Journal of the Korea Convergence Society
Vol. 10. No. 1, pp. 25-33, 2019

ISSN 2233-4890
https://doi.org/10.15207/JKCS.2019.10.1.025

쓰리 티어 방식의 스마트시티 관리시스템에서의 보안 관리

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

Smart City Security Management in Three Tier 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 스마트시티 시스템에서 다루는 데이터는 개인의 사생활이나, 공공재적인 요소가 많기 때문에 보안이 중요하며, 따라서 스마트시티 시스템에서 보안에 대한 연구는 필요하다. 본 논문에서는 3 티어(Tier)로 구성된 스마트시티 시스템을 위한 보안 요소들을 정의하고, 각각에 필요한 기술들에 대해서 기술한다. 또한, 스마트시티 시스템에서 가장 중요한 이슈 중 하나인 도시구성요소와 미들웨어와의 보안 관리를 위하여 스마트시티 미들웨어에 보안계층을 설계하고 구현한 내용을 소개한다. 인프라보안계층은 블록 암호 (Block Cipher) 알고리즘과 메시지 다이제스트 알고리즘을 기반으로 구성되었으며, 이를 통해 데이터의 기밀성과 무결성을 보장하고, 정책서버를 통한 장치 접근 관리를 하여 인가된 장치만 스마트시티 구성요소를 관리할 수 있도록 한다.

주제어 : 스마트시티, 스마트시티 미들웨어, 스마트시티 보안, 보안 계층, 인프라보안관리

Abstract The security of the data dealt by the smart city system is important because they have many privacy and public information. Therefore, it is necessary to study security in the smart city system. In this paper, we define the security factors for the smart city system composed of three tiers and describe the technologies for each. In addition, the design and implementation of the security layer in the Smart City middleware for the security management of the urban component in the Smart City Infrastructure and middleware, which is one of the most important issues in the Smart City system, is introduced.

Key Words : Smart City, Smart City Middleware, Smart City Security, Security Layer, Infrastructure Security Management

1. 서론

유시티(U-City: Ubiquitous City)는 유비쿼터스 도시의 건설 등에 관한 법률[1]에 따르면 “도시민의 삶의 질과 도시의 경쟁력 향상을 위하여 도시공간에 유시티기술을 구현함으로써 언제 어디서나 유시티서비스를 제공하는 도시”라고 정의하고 있다. 유시티는 스마트시티로 발전하였다. 스마트시티는 법률에 따르면 “도시의 경쟁력과 삶의 질의 향상을 위하여 건설·정보통신기술 등을 융·복합하여 건설된 도시기반시설을 바탕으로 다양한 도시

*Corresponding Author : Yong-Woo Lee (ywlee@uos.ac.kr)
Received September 11, 2018 Revised December 31, 2018
Accepted January 20, 2019 Published January 28, 2019

서비스를 제공하는 지속가능한 도시를 말한다[2].” 라고 정의하고 있다.

서울시의 지원을 받은 스마트시티사업단에서는 스마트시티가 다양한 지능적인 서비스들을 사용자에게 제공하기 위하여 3 티어로 이루어진 유토피아(UTOPIA) 스마트시티를 제안하였다. UTOPIA 스마트시티는 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)이 융합된 스마트시티에서, 언제 어디에서나 스마트시티의 인프라를 이용할 수 있으려면, 다양한 정보통신기술을 사용하여, 도시의 요소들을 유기적으로 연결하고 관리하여야 하다. 스마트시티를 하나의 시스템으로 유기적으로 관리하기 위해서는 스마트시티를 위한 전용 운영체제의 역할을 하는 미들웨어가 필요하다. 스마트시티 전용 미들웨어는 도시에서 생성되는 데이터 및 도시 인프라를 관리 하여야 하기 때문에 무엇보다 보안에 대한 고려가 필요하다. 하지만, 기존의 보안 솔루션 및 보안 기법들을 각각 산발적으로 적용한다면, 각각의 영역에 대한 보안만을 제공하고, 스마트시티 보안을 위한 통합적인 보안을 제공하지 못하게 된다. 본 논문에서는 스마트시티 시스템을 통합적으로 보안한 UTOPIA 스마트시티 보안 시스템을 제안한다.

본 논문은 다음과 같이 구성되었다. 2장에서는 UTOPIA 스마트시티의 보안의 필요성에 대해서 설명하고, SSL과 IPSec을 UTOPIA 스마트시티 인프라 보안계층과 비교하며 UTOPIA 인프라 보안계층의 필요성에 대해 설명한다. 3장에서는 UTOPIA 스마트시티 시스템에서의 보안 이슈 및 UTOPIA 스마트시티 시스템의 보안계층에 대해 설명한다. 4장에서는 UTOPIA 스마트시티 미들웨어 티어 내에 위치하면서 UTOPIA 스마트시티 인프라스트럭처 티어와의 연결 운영의 보안을 책임지는 인프라 보안계층에 대해 다룬다. 마지막으로 5장에서는 결론과 향후 연구 방향에 대해 다룬다.

