Journal of the Korea Convergence Society
Vol. 10. No. 1, pp. 53-59, 2019

ISSN 2233-4890
https://doi.org/10.15207/JKCS.2019.10.1.053

스마트시티 매니지먼트 시스템에서의 사용자인증보안관리

황의동[1], 이용우[2*]
[1]서울시립대학교 전자전기컴퓨터공학과 박사과정,
[2]서울시립대학교 전자전기컴퓨터공학과 교수

User Authentication of a Smart City Management System

Eui-Dong Hwang[1], Yong-Woo Lee[2*]
[1]Ph.D., Student, School of Electrical and Computer Engineering, University of Seoul
[2]Professor, School of Electrical and Computer Engineering, University of Seoul

요 약 본 논문에서는 스마트시티에 대한 사용자 인증을 통합하여 수행하는 UTOPIA 스마트시티 보안 관리 시스템을 소개한다. 스마트시티 관리 시스템은 엄청난 수의 사용자와 서비스를 관리해야하며 하나하나 개별적으로 신중하게 관리해야하므로, 특별히 고안된 보안 관리가 필요하다. UTOPIA는 ICT 기반의 스마트시티 시스템으로서 UTOPIA 포탈 시스템과, UTOPIA 프로세싱 시스템, UTOPIA 인프라 시스템의 삼 단계 구조를 가지고 있다. UTOPIA 프로세싱 시스템은 SmartUM 이라고 명명된 스마트시티 미들웨어를 기반으로 한다. UTOPIA 스마트시티 보안관리 시스템은 SmartUM 미들웨어의 최상층 계층인 어플리케이션 보안 계층과 최하위계층인 인프라 보안 계층에 구현되어져 있다. UTOPIA 스마트시티 보안관리 시스템은 현존하는 모든 사용자 인증 기술을 지원한다는 원칙하에 제작되었다. 본 논문에서는 어플리케이션 보안 계층을 소개하고, 어플리케이션 보안 계층에서의 인증관리에 대하여 설명한다.

주제어 : 유토피아 스마트시티 시스템, 스마트시티 미들웨어, 통합 보안 관리, 통합 인증, 스마트시티 보안 관리 시스템

Abstract In this paper, we introduce the UTOPIA Smart City Security Management System which manages a user authentication for smart cities. Because the smart city management system should take care of huge number of users and services, and various kinds of resources and facilities, and they should be carefully controlled, we need a specially designed security management system. UTOPIA is a smart city system based on ICT(Information and Communication Technology), and it has a three tier structure of UTOPIA portal system, UTOPIA processing system and UTOPIA infrastructure system. The UTOPIA processing system uses the smart city middleware named SmartUM. The UTOPIA Smart City Security Management System is implemented in the application security layer, which is the top layer of the SmartUM middleware, and the infrastructure security layer, which is the lowest layer. The UTOPIA Smart City security management system is built on the premise that it supports all existing user authentication technologies. This paper introduces the application security layer and describes the authentication management in the application security layer.

Key Words : UTOPIA Smar City System, Smart City Middleware, Integrated Security Management, Single Sign On(SSO), UTOPIA Smart City Security Management System

1. 서론

스마트시티는 대한민국의 법률에 따르면 “도시의 경쟁력과 삶의 질의 향상을 위하여 건설·정보통신기술 등을 융·복합하여 건설된 도시기반시설을 바탕으로 다양한 도시서비스를 제공하는 지속가능한 도시를 말한다[1].”

*Corresponding Author : Yong-Woo Lee (ywlee@uos.ac.kr)
Received October 4, 2018
Revised December 31, 2018
Accepted January 20, 2019
Published January 28, 2019

라고 정의하고 있다. 국제표준화기구 (ISO)는 스마트시티를 “도시의 계획과, 개발 및 관리를 위하고 스마트 서비스 제공을 할 수 있도록 IoT, 클라우드 컴퓨팅, 빅 데이터, 공간 정보/지리 정보 통합과 같은 최신 정보 기술이 적용되는 새로운 개념의 도시, 새로운 모델 도시”라고 정의하고 있다[2].

