Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.27, NO.2, Apr. 2017 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2017.27.2.181

보안성 향상을 위한 IoT 서비스 시스템 구현 및 평가*

김 진 보,† 김 미 선, 서 재 현‡
목포대학교

Implementation and Evaluation of IoT Service System for Security Enhancement*

Jin-bo Kim,† Mi-sun Kim, Jae-hyun Seo‡
Mokpo University

요 약

사물인터넷은 다양한 사물들로부터 발생되는 정보를 수집·공유·분석하여 사람들에게 유용한 정보 서비스를 제공하는 것을 의미한다. 본 논문은 사물인터넷 환경에서 발생하는 서비스 접근제어, 서비스 보안 기술 그리고 ID 관리 기술에 대한 서비스 영역에서의 보안 안전성을 향상시키는 방안을 제시한다. 서비스 보안의 안전성 향상을 위해 공개키 기반의 C&C(Certificate and Capability) 서비스 토큰 인증서를 설계하고 발급할 수 있는 서비스를 구현하였다. 또한 노드 디바이스로부터 수집된 데이터를 기반으로 리소스 서비스의 생성 시 이를 효율적으로 관리하고자 LCRS(Left Child-Right Sibling) 리소스 모델관리 방안과 서비스에 대한 접근제어를 위해 리소스 서비스 URI 보안 관리하는 IoT 서비스 시스템을 구현하였다.

ABSTRACT

Internet of Things includes the whole process of collected information generated from a variety of objects, as well as analyzing and sharing it, and providing useful information services to people. This study seeks ways to improve security and safety in the areas of service security technology, ID management technology and service access control, all of which take place in the IoT environment. We have implemented the services that can design and issue C&C (Certificate and Capability) service token authentication, which is based on a public key, to improve the service security. In addition, we suggest LCRS (Left Child-Right Sibling) resource model management for the efficient control of resources when generating the resource services from the data collected from node devices. We also implemented an IoT services platform to manage URL security of the resource services and perform access control for services.

Keywords: IoT, Service Access Control, Resource Service, Service Token

I. 서 론

사람과 사물 그리고 서비스 환경의 통합화 현상은 디바이스의 경량화와 다양한 센서 기술의 개발, 소프트웨어·하드웨어·개방형 서비스플랫폼 기술, 인식·상황 인지 기술, 통신·네트워크 기술 및 응용 서비스와 매시업 기술 등 정보통신기술 발전을 통해 서로 긴밀하게 연결하는 초연결 사회를 실현시키고 있다[1]. 초연결사회는 시간과 장소의 제약 없이 모든 사물이 인터넷을 통해 각각의 정보를 공유하거나 처리할 수 있는 유비쿼터스 센서 네트워크와 사물지능통신에서 한 단계 발전한 것이다[2]. ICT 기기들이 다양하게 보급됨에 따라 우리의 생활 패턴은 변화하고 있다.

Received(09. 22. 2016), Modified(1st: 01. 09. 2017, 2nd: 02. 14. 2017), Accepted(02. 17. 2017)
* 본 논문은 2014년도 정부(미래창조과학부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. NRF-2014R1A2A1A11053774)
† 주저자, progress97@mokpo.ac.kr
‡ 교신저자, jhseo@mokpo.ac.kr(Corresponding author)

이러한 환경에 사물인터넷이라는 각각의 정보를 공유하거나 처리할 수 있는 USN과 사물지능통신을 한 단계 발전한 서비스가 새롭게 나타났다.

사물인터넷 환경은 현재 통신 디바이스의 단순 정보를 이용해 다량의 정보 서비스를 만들어 제공하고 있으며 이로 인해 정보 서비스 보안 위협은 더욱 높아지고 있다. 사물인터넷 환경에서 대두되고 있는 보안 문제는 디바이스 보안, 통신·네트워크 구간의 보안, 데이터 수집·보관·처리 단계의 보안 그리고 서비스 영역에서의 보안으로 분류된다.