2. 관련연구

네트워크 보안 기술에는 네트워크 보안 일반, 전송계층 보안, IP 보안, 이동통신 보안, 무선 및 모바일통신 보안 등이 있다. 이를 스마트시티에 적용한 보안에 대한 연구는 많지 않다[4-6].

스마트시티 서비스들은 지리정보체계 (GIS: Geographic Information System) 데이터와 같은 복합적이고 큰 규모의 공간 정보들을 처리하기 때문에 많은 자원을 필요로 하며, 따라서 스마트시티사업단에서는 많은 자원들을 처리할 수 있도록 클라우드 컴퓨팅 기술을 스마트시티 시스템에 적용하여 UTOPIA 스마트시티를 위한 SmartUM 미들웨어를 제작하였다. UTOPIA 스마트시티는 여러 가지 지능적인 솔루션을 실시간으로 사용자들에게 제공하기 위해 클라우드 컴퓨팅 자원들을 관리한다[7]. 따라서, UTOPIA 스마트시티를 보안하기 위해서는 참고문헌[8]에서 언급하는 클라우드 컴퓨팅 환경의 보안관리도 감안하여야 한다. 즉, 클라우드 컴퓨팅 환경에서의 보안관리는 UTOPIA 스마트시티의 성공적인 운영을 위한 중요한 이슈 중 하나이다. 참고문헌 [9]와 [10]은 스마트시티사업단이 수행한 이에 관한 연구의 결과를 담고 있다. 이 참고 문헌외에는, 아직 스마트시티에서의 클라우드 컴퓨팅에 관한 보안 관리에 대한 연구는 찾아보기가 어렵다.

참고문헌[11-13]은 스마트시티 이전 버전인 유시티에서의 보안에 관한 내용을 담고 있다. 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[14-16].

3. 스마트시티 보안

UTOPIA 스마트시티는 스마트시티를 통합적으로 관리하기 위한 시스템으로 크게 UTOPIA 스마트시티 포탈 티어, 지능적인 여러 솔루션을 제공하는 UTOPIA 스마트시티 미들웨어 티어, 그리고 UTOPIA 스마트시티 인프라스트럭처 티어의 세 가지 티어로 구성되어 있다. UTOPIA 스마트시티 포탈티어는 사용자들이 온라인으로 다양한 스마트시티 서비스들을 이용할 수 있는 역할을 한다. UTOPIA 스마트시티 미들웨어 티어는 스마트시티 인프라스트럭쳐 티어에서 전송된 데이터들을 처리하는 역할을 한다. UTOPIA 스마트시티 인프라스트럭처 티어는 UTOPIA 스마트시티로 연결되어 통합운영되는 UTOPIA 스마트시티의 각 구성요소들로 구성되어져 있

다[3].

UTOPIA 스마트시티의 보안을 보장하기 위해서, UTOPIA 스마트시티 포탈 티어, UTOPIA 스마트시티 미들웨어 티어, UTOPIA 스마트시티 인프라스트럭처 티어의 각 티어에서 지원되는 보안요소들을 각 티어별로 기술하고, 각각에 기술들에 대해서 설명한다.

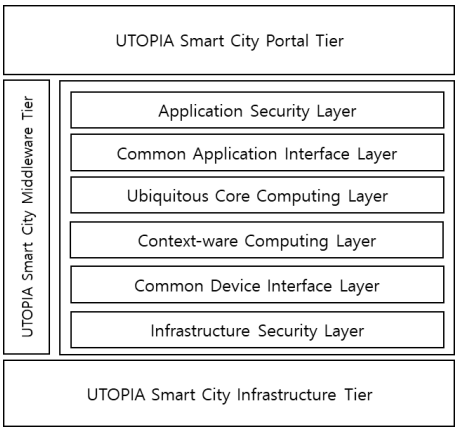

Fig. 1. UTOPIA three tiers structure

3.1 UTOPIA 스마트시티 포탈 보안

UTOPIA 스마트시티 포탈이 보안성을 유지하기 위해서 시스템 보안, 서비스 보안, 개인정보보호를 지원해야 한다.