스마트시티가 다양한 지능적인 서비스들을 사용자에게 제공하기 위하여 3 티어로 이루어진 지능형 스마트시티 시스템인 UTOPIA를 제안하고 이를 발전시켜오고 있다. UTOPIA 스마트시티 시스템은 UTOPIA 스마트시티 인프라스트럭쳐 티어, UTOPIA 스마트시티 미들웨어 티어, UTOPIA 스마트시티 포탈 티어로 구성된다[3].

기존의 도시 인프라를 기반으로 다양한 정보통신기술 (ICT: Information and Communication Technology)을 융합하여 스마트시티를 창조하여, 언제 어디에서나 다양하고 스마트한 스마트시티의 인프라를 이용할 수 있으려면, 다양한 ICT를 사용하여, 도시의 요소들을 유기적으로 연결하고 관리하는 것이 필요하다. UTOPIA 스마트시티에서는 주거, 환경, 의료, 비즈니스, 정부, 사회 등에서의 모든 정보들이 유기적으로 통합하여 관리된다. 이를 위하여, UTOPIA 스마트시티는 사실상 하나의 글로벌 시스템으로 작동하면서, 시민에게 여러 가지 서비스를 제공한다. 하나의 유기적으로 통합된 시스템으로 스마트시티를 관리하기 위해서는 스마트시티를 위한 전용 운영체제의 역할을 하는 미들웨어가 필요하다. 이 미들웨어는 도시에서 생성되는 방대한 데이터 및 무수하게 많고 다양한 도시 인프라들을 관리 하여야 하기 때문에 보안에 대한 고려가 반드시 필요하다. 스마트시티가 사용자에게 안전한 스마트시티 서비스를 제공하기 위해서는 사용자 인증, 정보 보호 및 액세스 제어와 같은 보안 문제를 신중하고 정확하게 해결해야 한다. 그러나 기존의 보안 솔루션 및 보안 기법들이 개별적으로 적용되어서 운영된다면, 각각의 보안 기능만을 제공하고, 통합적인 보안과 연동을 제공할 수 없게 되어서 스마트시티의 보안을 제대로 할 수 없다.

본 논문에서는 이런 면을 감안하여, 스마트시티 시스템을 통합적으로 보안한 UTOPIA 스마트시티 보안 시스템에서의 UTOPIA 통합인증을 제안한다. UTOPIA에서는 보안 관리를 위하여, 여러 가지 개인인증 방법과 기술을 지원하는데, 이 다양한 개인인증 방법과 기술을 통한 인증을 일회-사인-온 인증 기술 (Single Sign On: SSO)[4]을 사용하여 통합적으로 관리한다. UTOPIA 통합인증시스템의 의하여, UTOPIA 스마트시티 관리시스템을 사용하는 사용자는 UTOPIA가 제공하는 여러 종류의 서비스를 사용할 때마다 그 서비스를 제공하는 서로 다른 기관의 서버에 매번 다시 로그인 할 필요가 없이, 한 번만 로그인해도 안전한 보안이 유지되도록 편리한 보안 관리 서비스를 제공받는다.

본 논문은 다음과 같이 구성되었다. 2장에서는, 관련 연구를 설명한다. 3장에서는, UTOPIA 스마트시티 시스템에서의 보안에 대하여 설명한다. UTOPIA의 각 티어를 소개하고, 미들웨어 시스템과 각 계층을 설명한다. 이를 바탕으로 미들웨어 시스템내의 보안계층을 소개하고 통합 보안을 소개한다. 4장에서는, UTOPIA에서의 통합인증에 대하여 설명한다. 5장에서는, UTOPIA 통합인증 시스템을 어떻게 구현하는지와 작동 메커니즘을 설명한다. 마지막으로 6장에서는, 결론과 향후 연구 방향에 대해 설명한다.

