	Centered on U-home.
U-Daejeon	2004~2007	U-cluster. U-wellbeing.
U-Gyeongbuk	2004~2010	The largest U-City testbed. U-culture.
U-Pyong Chang	2006~2010	U-city for winter sports.
U-Chungbuk	2005~2009	3D GIS. U-cluster.
U-Jeju	2004~2006	Focused on telematics.
U-Sejong	2005~2030	U-government
Gwanggyo New-town	2005~2011	A ubiquitous well being town.
Pangyo New-town	2006~2010	A U-echo city.
U-Dongtan	2003~2007	GIS. ITS. BcN. IBS.
U-Jeonju	2005~2008	U-culture. U-tour. U-traffic.
U-Paju	2005~2009	Total Life-Card. Smart transport.
U-Bucheon	2010~2014	U-home network, U-traffic, U-tour. U-echo. U-safety.
U-Changwon	2004~2008	Digital broadcasting. Media center.
U-Ansan	2007~2012	U-Industry. U-tour.

B. Security management using personal authentication technology

Table 2 summarizes major personal authentication methods case by case. Currently SSO is popular and widely used [9]. We think SSO is one of the best solutions to the security management in U-City, since so many kinds of U-City services are provided, so many kinds of organizations such as public agencies, financial institutions, large corporations, educational institutions are integrated in U-City and the separately developed U-Cities can be merged into a larger U-City later. Currently no U-City uses SSO for their security management, and this work is the first case and the only research at the moment.

TABLE II. THE PERSONAL AUTHENTICATION

Security Technology	*Description*
ID/Password	It is a typical personal authentication method. It requires periodic renewal [10].
Public key certificate	It uses a digital signature to bind a public key with an identity. The private keys are stored in certificate storage location. Encryption / decryption processing, cryptography transmission method are usually used to protect them. By implementing programs to protect private key and certificate into client computers, the security can be improved. However, it requires users' agreement and actions and causes extra maintenance expenses. [11]
SSO (Single Sign On)	Users log in once and gain access to all systems without being prompted to log in again at each system [12].
MTM (Mobile Trusted Module)	It is a hardware-based authentication which was proposed by TCG (Trusted Computing Group). It is usually used for the authentication of mobile devices and is recently used for cloud computing authentication with SIM (Subscriber Identity Module) [13].
Finger Print and Identifier	It uses user's bio profiles such as finger print and etc. which are usually kept in the file system and are used to identify the user. But, it is weak to Trojan horse attacks, memory hacking and key-logging because users' profiles are store in the file system [14].
IP-Geographic location Identification	It uses user's IP location and is helpful to prevent MITM attacks [14].
Knowledge-based authentication	It asks the question about specific knowledge of user information. But, it is usually used with other methods because it is vulnerable to MITM attacks [14].
OTP(One-Time Password)	It uses a password which is valid during only one login session to avoid a shortcoming of static passwords. In order to deliver the OTP, text messaging or proprietary tokens or web-based method is used. It is vulnerable to key logging and MITB because it relies on a key input [14].
Out-of-Band authentication	Each time, it uses a different communication channel to verify a transaction request. It guarantees very high security but it requires initial registration. Thus it can be expensive [14] [15].
Internet Personal Identification Number (i-PIN)	It uses the Resident Registration Number for login. It is used in South Korea [16] [17].

III. CLOUD-BASED U-CITY MANAGEMENT

Our U-City management system, UTOPIA, supports the unified ubiquitous cloud environment by providing dynamic service deployment based on context-awareness, high performance and collaborative computing on Grid and cloud. It is based on three tiers paradigm as shown in Figure 1. The feeling tier is composed of U-City infrastructure such as buildings, bridges, loads, etc., and ubiquitous IT devices including sensors and video cameras and connected to the processing tier through Broadband Convergence Network (BcN) and Ubiquitous Sensor Network (USN). The processing tier plays a role of brain in human body, receives data from the feeling tier and processes them intelligently. Finally, the presentation tier receives the request of users and

 ISBN: 978-1-61208-153-3

sends it to processing tier and show the result from the processing tier to them. It acts as a window to the U-City system.