시스템 보안으로는 서버 보안, 데이터베이스 보안 등이 필요하다. 서버보안은 미들웨어 시스템을 보호하고 스마트시티 시스템에 저장된 데이터나 정보를 보호하기 위해서 필요하다. 이를 위해서는 운영체제에 최신 보안 업데이트 적용, 운영체제 취약점 점검, 웹 서버 전용 호스트 구축, 서버에 대한 접근제어, 중요한 서버는 DMZ(Demilitarized Zone) 영역에 배치, 관리자 계정관리 철저, 파일접근 권한 설정 등을 지원한다. UTOPIA 스마트시티는 분산 서비스 거부 공격(DDoS: Distributed Denial of Service attack) 공격 등의 위협에 대비하여야 하며, 상용인터넷망을 통한 해킹, 모바일 기기를 경유하여 인트라넷 서버에 접속하여 가해지는 여러 보안 위협을 방어할 수 있어야 한다. 데이터베이스 보안으로는, 정보의 최종 저장소인 데이터베이스에 대한 사전 접근통제, 데이터 암호화, 감사 등의 보안을 지원한다[17,18]. 스마트시티의 중요한 정보를 내부, 외부에 존재하는 유출 시도로부터 안전하게 보호하기 위해 데이터암호화, 접근제어, 감사기능, 보안에 관한 통계 및 리포팅 등을 포함하는 보안관리를 지원한다.

서비스 보안으로는 웹 보안, 이메일 보안, 통합인증(SSO: Single Sign-On) 보안 등이 지원된다. 웹 보안 게이트웨이로 로직 분석을 통한 웹 공격 탐지, 개인정보 노출 차단 등의 보안기능과 더불어 대쉬보드, 설정마법사와 같은 관리기능이 제공된다. 이메일 보안은 무분별한 메일발송으로 인한 업무효율 저하와 중요한 정보 유출을 막을 수 있는 기능을 제공한다. SSO 보안은 하나의 아이디로 여러 사이트를 이용할 수 있는 보안 방식으로서, 여러 개의 사이트를 이용하는 사용자를 통합 관리하는데 필요하다. SSO 방식을 스마트시티에 적용함으로써, 시스템 마다 사용자가 별도의 로그인 하지 않고서도 모든 서비스를 제공받을 수 있게 해준다. 또한, 사용자 접속 로그에 대한 투명성 제공과 더불어, 신뢰성을 높일 수 있고, 스마트시티의 서비스에 들어가는 비용을 줄이고 효율성을 높이는데 기여한다.

개인정보보호기능으로 ID관리/개인정보보호와 키보드 보안 등을 지원한다. ID관리 기술은 인증정보를 비롯한 개인의 특징, 신상정보, 선호도와 같은 ID의 생성부터, 변경, 유통, 폐기 등에 대한 라이프 사이클을 인터넷 환경에서 안전하고 통합적으로 관리하는 기능이다. 개인정보보호 기능은 사용자의 개인정보를 보호하기 위한 기술 및 정책을 필요로 한다. ID관리 및 개인정보보호기능은 사용자의 편의성과 안전성, 개인정보 보호 수준을 높인다. 이를 통하여, 시스템 보호 및 안전한 조직 간 서비스 연계 가 가능하다. 차세대 웹 환경과, IP 기반의 통합망인 차세대통신망/광대역통합망(NGN: Next Generation Network / BcN: Broadband Convergence Network) 과 클라우드 컴퓨팅 환경에서도 개인정보 보호가 가능하도록 지원한다.

3.2 UTOPIA 스마트시티 미들웨어 보안

UTOPIA 스마트시티 미들웨어인 SmartUM 미들웨어 보안에는 기반 보호 기능, 통신 및 네트워크 보안 기능, 보안 관리 기능 등이 지원된다. 기반보호는 스마트시티 미들웨어 해킹 등 위협으로부터 보호할 수 있도록 취약점 분석 및 평가, 보호대책 수립 등에 필요한 기술을 지원하여 스마트시티 기반 시설의 안정적인 운영을 도모하는 것을 말한다. UTOPIA 스마트시티 미들웨어 서버에 침입하여 악의적으로 스마트시티를 오작동 시키는 것과