2. 관련연구

유럽연합은 스마트시티 건설에 대하여, 2013년 말에 검토를 마무리하고, 2014년부터 스마트시티를 기반으로 하는 유럽 건설이라는 기치를 걸고, 열심히 노력해오고 있다[5]. 유럽연합의 활동에 힘입어, 호주, 중동, 인도, 중국, 일본 등에서도 스마트시티 붐이 조성되고 있다. 한국은 유시티라는 명칭으로, 정보통신기술을 기반으로 하는 미래도시에 대한 연구를 본격적으로 훨씬 전부터 시작하였으나, 결실을 제대로 맺지 못하다가, 최근에 유럽연합과 세계의 스마트시티 붐에 고무되어서, 유시티를 스마트시티로 탈바꿈하려는 시도를 하고 있다.

UTOPIA 스마트시티 패러다임을 2005년도에 제시함으로서 스마트시티를 전 세계에 소개한 이래, 본 연구진은, 전 세계에 UTOPIA 스마트시티에 관한 연구 결과를 꾸준히 발표해 왔고, 스마트시티의 필요성과 유용성을 중심으로, 스마트시티는 미래에 반드시 실현되어야 할 일임을 알려왔다.

본 연구진은, 2013년에 유럽연합의 스마트시티 계획에 자문을 하고, 사업 추진을 격려한 바 있다. 마침내, 큰 규모의 유럽연합의 스마트시티 사업이 시작되어 오늘에 이르게 되는 쾌거를 보게 되었다. 현재, 전 세계의 스마트시티 연구는 UTOPIA에서 제시한 바와 같은 패러다임을

중심으로 하여 연구가 전개되고 있다.

[6,7]은 스마트시티 이전 버전인 유시티에서의 보안에 관한 내용을 담고 있다. 전술한 바와 같이, 현재 스마트시티에 대한 연구개발과 실제 구축이 유럽을 중심으로 활발히 이루어지고 있고, 국내에서도 이를 인지하고, 연구개발을 시작하고 있으므로, 앞으로 스마트시티의 보안에 관한 연구결과가 많이 소개될 것으로 전망한다[8-14].

스마트시티에서, UTOPIA 스마트시티처럼 3 티어 구조를 갖춘 관리시스템을 구축하고, 전용 운영체제에 해당하는 스마트시티 미들웨어를 사용하면서, 이 미들웨어 내에 보안 계층을 두고, 그 보안 계층이, 일회-사인-온 기능을 중심으로 3장에서 설명하는 다양한 사용자 인증 방법과 기술을 통합적으로 지원 하는 통합보안관리 시스템에 대한 연구 결과는 아직 발견하기 어려웠다.

3. UTOPIA에서의 보안

UTOPIA는 클라우드 컴퓨팅 및 기타 최첨단 기술을 사용하여 상황 인식, 고성능 및 협업 컴퓨팅을 기반으로 한 동적 서비스를 제공함으로써 통합 된 스마트시티 관리를 지원한다. UTOPIA는 스마트시티를 통합적으로 관리하기 위하여, Fig. 1과 같이, UTOPIA 스마트시티 포탈 티어, 지능적인 여러 솔루션을 제공하는 UTOPIA 스마트시티 미들웨어 티어, 그리고 UTOPIA 스마트시티 인프라스트럭처 티어의 세 가지 티어로 구성되어 있다.