본 논문은 사물 간 연결을 통해 수집된 다양한 데이터를 기반으로 상황맞춤형 서비스를 제공하는 사물인터넷 서비스 모델에 관한 보안성 향상을 위한 방안과 C&C(Certificate and Capability) 서비스 토큰을 이용한 서비스 접근제어 시스템 및 리소스 서비스 시스템을 구현하고자 한다. 구현한 CapSG(Capability Service Gateway)는 주체가 소유한 서비스 접근 권한 리스트를 이용하여 접근하고자 하는 서비스에 대한 토큰을 제시하면 인가모듈은 서비스 토큰의 유효성을 판별하고 해당 리소스 서비스에 접근할 수 있도록 허가 할 수 있다.

기존 접근제어 시스템은 주체의 서비스 요청이 반복적인 경우 반복 인증 프로세스가 진행되지만 CapSG는 시스템에서 발행한 C&C 서비스 토큰의 인증서 정보를 기반으로 인증절차의 반복 작업을 최소화 할 수 있도록 구현하였고, CST(Capability Service Token)[11]을 통한 서비스 객체 접근제어를 수행하고 주체 간 소유 토큰에 대해 위임, 폐기 및 위임 거부를 통해 서비스 토큰을 관리 할 수 있도록 하였다.

사물인터넷 서비스 접근제어 시스템에 대한 보안 안전성 평가는 금융권에서 사용자 인증을 위해 사용되는 X.509 기반의 인증서와 CapSG 에서 발급한 C&C 인증서를 비교 분석하였다. 또한 CapSG 기반에서 디바이스 제어 리소스 서비스에 대한 공격 시나리오를 통해 CVSS(Common Vulnerability Scoring System) 보안 위협 평가를 실시하여 보안 안정성을 향상시키고자 하였다. 본 논문은 다음과 같이 구성되어 있다.

2장에서는 제안된 시스템의 구현 및 평가를 위해 연구된 CapSG, 사물인터넷 서비스 모델 및 리소스 서비스의 URI 보안 관리하는 IoT 서비스 시스템에 대해 설명하고, 3장에서는 CapSG 구현을 위한 테스트베드 구축 내용과 C&C 서비스 토큰 구현 및 리소스 서비스 구현에 대해 기술하였다. 4장에서는 주체의 인증을 위해 사용되는 공인증서와 C&C서비스 토큰의 비교분석 및 CVSS를 이용한 보안 취약성 평가를 실시한다. 마지막으로 5장에서는 결론과 미래 연구방향에 대해 제시한다.

II. 관련연구

2.1 CapSG

Fig. 1에 제시된 CapSG는 사물인터넷 환경에서 디바이스 장치로부터 수집된 정보를 분석하여 리소스와 리소스 서비스를 정의하고, 주체의 인증을 위한 인증서와 서비스 인가를 위한 Capability 토큰을 통합한 C&C 서비스 토큰을 이용한 사물인터넷 시스템 구성도이다.[10].

Fig. 2는 CapSG 구성도로 주체의 요청에 대해 서비스를 분류하는 요청핸들러, 주체의 인가와 서비스 접근제어, 리소스를 관리하는 서비스핸들러, 리소스와 C&C 토큰 정보관리를 위한 리소스핸들러로 구성된다[11].