Our middleware in the processing tier, which we call SOUL, supports cloud computing and security management facilities including user authentication. It also supports Computational Grid so that it can smoothly satisfy applications which require real-time high performance computing. It supports computer supported cooperative work (CSCW) through Access Grid that is the best choice currently and a next generation CSCW.

It has the following additional characteristics. First, it provides common device interface which was designed to support variable sensor network data-sinks and protocols. Therefore, it can be used as the common gateway for various kinds of sensors and ubiquitous sensor networks which collect sensed data.

Second, it uses ontology-based intelligent inference engine which provides context-aware, that is, intelligent information using the sensed data through the common device interface. Third, it provides a user-transparent infrastructure that generates and provides intelligent services, which are invisible to users, to various applications. Fourth, it enables user to control remote devices in real-time mode so that remote control devices such as fire doors and other emergency devices can be controlled remotely in real-time mode. Fifth, it has the advantages of layered architecture since it is designed to have layer architecture. Lastly and sixth, it can directly be connected to easy-to-use, yet convenient, user interfaces, the U-City portal.

We believe that these advantages make SOUL possible to be used in various kind of U-city applications of our project and it can shorten the period and expense to develop the U-city applications. [18]

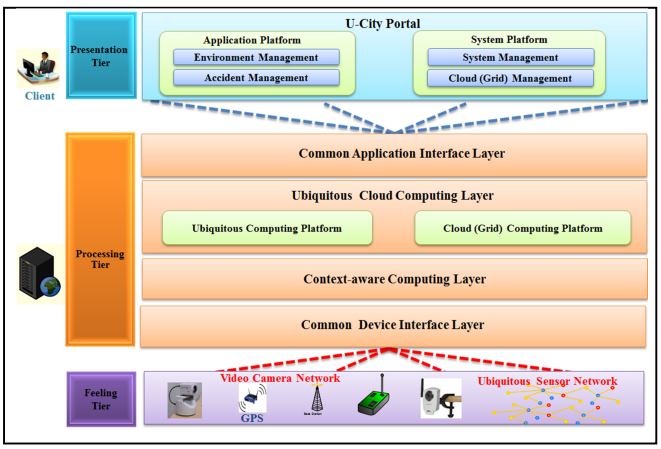

Figure 1. UTOPIA: A U-City Management System.

The U-City portal has the security management component and beyond it, it has two distinctive components as shown in figure 2. One is the application platform and the other is the system platform. The environment management application is one of the application services which belongs to the application platform and give services in the management of noise, air-pollution and water quality using GIS visualization technology. The cloud management belongs to the system platform [19][20].

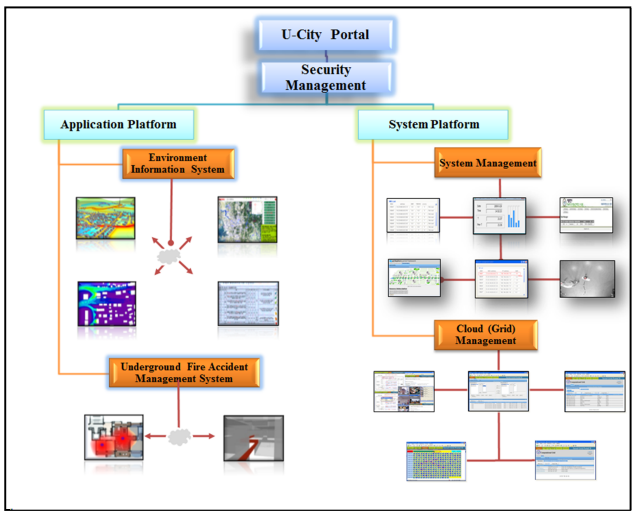

Figure 1. The architecture of the U-City portal.