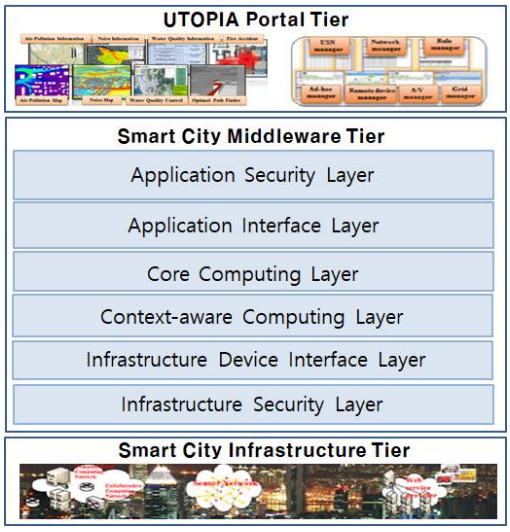

Fig. 1. The architecture of UTOPIA

UTOPIA 스마트시티 포탈티어는 사용자들이 온라인으로 다양한 스마트시티 서비스들을 이용할 수 있는 역할을 한다[3,15,16]. UTOPIA 스마트시티 인프라스트럭처 티어는 UTOPIA 미들웨어 티어와 연결되어 통합운영된다. UTOPIA 스마트시티 인프라스트럭처 티어는 빌딩, 교량, 부하 등과 같은 스마트시티 인프라와 센서, 비디오 카메라 및 IoT 장치를 포함한 스마트 유비쿼터스 정보통신 장치들을 포함한다. 스마트시티 인프라스트럭처 티어는 Broadband Convergence Network (BcN) 및 Ubiquitous Sensor Network (USN)를 통해 미들웨어 계층, 즉 처리 계층에 연결된다.

UTOPIA의 미들웨어티어는 스마트시티 인프라스트럭처 티어에서 전송된 데이터들을 처리하고 각종 스마트한 기능을 융복합하는 역할을 한다. SmartUM이라고 명명된 스마트시티 미들웨어는 여기에 속하는데, 사용자 인증을 포함한 클라우드 컴퓨팅 및 보안 관리 기능을 지원한다.

SmartUM은 다음과 같은 특성을 가진다. 첫째, 계층화 된 아키텍처의 장점이 있다. 둘째, 가변 센서 네트워크 데이터 싱크 및 프로토콜을 지원하도록 설계된 인프라 장치 인터페이스 계층을 제공한다. 따라서 다양한 종류의 센서를 가지고 센서로부터 감지 된 데이터를 수집 하는 유비쿼터스센서네트워크의 공통 게이트웨이로 사용될 수 있다. 세 번째로, 상황인식계층은 온톨로지 기반의 지능형 추론 엔진을 가지고 있으며 인프라 장치 인터페이스 계층에서 전달되는 감지 된 데이터를 사용하여 상황을 인식해서 지능형 정보를 제공한다. 네 번째로, 코어 컴퓨팅 계층은, 미들웨어의 핵심처리 계층으로서, 클라우드 컴퓨팅, 스마트서비스를 제공하기 위한 각종 융복합 처리 등을 하는 계층이다. 컴퓨터 지원 협력 작업 (CSCW: Computer Supported Cooperative Work)도 여기에서 지원된다. 지능형 서비스를 생성하고 다양한 애플리케이션에 제공한다. 이 계층의 기능을 사용하여, 사용자는 원격 IoT 장치를 실시간 모드로 제어하여 원격 IoT 방화문 및 기타 비상 원격 IoT 장치와 같은 원격 IoT 장치를 실시간 모드로 원격 제어 할 수 있다. 다섯 번째로, 어플리케이션 인터페이스 계층은, 사용하기 쉽고 편리한 사용자 인터페이스를 가진 UTOPIA 포털을 지원한다. 다양한 종류의 스마트시티 어플리케이션을 지원하는 계층이다. 여섯 번째로, 보안 계층이 1층과 6층에 자리잡고 있다. 스마트시티 인프라에 대한 접근 보안을 실행하

기 위하여 스마트시티 인프라 보안 계층이 1층에 위치한다. 어플리케이션 보안 계층은 6층에 위치하면서, UTOPIA 포탈티어를 통한 사용자의 접근에 대한 보안을 관리한다. UTOPIA 어플리케이션 보안 계층이 지원하는 주요 개인인증방법을 Table 1에서 요약하여 소개한다.

Table 1. User authentication technologies supported by UTOPIA

Security Technology	Description
ID/Password	It is a typical personal authentication method. It requires periodic renewal [17].
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 [18].
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) [19].
Bio profiles including finger print.	It uses user's bio profiles such as finger print 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 [20].
IP-Geographic location Identification	It uses user's IP location and is helpful to prevent MITM attacks [20].
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(Man in the Middle) attacks [20].
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 [20].
OOB (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 [20][21].
Internet Personal Indentification Number (i-PIN)	It is used instead of the Korean Resident Registration Number for login in South Korea [22][23].