요청핸들러는 사용자의 인증서 발급과 인증처리, 리소스 서비스 토큰을 통한 서비스 요청에 따른 서비

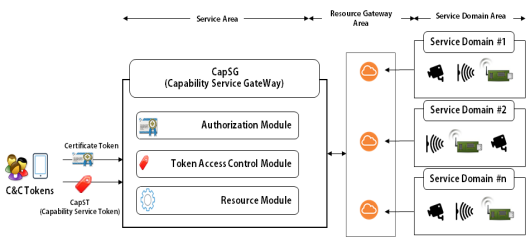

Fig. 1. Architecture of Service Access Control System

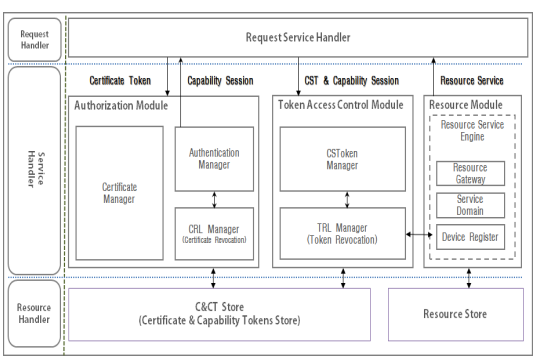

Fig. 2. Capability Service Gateway Diagram

스 분류 처리 역할을 수행한다. 서비스핸들러는 주체의 인증서관리, 인증처리, 폐기된 인증서 목록을 관리하는 인가모듈과 리소스모듈에서 정의된 리소스 서비스에 대한 접근제어를 위한 토큰접근제어모듈, 리소스 서비스 엔진을 관리하는 리소스 모듈로 기능을 나누어 설계하였다.

2.2 사물인터넷 LCRS 리소스 모델

Fig 3 은 본 논문에서 구현한 테스트베드 환경을 LCRS(Left-Child Right-Sibling) 리소스 서비스 모델로 표현한 것으로 LCRS 리소스 서비스 모델은 서비스 분류 과정을 통해 새로운 융합 서비스를 생성할 수 있다.

제어서비스를 습도환경 정보 서비스 하단 영역으로 리소스 서비스를 복사하면 습도환경 정보를 취득할 수 있는 서비스에서 장치제어에 대한 서비스 권한을 부여 받아 처리 할 수 있으며, 도메인 영역의 리소스를 재배치를 하고자 할 경우 해당 리소스 서비스를 변경하고자 하는 서비스도메인으로 이동 시키면 리소스 서비스에 대한 재분류가 가능하다.

디렉토리 구조 형태의 서비스 모델 관리 형태는 최하단에 서비스를 위치시켰으나, LCRS 서비스 관리 모델은 각 서비스 모델 노드에 리소스를 연결하여 해당 리소스 서비스에 각각의 독립된 서비스가 이루어지도록 하였다[12].

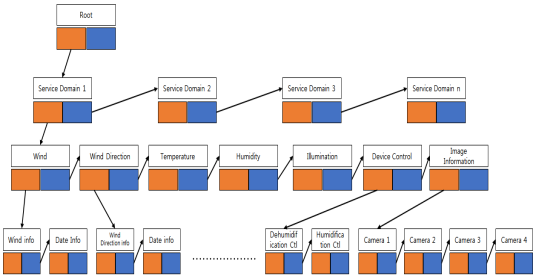

Fig. 3. LCRS Resource Model

2.3 리소스 매핑 테이블을 이용한 리소스 URI 관리

사물인터넷 환경에서 각 노드 장치와의 서비스 통신을 위해 REST 개념을 적용하여 서비스를 제공하고 있다.

REST는 통신 규약이나 표준 또는 스펙이 아니라 분산 하이퍼미디어 시스템을 위한 HTTP 같은 형식으로 네트워크에서 클라이언트와 서버 사이의 통신 방식으로 서비스 제공 형식은 "/groups/groupid/groupid/member/sensor" 와 같이 계층적 구조로 구성된다[15]. REST의 장점은 통신을 위한 별도의 서비스를 설치하지 않아도 되고 특정 언어에 귀속되지 않게 서비스를 구성 할 수 있다. 하지만 설계 및 구성에 표준이 없어 각 서비스별로 아키텍처가 달라질 수 있고, 이것에 따를 서비스 구현 방안이 달라져 시스템의 복잡도가 높아질 수 있다.

REST을 기반으로 한 유일한 URI을 가지는 서비스는 사물인터넷과 같은 다양한 서비스가 존재하는 환경에서 효율적 구성이 아니다. 또한 계층적으로 구성된 URI는 직관적으로 어떤 기능을 제공하는지 예측이 가능하다. 이러한 서비스의 URI 정보는 비 인가된 주체로부터 공격 대상이 될 수 있는 위험요소가 된다[14].

본 논문에서는 비 인가된 사용자가 리소스 서비스의 정보를 획득하더라고 URI 정보를 유추할 수 없도록 하였다. 주체의 리소스 서비스 URI는 암호화를 통해 CapSG 의 리소스 모듈 단계에서 URI 암호 매핑 테이블을 적용함으로써 리소스 서비스에 대한 보안성을 강화 하였다.