스마트시티 시스템을 파괴하는 행위를 차단할 수 있어야 한다. 기반 보호 기능에는 암호기능, 인증기능, 디렉토리 서비스 기능 등이 있다. 암호기능은 유비쿼터스 컴퓨팅 환경에 적합한 초경량/저전력/초고속 암호 기능과 IT 서비스 이용과정에서 발생될 수 있는 프라이버시 침해 방지를 위한 보안 프로토콜 기능 등이 지원된다. 암호키를 알아내기 위한 암호 알고리듬에 대한 공격은 공격자가 제어할 수 있는 정보의 종류와 양에 따라서 블랙박스 공격, 그레이박스 공격, 화이트박스 공격으로 분류할 수 있는데, 이를 막아내는 기능들이 지원된다. UTOPIA 스마트시티의 포탈의 보안을 지원하기 위하여 SmartUM 미들웨어가 제공하는 인증기능으로서 공개키기반구조(PKI : Privilege Management Infrastructure) 인증기능을 지원한다. 공개키기반구조는 공개키 암호기술에 기반을 둔 인증서의 생성 관리를 담당한다. 인증서 프로파일, 인증서 관리 프로토콜, 인증서 운영프로토콜, 인증서 검증 프로토콜, 사용자 인터페이스 기술, 전자서명 키 보호 기술 등을 이용하여 보안 서비스를 제공할 수 있게 한다. 공개키기반구조의 보안은 UTOPIA 스마트시티의 인트라넷 구축, 기관 간의 전자문서 교환 등에 적용되어 진다. 키관리를 통하여, 보안 정책에 의거한 키의 생성, 등록, 인가, 등록 취소, 분배, 설치, 저장, 압축, 폐지, 유도와 파괴를 감독한다. 키관리를 위하여, 데이터 무결성과 기밀성과 같은 서비스를 제공할 수 있는 잘 설정된 암호 기법을 필요로 한다. 트리플 데이터 암호화 표준(Triple-DES: Data Encryption Standard), 고급 암호화 표준(AES: Advanced Encryption Standard)와 같은 대칭 암호 기법들은 스마트시티 서비스에서 매우 유용하므로 SamrtUM 미들웨어에서 지원한다. 디렉토리 서비스(LDAP: Lightweight Directory Access protocol) 는 UTOPIA 스마트시티 내의 정보를 인터넷 프로토콜을 이용하여 접근할 필요가 있는 경우에 주로 사용된다. 특히 UTOPIA 스마트시티 자료를 대외적으로 공개할 목적으로 사용되며, 일반 데이터베이스에 비해 빠른 검색능력과 표준화된 인터페이스 및 자료정의가 가능하다. LDAP의 주요 서비스 컴포넌트는 다음과 같다. 사용자 통합인증 및 SSO Repository, 보안 및 권한정보 제공, 주소록, 조직도 및 조직 내의 정보, 서비스, Configuration 및 기타 Profile 정보이다. 디렉토리시스템에서, 시스템관리자와 보안관리자의 업무권한 설정이 분명히 하기 위하여, 접근통제, 필요한 특정자료암호화 등 보안에 관한 사항은 오직 보안 관리자만이 권한을 갖도록 분리하는 기능이 스마트시티 미들웨어 티어의 보안을 위하여 지원된다.

통신 및 네트워크 보안을 위하여, 침입방지시스템(IPS: Intrusion Prevention System), 가상사설망(VPN: Virtual Private Network), 네트워크접근제어(NAC: Network Access Control) 등이 지원된다. IPS는 네트워크에서 공격 시그니처를 탐지하여 자동으로 조치를 취함으로써 비정상적인 행위를 중단시키는 보안 솔루션이다. 침입 경고 이전에 공격을 중단시키는데 초점을 두고 정보 유출을 자동으로 탐지하여 차단 조치를 취함으로써 인가자의 비정상 행위를 통제하는 것을 지원한다[19-21]. VPN은 인터넷과 같은 공중망(public network)을 마치 전용선처럼 사용할 수 있도록 구축한 것으로서, VPN으로 구축된 가상사설망은 별도로 값비싼 장비나 소프트웨어를 구입하고 관리할 필요가 없고 전용회선에 비해 비용 절감 효과를 기대할 수 있어서 UTOPIA 스마트시티는 VPN을 주요 네트워크요소로 지원한다. NAC는 스마트시티 네트워크 상에서 확산되는 보안위협 경로를 미리 차단해 사전 방어적인 네트워크 보안체계를 구현하는 것을 목적으로 한다. 이에 대한 보안 기능들이 지원된다.

보안관리 기능을 위하여 UTOPIA 스마트시티는 ISO 27001를 따른다. 정보보안관리(ISMS: Information Security Management System))는 BS 7799를 기반으로 한 ISO 17799의 인증 체계를 대부분 수용해 국제표준인 ISO 27001로 발전되었다. 스마트시티 미들웨어에서의 정보보안관리는 이를 근거로 하여, 정보자산의 비밀성, 무결성, 가용성 등 정보보호 목적의 적절한 수준을 달성하고 유지하는 것을 목표로 하고 있다. SmartUM 미들웨어의 정보보안관리는 이 목표를 달성하기 위한 활동을 기획, 구현, 운영하기 위한 일련의 관리과정과 이를 위한 정보보호대책으로 구성되어 있다.

3.3 스마트시티 인프라스트럭처티어 보안

UTOPIA 스마트시티의 스마트시티 인프라스트럭처티어를 위해 지원되는 보안에는 원거리 유선 무선 복합 정보통신의 보안, RFID/USN 보안, 바이오 인식 등이 있다.

원거리 유선 무선 복합 정보통신 보안은 원거리 유선 무선 복합 정보통신을 통하여 연결되고 원격조정되는 스마트시티 인프라의 원격장치들의 인가된 조정과 운영 외에는 차단될 수 있도록 보안 기능을 제공 한다. 원격 장치들의 펌웨어 변조에 따라 보안 기능을 약화시킬 가능

성을 차단하고, 무선구간에서 패킷 스니핑(패킷 가로채기) 등의 여러 보안 위협을 방어할 수 있도록 지원한다.