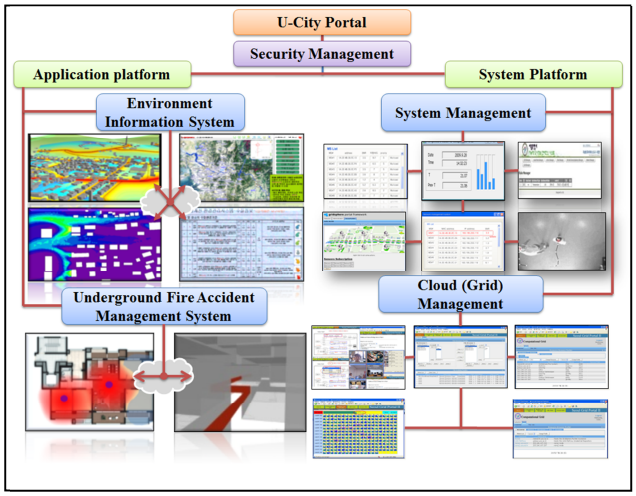

Figure 2. The architecture of the U-City portal.

IV. SSO AND SAML IN UTOPIA

The advantage of the adopting SSO in the U-City management system can be explained in following two viewpoints.

1) Users' viewpoint:

Without SSO, users are asked to log in each service or each organization when they want to use the U-City service and therefore users should remember their IDs and passwords in each login. With SSO, users just should log in one time. It is more convenient, easier and more efficient than without SSO.

2) Administrators' viewpoint:

With SSO, administrators can trace users activities and manage users security at the level of overall or total management of U-City, not at the level of individual organization or services. That is, U-City can have total solution for security management with easy administration and more consistant manner with SSO.

SSO in UTOPIA is operated as shown in Figure 3 and Figure 4. When a user accesses UTOPIA through the U-City portal to use the U-City services, the login facility starts. The SSO agent in the login facility for the security management in UTOPIA sends the user's information to the authentication manager using the SAML request. SAML messages at each step are encrypted using the SSL protocol. Then, the authentication manager does the security screening by asking the credential database and makes a decision. Since UTOPIA uses SSO, the user does not have to be bothered by login many times if he/she wants to use several services in UTOPIA.

.

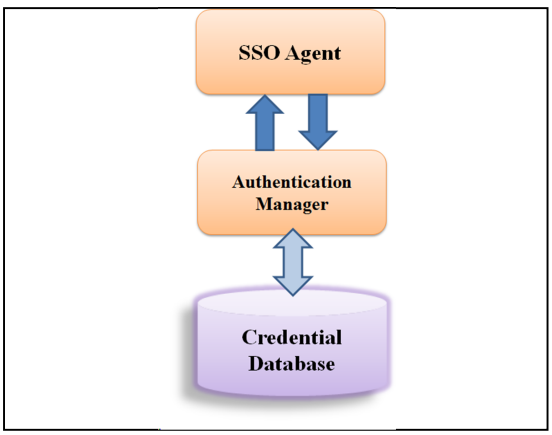

Figure 3. SSO management in UTOPIA.

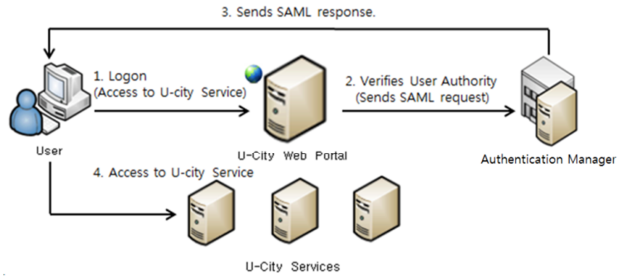

Figure 4. Single-Sign-On Service in UTOPIA.