Fig 5는 리소스관리자가 등록한 리소스 서비스에 대해 서비스 주체가 리소스 URI 매핑 테이블 정보를 이용하여 리소스 서비스에 접근하는 과정이다.

i. 리소스 서비스 관리자는 노드 디바이스 제어 서비스 또는 수집된 데이터를 활용하여 정보를 제공하는 리소스 서비스를 만든다. 리소스 서비스에 ID를 발급하여 서비스 목록에 등록한다.

ii. 인가된 주체는 리소스 관리자 등록한 리소스 서비스 목록에서 이용하고자 하는 서비스에 대해 접속

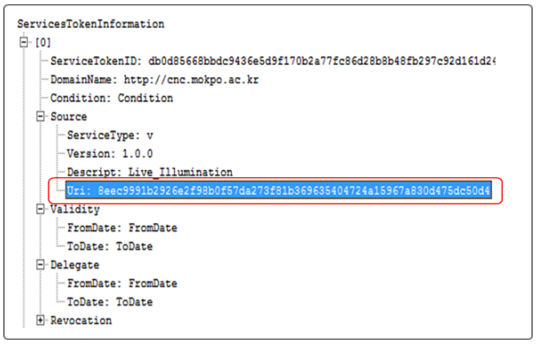

Fig. 4. Capability Token URI Information

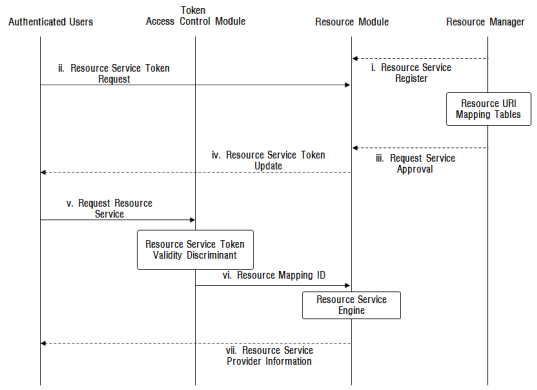

Fig. 5. Service Request Process Using Resource mapping Table

할 수 있는 리소스 서비스 토큰을 요청한다.

iii. 리소스 관리자는 주체가 요구한 리소스 서비스에 대해 승인한다. 승인 과정에서 요청 주체의 암호화 알고리즘 정보를 이용하여 리소스 서비스 ID 값을 인증 개인키로 암호화 하여 리소스 서비스 매핑테이블에 정보를 저장한다.

iv. 토큰접근제어 모듈은 리소스 관리자가 승인 한 리소스 서비스 토큰 정보를 갱신하여 인가된 주체에게 전달한다.

v. 리소스 관리자가 접근을 허용한 리소스 서비스 토큰을 가지고 서비스 주체는 토큰접근제어모듈에 인증서정보와 암호화된 리소스 서비스 정보를 전송한다.

vi. 토큰접근제어 모듈은 주체의 요청 리소스 서비스 토큰의 리소스 영역 정보를 확인하여 요청서비스 분석, 공개키의 위변조 확인과 유효기간, 서비스 토큰 폐기목록을 참조하여 유효성 판별 후 주체 서비스 토큰 정보를 갱신하다. 마지막으로 주체의 개인키를 이용하여 암호화된 리소스 서비스 정보를 복호화 한 후 URI 매핑 테이블 통해 최종 리소스 서비스 URI를 리소스 모듈로 전달한다.

vii. 리소스 서비스 엔진은 해당 서비스 URI 정보를 통해 서비스를 주체에게 제공한다.