RFID/USN보안은 BcN 보안 기술과 함께 스마트시티 구축에 있어서 매우 중요한 보안요소이다. 스마트시티 인프라에서의 사물의 자동식별과 이력추적 등의 RFID/USN 이용서비스를 제공할 때에 정보누출을 막을 수 있고, 개인 프라이버시를 보호할 수 있도록 지원한다.

UTOPIA 스마트시티 인프라스트럭처티어 보안에서는 UTOPIA 스마트시티 인프라의 각 장치들을 보안하기 위하여 바이오 인식을 지원한다. 사람마다 고유한 생체정보 등을 개인 식별의 수단으로 활용하고, 이를 자동화된 수단으로 등록·저장하여 제시한 바이오정보와 비교/판단하여 접근 제어 분야에서 다양한 보안 서비스를 제공하는 기능을 지원할 수 있게 설계되었다. 지문·안면·홍채·망막·정맥 등의 신체적 특성을 이용한 방법과 서명·음성·걸음걸이 등의 행동학적 특성을 이용하는 방법이 대표적인 보안 기능들이다[22, 23]. 바이오인식 기반의 스마트시티 인프라에 대한 출입관리, 범죄 활동을 인식하여 봉쇄할 수 있는 보안관리, 네트워크 인프라 및 중요 시스템에 대한 접근통제 등에 바이오 인식 기술을 적용함으로서 기간 시설의 안전성을 확보할 수 있도록 지원한다.

4. 스마트시티 미들웨어의 인프라 보안

본 절에서는 SmartUM 미들웨어 내부에, 스마트시티 인프라(구성요소)에 대한 접근 보안을 실행하기 위하여 스마트시티 인프라 보안 계층을 구축하는 것을 제안하고 그 내용과 작동 메커니즘을 상세히 설명한다.

UTOPIA 스마트시티의 SmartUM 미들웨어의 보안 계층은 그림 1에서 보듯이 1층과 6층에 자리잡고 있다. UTOPIA 스마트시티 어플리케이션 보안 계층은 6층에 위치하면서, UTOPIA 스마티시티 포탈 티어를 통한 사용자의 접근에 대한 보안을 담당하고 있다. 본 절에서는 1층의 UTOPIA 스마트시티 인프라 보안 계층에 대하여 상세한 구조와 작동원리를 설명한다. 인프라 보안 계층은 3장에서 설명한 UTOPIA 스마트시티의 여러 가지 보안 이슈들 중에서 통신과 통신망의 보안을 위주로 구현되었다

UTOPIA 스마트시티에서는 UTOPIA 스마트시티 인프라스트럭처 티어의 원격장치들은 인프라 보안 계층에서 제공하는 보안모듈을 통해 데이터를 송수신한다. 이를 통하여, SmartUM 미들웨어와 원격장치들간의 데이터 송수신에 있어서 보안을 유지 할 수 있도록 하였다. 또한, 장치 접근 제어 기능을 이용하여 인가된 장치만 접근 할 수 있도록 하였다.

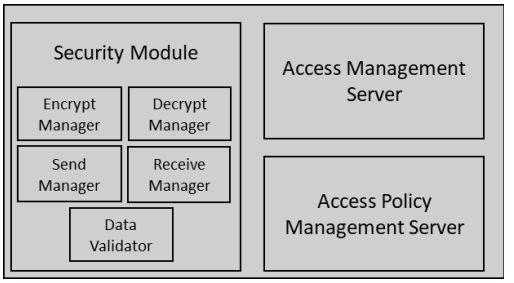

Fig. 2. Infrastructure security layer in smart city middleware

UTOPIA 스마트시티의 SmartUM 미들웨어의 인프라 보안 계층은 SmartUM 미들웨어에서 원격에 있는 인프라스트럭처 장치들에 대한 전반적인 인터페이스를 제공하는 인프라장치 인터페이스 계층의 아래에 위치하면서 원격에 있는 인프라스트럭처 장치들과의 정보통신에 있어서 보안을 담당한다.

인프라 보안 계층에서는, 데이터 송수신의 과정에 데이터에 대한 암호와 복호화 및 검증을 수행할 수 있다. 인프라 보안계층에서는 보안 모듈의 동작에 관련된 전반적인 인터페이스를 제공하며 보안 모듈의 동작을 관리한다. 따라서 SmartUM 미들웨어와 장치들과의 송수신되는 데이터에 대한 무결성과 신뢰성을 보장 한다.