Table 1에서 요약 설명한 여러 가지 개인인증을 UTOPIA가 사용할 때, 이와 같은 개인인증을, 일회-사인-온 기능을 사용하여서, 통합적으로 관리하는 스마트시티 보안 관리가 필요하다고 판단했다. 그 이유는 아래와 같다. 첫째로, 스마트시티에는 공공 기관, 금융 기관, 대기업, 교육 기관과 같은 많은 종류의 조직이 스마트하게 통합되어 있다. 둘째, 이를 기반으로, 다양한 스마트시티 서비스가 제공되고 있다. 셋째, 각기 별도로 개발 된 스마트시티는 나중에 더 큰 스마트시티로 병합 될 수 있다. 이런 이유로, 어플리케이션 보안 계층은 위의 여러 가지 개인인증을 통합관리하기 위하여, 일회-사인-온 기능을 사용하는 사용자 통합 인증 기능을 제공한다. 일회-사인-온 기능을 사용하는 사용자 통합 인증은 다음의 두 가지 관점에서 이점이 있다.

1) 사용자 관점: 일회-사인-온 기능이 지원되지 않으면, 사용자는 각 시스템에 별도로 사용자 인증을 거쳐야 한다. 일회-사인-온 기능을 사용하면 사용자는 한 번만 사용자 인증을 하면 된다. 일회-사인-온 기능을 사용하지 않는 경우 보다 편리하고 쉽고 효율적이다.

2) 관리자 관점: 스마트시티 관리 시스템에서 일회-사인-온 기능을 사용하면 관리자는 개별 조직이나 서비스 수준이 아닌 스마트시티 전체 또는 전체 관리 수준에서 사용자 활동을 추적하고 사용자 보안을 관리 할 수 있다. 따라서 스마트시티 관리 시스템은 일회-사인-온 기능을 통해 보다 효율적인 관리와 일관된 방식으로 보안 관리를 위한 토탈 솔루션을 제공 할 수 있다.

4. UTOPIA에서의 통합 인증

본 절에서는 SmartUM 미들웨어의 최상위 층인 응용 보안 계층이 제공하는 통합 인증에 대하여 상세한 구조와 작동원리를 설명한다. UTOPIA의 일회-사인-온 기능은 Fig. 3 및 Fig. 4와 같이 작동한다. 사용자가 스마트시티 서비스를 사용하기 위해 스마트시티 포털을 통해 UTOPIA에 액세스하면 로그인 기능이 시작된다. UTOPIA 로그인 기능의 일회-사인-온 기능 에이전트는 Security Assertion Markup Language (SAML) 요청을 사용하여 사용자 정보를 인증 관리자에게 전송한다. 각 단계의 SAML 메시지는 Secure Sockets Layer (SSL) 프로토콜을 사용하여 암호화된다. 그런 다음, 인증 관리자는 자격 증명 데이터베이스에 요청하여 보안 심사를 수행하여 결정한다. UTOPIA는 일회-사인-온 기능을 사용하기 때문에 사용자는 UTOPIA의 여러 조직에서 제공

하는 여러 가지 서비스를 사용하고자 할 때 여러 번 로그인 할 필요가 없다.

Fig. 2. The unified authentication management in UTOPIA

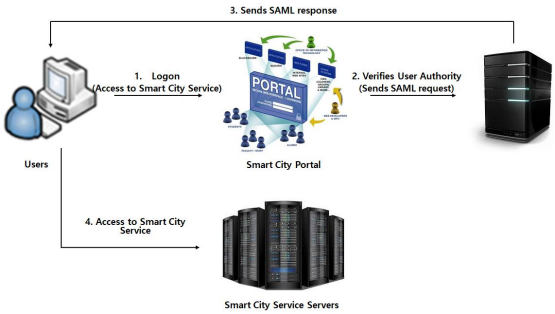

Fig. 3. The unified authentication process in UTOPIA

5. UTOPIA 통합인증시스템 구현

본 절에서는 SmartUM 미들웨어의 최상위 계층인 어플리케이션 보안 계층에, 어떻게 SAML 기반 일회-사인-온 기능을 구현하였는지에 대하여 상세히 설명한다. Fig. 3는 UTOPIA가 SAML 기반 일회-사인-온 기능을 처리하는 방법을 보여준다. UTOPIA에 어떻게 구현되었는지 구현 내용과, 어떻게 작동하는지 작동 메커니즘을, Fig. 4를 사용하여, 아래에 설명한다.