2.4 CVSS 평가

미국 국가인프라검증위원회(National Infrastructure Assurance Council)의 지원하에 개발된 CVSS는 이 기종의 하드웨어와 소프트웨어 플랫폼에 걸쳐 있는 취약점들을 평가하고 확인할 수 있는 글로벌 취약점 오픈 프레임워크이다. 시간과 사용자 환경에 의해 변하지 않는 취약점에 본질적이고 근본적인 특징을 나타내는 기본 메트릭스(Base Metrics), 사용자들의 환경에 의한 것이 아닌 시간의 흐름에 따라 변경되는 취약점의 특징을 나타내는 시간 메트릭스(Temporal Metrics)와 특정한 환경과 관련 있는 취약점 특징을 나타내는 환경 메트릭스(Environmental Metrics) 그룹을 이용하여 CVSS 점수를 산출하는 과정을 나타낸 것으로 취약점을 평가한다[7].

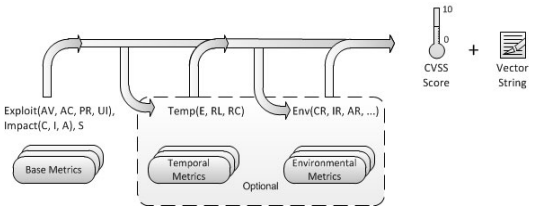

Fig. 6. CVSS Metrics and Equations

각각의 메트릭스 계산식은 0부터 10 까지 범위에서 메트릭스에 대한 평가 등급에 따른 점수가 있고 계산 과정은 1차적으로 기본 메트릭스에서 선택된 값을 기본 메트릭스의 계산식에 대입하여 계산을 완료하고 2차에는 시간 메트릭스에서 선택된 값은 기본 메트릭스의 값과 함께 시간 메트릭스 계산식에 대입하여 계산하다. 마지막으로 3차에는 환경 메트릭스에서 선택된 값은 시간 메트릭스 값과 함께 환경 계산공식에 대입하여 최종 값을 산출한다[7]. 최종 산출된 평가 값을 Table 1.의 CVSS 보안 위험 등급표에 적용하면 보안 취약점에 대한 등급을 확인 할 수 있다.

Table 1. Qualitative severity rating scale

Rating	Low	Medium	Heigh	Critical
CVSS Score	0.1~3.9	4.0~6.9	7.0~8.9	9.0~10.0

III. 본 론

본 논문에서 Fig 7과 같이 온도, 습도, 조도, 풍향, 풍속 센서 디바이스와 IP 카메라 및 디바이스 제어 컨트롤을 설치한 CapSG 기반의 사물인터넷 서비스를 구축하였다.

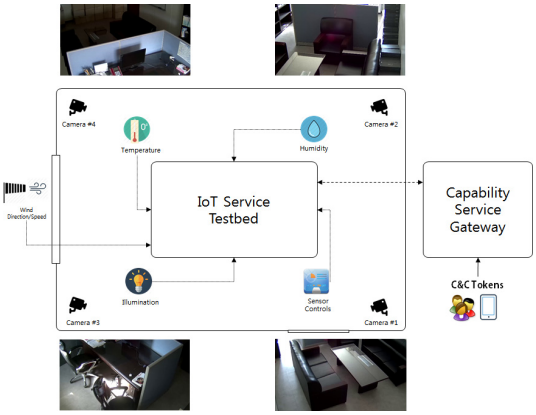

Fig. 7. IoT Testbed

3.1 구현환경

테스트베드에서는 센싱 데이터 수집을 위해 다채널 데이터로거 장치(midi LOGGER GC220)에 온도, 습도, 조도, 풍향, 풍속의 디바이스를 연결하여 시간에 따라 전기적 수치정보를 측정하고 기록하였다.

Fig 8은 본 논문의 시스템 환경에서 사용하는 데이터로깅 화면으로 10개 채널을 통해 디바이스 정보를 수집할 수 있지만 테스트 환경에서는 온도, 습도, 조도, 풍향, 풍속 정보 수집할 수 있도록 하였고, 가습기와 제습기 제어를 위해 제어 컨트롤 장치를 제작하여 온·오프 할 수 있도록 하였다.

데이터로깅 과정에서 추출한 전기적 신호는 리소스 서비스 제공을 위해 디지털 값으로 변경하였고 변환된 데이터를 저장할 수 있는 데이터베이스를 설계하고 구축했다.