V. IMPLEMENTATION

Figure 5 shows how UTOPIA processes SAML-based SSO for U-City. SAML supports implementing SSO. We use OpenSAML2 Library and openssl. The RSA key pair is generated with openssl for authentication. The RSA key pairs are UTOPIA_sso_private.der and UTOPIA_sso_public.der. SSO is implemented with original RSA public key. The user accesses the service provider, the U-City portal of UTOPIA, to use the U-City service. ServiceProviderForm in U-City portal is the access web page. The elements of ServiceProviderForm are loginForm, providerName, RelayState, acsURI. LoginForm is for authentication in identity provider. ProviderName is the name of service provider providing the service. RelayState is the redirected service page after ACS authentication. AcsURI is the URL to verify SAMLResponse in identity provider. The U-City service provider generates SAMLRequest in a XML format. SAMLRequest is sent to authentication provider, that is, Identity Provider, through the user's browser. The authentication provider parses the SAMLRequest and process user authentication. The authentication provider generates a SAMLResponse. The authentication provider sends SAMLResponse to the Assertion Consumer Service (ACS) through the user browser. The ACS in the service provider receives the SAMLResponse sent by the authentication provider and validates it. If it is o.k., then the service provider gives the user a permit to log in UTOPIA. Now, the user can successfully log in to UTOPIA and use the wanted U-City service.

 ISBN: 978-1-61208-153-3

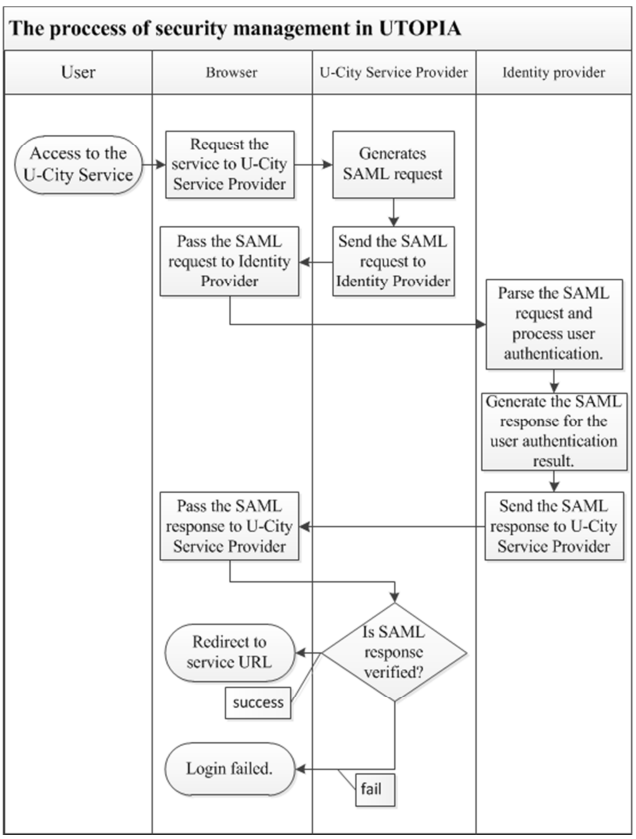

Figure 5. The sequence diagram of security management in UTOPIA.

VI. CONCLUSION

This paper explained the security management of U-City management system which uses cloud computing heavily. Our U-City management system, UTOPIA, adopted SAML-based SSO as a user authentication methodology for our security management facility. It is the first and the only U-City management system to use SSO currently. Users can use the services of UTOPIA through the U-City portal with unified authentication which uses one-time login for all UTOPIA services. The work is still in progress since we have been continuously adding many organizations and more services and in future work, we will continue to support a more fine-grained privilege management.

ACKNOWLEDGMENT

This study was supported by the Seoul Research and Business Development Program (10561), Smart (Ubiquitous) City Consortium, Seoul Grid Center. We would like to give thanks to Mr. Cheol Sang Yoon, Mr. Tae Ho Hong, Mr. Eui Dong Hwang, Mr. Kyoung-gyu Lee and the staffs of Seoul Grid Center and the members of Smart (Ubiqitous) City Consortium for their contribution to this research.