SAML은 일회-사인-온 기능을 구현을 지원한다. OpenSAML2 라이브러리와 openssl을 사용하였다. RSA 키 쌍(pair)은 인증을 위해 openssl을 사용하여 생성된다. RSA 키 쌍은 UTOPIA_sso_private.der와 UTOPIA_sso_public.der로 이루어진다. SSO는 원본 RSA 공개 키로 구현되었다.

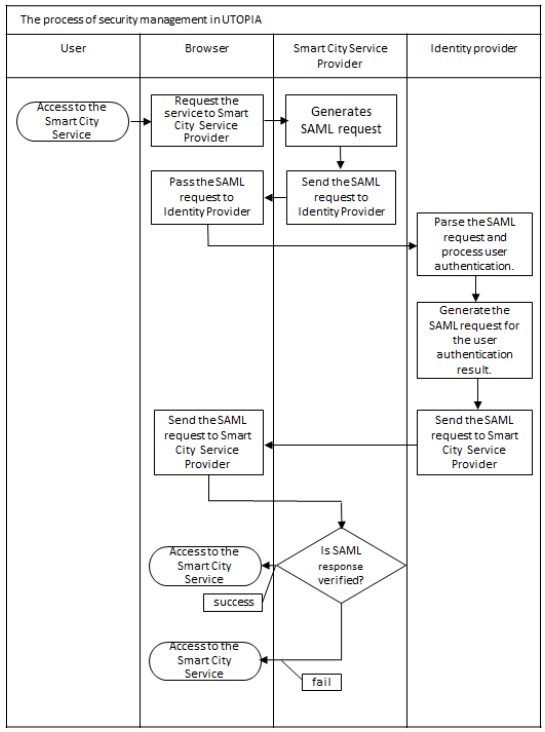

Fig. 4. The SSO based unified user authentication in UTOPIA

사용자가 스마트시티 서비스를 사용하기 위해 UTOPIA 포털을 액세스하면, 인증을 위하여, 먼저 ServiceProviderForm이 작동하는데, ServiceProviderForm은 loginForm, providerName, RelayState, acsURI 등으로 구성되어 있다. 각각의 역할은 다음과 같다. LoginForm은 ID 공급자의 인증을 위한 요소이다. ProviderName은 서비스를 제공하는 서비스 공급자의 이름이다. RelayState는 ACS 인증 후 리디렉션 된 서비스 페이지이다. AcsURI는 ID 공급자의 SAMLResponse를 확인하기위한 URL이다.

스마트시티 서비스 공급자는 SAMLRequest를 XML 형식으로 생성한다. SAMLRequest는 사용자의 브라우저를 통해 인증 공급자인 Identity Provide로 전송된다. 인증 공급자는 SAMLRequest를 구문 분석하고 사용자 인증을 처리한다. 인증 공급자는 SAMLResponse를 생성한다. 인증 공급자는 SAMLResponse를 사용자 브라우저를 통해 ACS (Assertion Consumer Service)로 보낸다. 서비스 공급자의 ACS는 인증 공급자가 보낸 SAMLResponse를 수신하고 유효성을 검사한다.

검증에 통과하면, 서비스 제공자는 사용자에게

UTOPIA의 인증 허가를 준다. 이제, 사용자는 UTOPIA의 인증관문을 성공적으로 통과하여, 원하는 스마트시티 서비스들을 사용할 수 있게 된다.

이와 같이 인증에 통과한 사용자만이 시스템을 사용할 수 있게 함으로서, 유토피아 시스템은 외부 침입을 원천적으로 차단하고 있다. 이 인증시스템이 없을 때는, 3장에서 설명하는 여러 인증 방법이 유기적으로 연결되어 시행되지 못하였으나, 본 논문의 인증시스템을 사용함으로서, 이 문제를 해결하였다.