인프라 보안계층에서 제공하는 모듈은 크게 5가지로 나누어 지며, 그 역할은 다음과 같다: 암호화 관리자는 블록 암호(Block Cipher)를 통한 데이터 암호화를 수행한다. 복호화 관리자는 블록사이퍼를 통한 데이터 복호화를 수행한다. 데이터 검증기는 메시지 다이제스트 및 데이터 검증을 수행한다. 송신관리자는 암호화된 데이터를 송신한다, 수신관리자는 암호화된 데이터를 수신하는 역할을 수행한다.

SmartUM 미들웨어의 인프라 보안계층은 정책적으로 미리 설정된 블록 암호 알고리즘[24], 키, 그리고 해시함수[25]를 바탕으로 몇 단계에 걸쳐 데이터에 대한 암호화와 복호화 및 인증을 수행한다. 암호화와 복호화 그리고 인증은 인프라 보안 계층의 여러 모듈들의 협업으로 이루어진다.

4.1 장치 접근 관리 보안

먼저, 데이터를 전송하고자 하는 장치에 대한 접근 허용을 위한 접근 관리가 필요하다. 장치 인증을 위하여, 장치 접근 요청자, 장치 접근 정책관리 서버, 장치 접근 정책 집행 서버 등의 세가지의 요소를 사용한다[26]. 장치 접근 요청자는 SmartUM 미들웨어에 정보 전송을 하기 위한 목적으로 접근하려는 장치를 말한다. 장치 접근 정책관리 서버는 인프라 장치의 접근 정책 및 인가정책에 따라 접근하고자 하는 장치를 점검하는 역할을 하며, 차단해야 할 장치에 대한 정보를 생성하고 저장하는 서버이다. 장치접근정책집행서버는 접근 요청에 장치에 대하여 장치접근정책관리서버가 제공하는 정보를 전달 받아 인증을 수행하고, 인가 불가 장치에 대한 차단 역할을 수행한다. 장치에 대한 인증은 접근을 요청한 장치에 대하여 저장되어 있는 정보를 사용하여 수행된다, 최초 장치가 SmartUM 미들웨어에 접근을 요청할 때 패킷 헤더에 장치의 ID, MAC 주소, IP주소, 장치 타입에 대한 정보를 함께 보내게 된다. 장치접근정책관리서버에는 로그 테이블이 존재하며, 이 로그 테이블은 인가된 장치의 ID, MAC주소, IP주소 그리고 장치 타입이 저장된 테이블과 정책 위배 사항들을 저장하고 관리한다.

장치 접근 정책의 집행은 장치접근정책집행서버에서 수행한다. SmartUM 미들웨어의 인프라 보안계층을 기반으로 구현한 장치 인증 방법의 흐름은 그림 3과 같다.

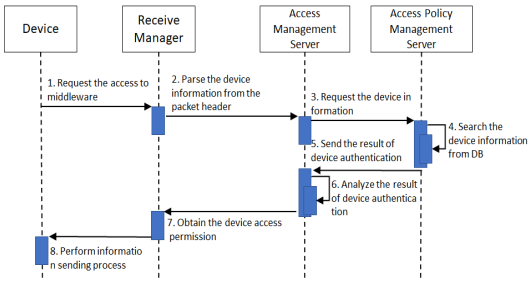

Fig. 3. The sequence diagram of authentication processing about remote devices with infrastructure security layer of SmartUM middleware

특정 장치가 SmartUM 미들웨어에 접근을 시도하면 SmartUM 미들웨어의 인프라보안계층의 수신 관리자(Receive Manager)로 접근정보 패킷이 전송된다. 이후 수신 관리자는 헤더에 포함된 장치에 대한 정보를 파싱하여 스마트시티 미들웨어의 보안계층 안에 있는 장치접근정책관리서버로 파싱된 정보를 전달한다. 장치접근정책관리서버에서는 전달 받은 정보에 대하여, 검증을 수행한다. 이 때에, 장치접근정책관리서버에서는 데이터베이스에 저장된 정보를 바탕으로 일치하는 장치가 있는지를 확인한 후에 인증 결과를 저장한다. 장치접근정책관리서버에서는 트랜스폼 세트 (Transform Set)를 사용한다. 트랜스폼 세트는 데이터의 보호 범위를 정하는 IPSec 프로토콜, 암호 방식을 정하는 암호화 알고리즘, 그리고 데이터 검증을 할 수 있도록 메시지 다이제스트를 수행하는 해쉬함수 등의 세가지 명세로 구성된다.

인증 결과가 “비인가” 인 경우에는, 접근을 요청한 장치를 비인가 장치로 차단 목록에 추가하고, 기록에 비인가 내역을 저장한다. “인가”로 결정된 경우에는, 접근 허가를 전달하는 과정을 수행한다. 인프라 장치 인터페이스 계층이 데이터 송수신을 하도록 허락한다.