REFERENCES

[1] J. W. Park, C. H. Yun, S. Kim, H.Y. Yeom and Y. W. Lee, "Cloud Computing Platform for GIS Image Processing in U-City," 13th International Conference on Advanced Communication Technology (ICACT), pp. 1151-1155, 2011.

[2] Gartner's Cloud Computing website [online], May 2011, Available from: http://www.gartner.com/technology/research/cloud-computing/index.jsp.

[3] Amazon S3 Availability Event: July 20, 2008 [online], May 2011, Available from: http://status.aws.amazon.com/s3-20080720.html.

[4] Extended Gmail outage hits Apps admins [online], May 2011, Available from: http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9117322.

[5] Google's response to Google Docs concerns. [online], May 2011, Available from: http://googledocs.blogspot.com/2009/03/just-to-clarify.html.

[6] T. Gross, "Security Analysis of the SAML Single Sign-on Browser/Artifact Profile," Annual Computer Security Applications Conference, vol.19, pp. 298-307, 2003.

[7] U-City of Seoul website [online], May 2011, Available from : http://info.seoul.go.kr/.

[8] U-City of Hwasong Dongtan website [online], May 2011, Available http://www.udongtan.or.kr.

[9] Alessandro Armando, Roberto Carbone, Luca Compagna, Jorge Cuellar, Llanos Tobarra, "Formal Analysis of SAML 2.0 Web Browser Single Sign-On: Breaking the SAML-based Single Sign-On for Google Apps," the 6th ACM workshop on Formal methods in security engineering, 2008

[10] P. Beynon-Davies, "Personal identity management as a socio-technical network," Technology analysis & strategic management, vol.22, no.4, pp. 463-478, 2010.

[11] G. Bick, M. C. Jacobson and R. Abratt, "The Corporate Identity Management Process Revisited," Journal Of Marketing Management, vol.19, no.7-8, pp. 835-856, 2003.

[12] Y. Y. Chan, "Weakest Link Attack on Single Sign-On and Its Case in SAML V2.0 Web SSO," Lecture Notes in Computer Science, vol. 3982, pp. 507-516 , 2006.

[13] Trusted Computing Group website [online], May 2011, Available from: http://www.trustedcomputinggroup.org.

[14] H. S. Kim, "Cloud Computing and Personal Authentication Service", Information & Communications Magazine, vol. 20, no. 2, pp. 11-92, 2010.

[15] A. Litan, "Where String Authentication Fails and What You Can About It," Gartner Research, 2009.

[16] Y. Oh, T. Obi, J. S. Lee, H. Suzuki, and N. Ohyama, "Empirical analysis of internet identity misuse: case study of south Korean real name system," he 6th ACM workshop on Digital identity management (DIM '10), pp. 27-34, 2011.

[17] S. K. Un, N. S. Jho, Y. H. Kim and D. S. Choi, "Cloud Computing Security Technology," Electrical Communication Trend Analysis, vol. 24, no. 4, pp. 79-88, 2009.

[18] H. S. Jung, C. S. Jeong, Y. W. Lee and P. D. Hong, "An Intelligent Ubiquitous Middleware for U-city: SmartUM," Journal of Information Science and Engineering, vol. 25, no. 2, pp.375-388, 2009.

[19] S. W. Rho and Y. W. Lee, "U-city Portal For Smart Ubiquitous Middleware," 2010 The 12th International Conference Advanced Communication Technology (ICACT), pp. 609-613, 2010.

[20] S. W. Rho, C. H. Yun and Y. W. Lee, "Provision of U-city web services using cloud computing," 13th International Conference on Advanced Communication Technology (ICACT), pp. 1545-1549, 2011.

 ISBN: 978-1-61208-153-3