6. 결론

지금까지, UTOPIA 스마트시티 시스템과 SmartUM 미들웨어에서, 어플리케이션 보안 계층이 어떻게 설계되어 구현되었는지와, 어떤 종류의 사용자 인증이 어떻게 어플리케이션 보안 계층에 적용되었는지를 작동원리와 함께 소개하였다. 또한, UTOPIA 스마트시티 시스템에 구현된 일회-사인-온을 사용하여 이 모든 사용자 인증을 통합하여 어떻게 보안관리를 실행하는지 설명하였다.

UTOPIA는 모든 UTOPIA 서비스에 대해 여러 가지 사용자 인증 방법과 기술을 지원하면서, 이를 통합적으로 인증 관리하는 기능을 제공한다. 아이디와 암호를 사용하는 보편적인 인증방법과 함께, 엠티엠(MTM), 지문인식등의 바이오 프로필, IP 위치인식, 지식기반인증, 일회성 암호, 대역외 인증, 아이핀 인증 등의 사용자 인증 기술을 지원함과 동시에, 사용자는 UTOPIA 포털을 통하여 한번만 사용자 인증 기능을 거침으로서, 여러 기관에서 제공하는 UTOPIA 서비스를 사용할 때에, 매번 여러 기관에서 사용자 인증을 해야 하는 불편 없이, UTOPIA 스마트시티에서 제공하는 모든 서비스를 사용할 수 있게 되었다. 향후 작업에서는 보다 세분화 된 권한 관리에 대한 연구개발을 하고자 한다. 여러 가지 지능적인 서비스를 사용자들에게 제공하는 스마트시티에서는 보안 관리가 필수적이다. 따라서 본 논문에서 제안한 방법론과 보안계층 뿐만 아니라 다른 보안 이슈에 대한 연구가 지속되어야 한다.

감사의 글

스마트시티사업단과 서울그리드센터의 관련된 분들에게 감사드립니다. 특히, 최근의 스마트시티 연구동향, 논문 교정 등에 관한 조언을 주신, 정혜선, 박종원, 윤철상 연구원에게 깊이 감사드립니다.

REFERENCES

[1] Ministry of Land, Infrastructure and Transport, *Act on Smart City Creation and Industry Promotion, etc. This Decree enter into force on Sept.* 22, 2017. Law No.14718.

[2] ISO/IEC JTC1. (2014). *Smart Cities Report.*

[3] H. S. Jung, C. S. Jeong, Y. W. LEE, & P. D. Hong. (2009). *An Intelligent Ubiquitous Middleware for U-city: SmartUM, Journal of Information Science and Engineering, 25(2)*, 375-388.
DOI: 10.1688/JISE.2009.25.2.3

[4] A. Armando, R. Carbone, L. Compagna, J. Cuellar, & L. Tobarra. (2008). *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.*
DOI : 10.1145/1456396.1456397

[5] European Union. (2018). *The Marketplace of the European Innovation Partnership on Smart Cities and Communities.*
https://eu-smartcities.eu/.

[6] S. K.. Yoon & H. S. Jang. (2011). *Design of Information Security in Ubiquitous City, Journal of Information and Security, 11(4),* 37-42.
ISSN: 1598-7329

[7] Y. S. Kim & S. C. Park. (2008). *Analysis and Protection Method of Security Threat Factor in u-City Management Center, Proc. Korean Society For Internet Information,* 9(1), 129-132.
ISSN: 1738-9593

[8] C. J. Chae, S. K. Han & H. J. Cho. (2016). *Security Vulnerability and Countermeasures in Smart Farm, Journal of digital convergence, 14(11)*, 313-318, DOI: 10.14400/JDC.2016.14.11.313

[9] J. N. Kim. (2016). *Implementation of Domain Separation-based Security Platform for Smart Device, Journal of digital convergence, 14(12)*, 471-476.
DOI: 10.14400/JDC.2016.14.12.471