영상정보는 실시간 영상과 녹화 된 영상 재생을 위해 별도의 영상기록시스템으로 나누어 구축했다. 영상정보와 센싱 디바이스는 실시간으로 데이터로거를 통해 CVS 형식으로 로컬 시스템에 저장하도록

Fig. 8. Sensor Data Logging

하였고 파일 정보가 갱신되는 시점에 데이터베이스에 저장한다.

센싱 데이터 수집 방법으로는 데이터 로거를 이용하여 유선으로 연결된 USB를 통해 로컬 시스템에 저장된다. 저장된 파일의 형식은 CVS 형식으로 데이터 로거에 의해 실행 시 중복 방지를 위해 새 파일명으로 저장된다. 데이터로깅으로 생성된 CVS 파일을 NodeJs Supervisor Modules을 이용하여 실시간으로 데이터베이스에 센서 데이터를 전송한다. 센싱 데이터를 저장하는 데이터베이스관리시스템은 DAO(Data Access Object) 연결을 이용하였고 뷰, 테이블, 스케줄러, 트리거 사용이 용이한 오라클 데이터베이스 11g 버전을 사용하여 데이터를 저장하였다. Capability 서비스를 제공하는 웹서버는 시스템 가상화를 통해 솔라리스 x86 운영체제를 설치하고 Apache 와 Tomcat WAS로 구성한 웹 서버를 구축했다. C&C 리소스 토큰을 이용한 서비스 접근제어 시스템 구축은 JDK 1.8 기반의 이클립스 개발 툴을 사용하였으며, 효율적 데이터베이스 연결관리를 위해 iBATIS 이용하여 서비스를 개발했다.

서비스 접속 사용자에게 RIA 환경 제공을 위해 JQuery를 이용한 센싱 정보 서비스를 개발하고 등록했다. C&C 서비스 토큰을 이용하여 리소스 서비스에 접근하기 위한 클라이언트 접속 프로그램은 C#를 이용하였다. 구현을 위한 개발 환경은 Table 2 와 같다.

Table 2. System development tools

Component	Develoment Tool
Data Logging	CVS, Nodejs
Database	Oracle 11g
Web Server	Solaris X64, Apache 2.x + Tomcat 1.8.x
Service Management	JDK 1.8 , Spring Framework, iBATIS, JQuery
Client	Visual Studio 2010, C#, Android

3.2 C&C 서비스 토큰 발행

시스템 접속과 리소스 서비스 요청을 위해 주체는 C&C 서비스 토큰을 발급 받아야 한다.

Fig 9 는 C&C 서비스 토큰을 발급하는 화면으로 본 논문에서 구현한 사물인터넷 서비스를 이용하고자 하는 주체가 계정과 개인키 암호화를 위한 비밀

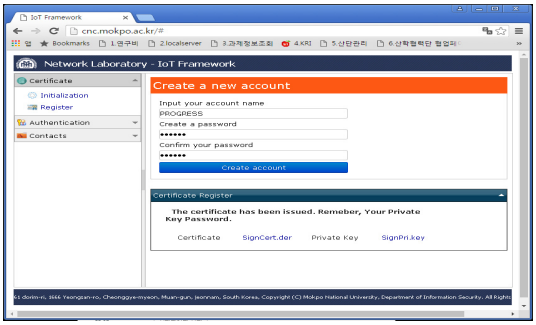

Fig. 9. C&C Services Issued Token

번호 입력 후 생성버튼을 클릭하면 시스템에 등록된 공개키를 이용하여 인증서와 개인키가 생성되고 주체에 대한 인증서를 로컬 또는 이동디스크에 저장 할 수 있다.

Fig 10은 C&C 서비스 토큰 발급 요청에 의해 만들어진 "SignCert.der"는 공개키 기반구조로 유효기간은 인증서가 발급된 시점에서 2년이 경과된 일자로 설정하였다. 인증서 "SignCert.der" 파일은 발급대상이 "PROGRESS"로 발급 시 신청한 계정으로 발급자와 공개키 정보를 포함한다.

생성된 인증서의 내용을 살펴보기 위해 인증서와 개인키로 분리하여 출력되도록 테스트 한 것으로 주체의 C&C 서비스 토큰은 직렬화를 통해 다시 재구조화 한다.