4.2 데이터 보안

장치에 대한 접근이 인가되면, 데이터를 수신하고 송신할 수 있다. UTOPIA 스마트시티 인프라스트럭처의 원격장치들은 크게 두 종류로 나뉜다. 하나는 데이터 송수신할 때에, SmartUM 미들웨어의 암호화와 복호화 기능을 지원하는 장치와 그렇지 못한 장치의 두 종류로 나뉜다. SmartUM 미들웨어의 암호화와 복호화 기능을 지원하는 스마트시티 인프라스트럭처의 장치들은 인프라 보안계층의 보안 모듈 또는 이와 동일한 기능을 하는 소프트웨어를 보유하고 있어야 한다.

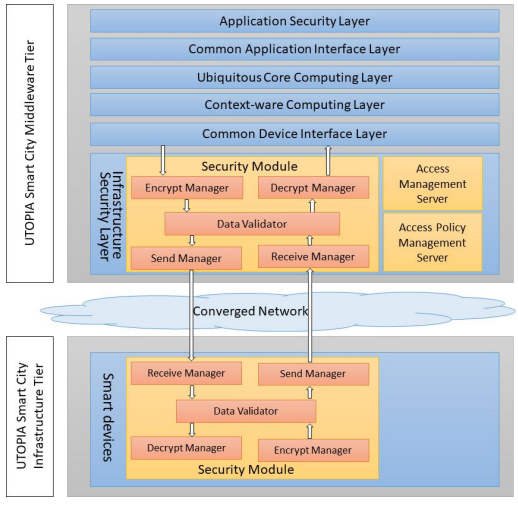

Fig. 4. Data flow of infrastructure security layer

그림 4는 SmartUM 미들웨어와 암호화와 복화화 기능을 지원하는 UTOPIA 스마트시티 인프라스트럭처의 원격장치들이 서로 데이터를 주고 받는 과정을 보여주고 있다.

SmartUM 미들웨어와 암호화와 복화화 기능을 지원하는 UTOPIA 스마트시티 인프라스트럭처의 원격장치에게 데이터를 송신하는 경우에 다음과 같은 과정으로 처리된다. 먼저, 암호화 관리자에서 데이터를 암호화한다. 다음으로, 데이터 검증기에서 암호화된 데이터에 대한 메시지 다이제스트를 수행한다. 최종적으로, 송신관리자가 패킷 헤더에 인덱스를 부여하여 암호화된 데이터를 전송한다. 송신한 데이터를 수신하는 UTOPIA 스마트시티 인프라스트럭처의 원격 장치에서는 역방향의 정보처리가 다음과 같이 진행된다. 먼저, 수신관리자가 패킷을 파싱한 후 인덱스를 확인한다. 다음으로, 데이터 검증기가 파싱된 메시지 다이제스트와 원본 메시지 다이제스트를 비교한다. 검증이 완료되면, 복호화 관리자가 암호화된 데이터를 복호화한다. 제대로 수신되었으면, 수신측은 수신확인 (Acknowledgement)을 송신 측에 보낸다. 수신확인을 받은 송신측은, 수신확인이 성공적 수신인 경우이면 다음 번 메시지를 보낸다. 만약 검증이 확인되지 않으면 재전송을 요청한다. 수신확인에 관련된 이 과정들을 데이터 송수신이 완료될 때까지 반복한다. 데이터를 수신하고 하는 경우에는 송신하고자 하는 과정의 역방향으로 처리가 진행된다.

본 논문에서 제안한 보안 시스템은 쓰리 티어 스마트시티 관리 시스템에 맞게 제안되고 제작되었다는 특징이 있다. 그렇게 함으로서, 각 티어별로 보안이 용이하다는 장점이 있고, 티어의 어느 부분으로 침입을 시도하더라도, 보안이 잘 지켜진다는 장점이 있다. 또한, 각각의 보안 요소들이 유기적으로 협력하여 크나큰 시너지 효과를 내는 큰 장점을 가지고 있다.

5. 결론

지금까지 UTOPIA 스마트시티 시스템에서의 보안 관리요소들을 살펴보고, 인프라 보안 계층의 설계에 대하여 소개하였다. 인프라 보안 계층은 UTOPIA 스마트시티 인프라스트럭처의 장치들과 스마트시티 미들웨어인 SmartUM이 서로 데이터를 송수신할 때에, 보안 관리를 위하여 개발되었다. 개발된 인프라 보안 계층은 SmartUM 미들웨어에서 구동되도록 설계되었다. 본 논문에서 그 설계 내용과 작동원리를 소개하였다.

본 논문에서 제시한 SmartUM 미들웨어의 인프라 보안계층을 사용함으로서, 송수신 되는 데이터에 대한 불법적인 접근으로부터 데이터의 기밀성, 무결성을 보장하여 가용성을 증진시킬 수 있게 되었다. 이를 통하여, UTOPIA 사용자들에게 보다 정확하고 신뢰성 있는 서비스를 제공할 수 있게 되었다.