[10] S. J. Kim & D. E. Cho. (2012). *A Study on Secure Home Network in Environment Smart Grid, Journal of digital convergence, 10(1)*, 463-469.
DOI: G704-002010.2012.10.1.001

[11] J. Hoh and C. Y. Jung. (2017). Convergence-based Smart Factory Security Threats and Response Trends. *Journal of the Korea Convergence Society, 8(11)*, 29-35, DOI: 10.15207/JKCS.2017.8.11.029

[12] S. W. Lee, J. J. N. Kim. (2017). Service-oriented protocol security framework in ICT converged industrial environment. *Journal of the Korea Convergence Society, 8(12)*, 15-22. DOI: 10.15207/JKCS.2017.8.12.015

[13] K. H. Lee. (2010). Analysis of Threats Factor in IT Convergence Security. *Journal of the Korea Convergence Society, 1(1)*, 2233-4890. ISSN: 2233-4890

[14] S. H. Lee, D. H. Shim & D. W. Lee. (2016). Actual Cases of Internet of Thing on Smart City Industry. *Journal of Convergence for Information Technology, 6(4)*. 65-70. DOI: 10.22156/CS4SMB.2016.6.4.065

[15] S. W. Rho & Y. W. Lee. (2010). *U-city Portal For Smart Ubiquitous Middleware, 2010 The 12th International Conference Advanced Communication Technology (ICACT)*, 609-613. ISBN: 978-1-4244-5427-3

[16] S. W. Rho, C. H. Yun & Y. W. Lee. (2011). *Provision of U-city web services using cloud computing, 13th International Conference on Advanced Communication Technology (ICACT)*, 1545-1549. ISBN: 978-89-5519-154-7

[17] P. Beynon-Davies. (2010). *Personal identity management as a socio-technical network, Technology analysis & strategic management,* 22(4), 463-478. DOI: 10.1080/09537321003714527

[18] G. Bick, M. C. Jacobson & R. Abratt. (2003). *The Corporate Identity Management Process Revisited, Journal Of Marketing Management,* 19(7-8), 835-856. DOI: 10.1080/0267257X.2003.9728239

[19] *Trusted Computing Group website.* (2011). http://www.trustedcomputinggroup.org.

[20] H. S. Kim & C. S. Park. (2010). *Cloud Computing and Personal Authentication Service, Information & Communications Magazine, 20(2)*, 11-92. ISSN: 1598-3978

[21] A. Litan. (2009). *Where String Authentication Fails and What You Can About It, Gartner Research.*

[22] Y. Oh, T. Obi, J. S. Lee, H. Suzuki, & N. Ohyama. (2010). *Empirical analysis of internet identity misuse: case study of south Korean real name system, the 6th ACM workshop on Digital identity management (DIM '10),* 27-34. DOI: 10.1145/1866855.1866863

[23] S. K. Un, N. S. Jho, Y. H. Kim & D. S. Choi. (2009). *Cloud Computing Security Technology, Electrical Communication Trend Analysis, 24(4),* 79-88. p-ISSN: 1225-6455

황 의 동(Hwang, Eui Dong) [정회원]

- 1989년 2월 : 서울과학기술대학교 전산학과(공학사)
- 1994년 2월 : 성균관대학교 전산 감사학과(행정학석사)
- 2011년 2월 ~ 현재 : 서울시립대학교 전자전기컴퓨터학과 박사과정
- 관심분야 : 스마트시티, 보안관리
- E-Mail : hed0901@hanmail.net

이 용 우(LEE, Yong Woo) [정회원]

- 1981년 : 서울대학교 전기공학과 (학사)
- 1981년 : Schlumberger Inc. International Engineer.
- 1982년 ~ 1998년 : KIST 선임연구원
- 1997년 : 영국 에딘버러대학교 컴퓨터학과 (박사)
- 1998년 : 한국교육학술정보연구원, 책임연구원
- 1999년 ~ 현재 : 서울시립대학교 전자전기컴퓨터공학부 교수
- E-Mail : ywlee@uos.ac.kr