각각의 사항에서, 각 티어별로 보안성능을 잘 설명하였다. 제안한 보안 시스템의 전체적인 보안 성능은 우수하다. 유토피아 시스템에서 보안 시스템이 유기적으로 잘 작동하여서, 개별적인 보안과 더불어, 전체적인 보안이 잘 이루어짐으로서, 우수한 보안 성능이 보장된다.

여러 가지 지능적인 서비스를 사용자들에게 제공하는 스마트시티에서는 보안관리가 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, Transport and Maritime Affairs(Ministry of land, transport and maritime affairs), Korea, *ACT ON THE CONSTRUCTION, ETC. OF UBUQUITOUS CITIES*, amended by Act No. 9705, May 22, 2009.

[2] 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.

[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] 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

[5] 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

[6] 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

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

[8] S. Ramgovind, M. Eloff & E. Smith. (2010). The Management of Security in Cloud Computing. *Information Security for South Africa (ISSA)*, 1-7, DOI: 10.1109/ISSA.2010.5588290

[9] S. M. Kim, J. O. Kim, C. H. Yun, J. W. Park, H. S. Jung & Y. W. Lee. (2011). Security Management of a Cloud-based U-City Management System, *The Second International Conference on Cloud Computing, GRIDs, and Virtualization*, 74-78. ISBN: 978-1-61208-153-3

[10] J. O. Kim, C. H. Yun, J. W. Park, T. H. Hong, K. G. Lee, E. D. Hwang, S. M. Kim & Y. W. LEE. (2011) Implementation of Security Layer for U-City Middleware, *Proc. Korean Society For Internet Information. 12(1)*. 217-218. ISSN: 1738-9593

[11] 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

[12] Y. S. Kim & S. C. Park, 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

[13] J. O. Kim, C. H. Yun, J. W. Park, T. H. Hong, K. G. Lee, E. D. Hwang, S. M. Kim, Y. W. LEE, Device Access Management in the U-City Middleware, *Proc. Korean Society For Internet Information, 12(2)*. ISSN: 1738-9593

[14] S. H. Lee & D. W. Lee. (2013) A Study on Digital Convergence and Smart City. *The Journal of Digital Convergence, 11(9),* 167-172. DOI: 10.14400/JDPM.2013.11.9.167

[15] S. H. Lee. (2014) A Case Study on Foreign Smart City. *The Journal of Digital Convergence, 12(4),* 305-310. I: 10.14400/JDC.2014.12.4.305

[16] 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

[17] K. G. Im & J. S. Kim. (2007). u-City operating Center and Platform as a u-City Infrastructure, *TTA Journal IT Standard & Test, 112*, 60-66. UCI: http://uci.or.kr/G901:A-0002388813

[18] Ministry of Public Administration and Security. (2010). *Practices Guide for Information Security Management*.[Online]. http://mois.go.kr/frt/bbs/type001/commonSelectBoardArticle.do?bbsId=BBSMSTR_000000000015&nttId=39918

[19] National Intelligence Service. (2018). *White Paper on National Information Security*, [Online]. https://isis.kisa.or.kr/ebook/ebook2.html#

[20] S. Frankel, P. Hoffman, A. Orebaugh, & R. Park. (2008). Guide to SSL VPNs. *Special Publication (Nist SP) 800-113, 87*. DOI: 10.6028/NIST.SP.800-113

[21] S. Frankel, K. Kent, R. Lewkowski, R., A. D. Orebaugh, R. W. Ritchey, & S. R. Sharma. (2005). Guide to IPsec VPNs. *Special Publication (Nist SP) 800-77, 126*. DOI: 10.6028/NIST.SP.800-77

[12] Korea Institute for Advancement of Technology. (2012) *Technical Road Map for Information Security*, [Online]. http://www.itfind.or.kr/report/analysis/read.do?selectedId=02-004-150421-000029

[23] Telecommunications Technology Association (TTA). (2009), *Information Telecommunication Technology Standards Roadmap 2009*, ISBN: 9788993092226

[24] Advanced Encryption Standard (AES). (2001) *Federal Information Processing Standards Publication 197*. DOI: 10.6028/NIST.FIPS.197

[25] Secure Hash Standard(SHS). (2015) *Federal Information Processing Standard (FIPS) 180-4*. DOI: 10.6028/NIST.FIPS.180-4

[26] D. Geer. (2010) Whatever Happened to Network Access Control Technology?. *IEEE Computer, 43*, 13-16, DOI: 10.1109/MC.2010.2692010

황 의 동(Hwang, Eui Dong) [정회원]

- 1989년 2월 : 서울과학기술대학교 전산학과(공학사)
- 1994년 2월 : 성균관대학교 전산감사학과(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