인증서와 함께 발급된 "SignPri.key" 개인키는 주체가 설정한 비밀번호로 암호화 되어 Fig 9 와 같이 저장된다. 개인키에 대한 암호화 및 복호화 과정은 모두 서버 사이드에서 관리한다. C&C 서비스 토큰은 인증영역과 개인키 영역의 통합한 인증서영역과 리소스 서비스 토큰의 정보를 저장하는 영역으로 구분된다.

리소스 서비스 토큰 생성 시 직렬화 과정을 통해

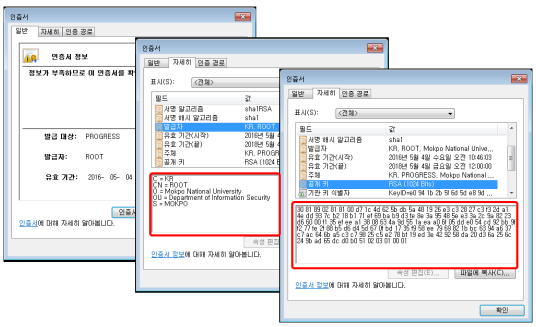

Fig. 10. C&C Service Token Certificate Information

```
import java.io.Serializable;
import java.security.cert.X509Certificate;
public class IotCnCToken implements Serializable {
        public IotCnCToken(X509Certificate _cert,byte[] _userpk, RSToken _RStoken)
        {
                super();
                this.cert = _cert;
                this.userpk = _userpk;
        }

        X509Certificate cert;
        byte[] userpk;
        RSToken rstoken;

        public X509Certificate getCert() {
                return cert;
        }
        public void setCert(X509Certificate cert) {
                this.cert = cert;
        }
        public byte[] getUserpk() {
                return userpk;
        }
        public void setData(byte[] userpk) {
                this.userpk = userpk;
        }
        public RSToken getRstoken() {
                return rstoken;
        }
        public void setRstoken(RSToken rstoken) {
                this.rstoken = rstoken;
        }
}
```

Fig. 11. C&C Resource Service Object

인증서 파일을 생성한다. 그리고 생성된 인증서에 대해 역직렬화 과정을 거쳐 정보를 추출하고자 할 경우 C&C 리소스 서비스 객체가 필요하다. Fig 11 은 C&C 서비스의 직렬화와 역직렬화를 위해 필요한 객체 정보를 기술한 것이다.

C&C 리소스 서비스 객체는 주체가 파악 할 수 없도록 서버 측에서만 사용된다. 주체의 인증과정에서 인증서 객체를 스트림으로 서버에 전송하고 서버는 인증정보를 로컬에 저장하지 않고 메모리 힙 영역에서 정보를 처리하고 인증연결세션을 생성한 후 메모리 힙 영역에 상주한 인증서 정보를 삭제한다. 이러한 처리 과정을 수행함으로써 객체의 전송과정에서 외부의 공격에 대해 패킷 정보가 누출되더라도 인증서 생성 시 암호화된 정보를 복호화 할 수 없고, 인증서 역직렬화를 위한 객체 정보를 파악하기 어렵도록 하는 보안성을 제공하였다. 차후 객체에 대한 역직렬화 시 serialVersionUID 필드를 선언하고 특정 해시값을 입력하여 직렬화 과정 시 특정 필드를 암호화할 수 있도록 하는 기능을 추가하고, 직렬화 되어진 객체에 대해서 javax.crypto.SealedObject 클래스나 java.security.SignedObject 클래스를 사용하여 SealedObject 클래스를 이용한 것만으로 데이터에 대한 보안 검증을 수행하도록 할 것이다.

3.3 리소스 서비스 구현

C&C 서비스 토큰 정보를 이용하여 접속하고자 하는 리소스 서비스를 구현하였으며, 사용자에게 RIA 환경을 제공하기 위해 JQuery를 사용하였다.

Fig 12 는 본 논문에서 구현한 리소스 서비스를 메뉴로 구성한 것으로 센서 디바이스의 정보를 확인할 수 있는 서비스와 제어 컨트롤을 이용한 디바이스

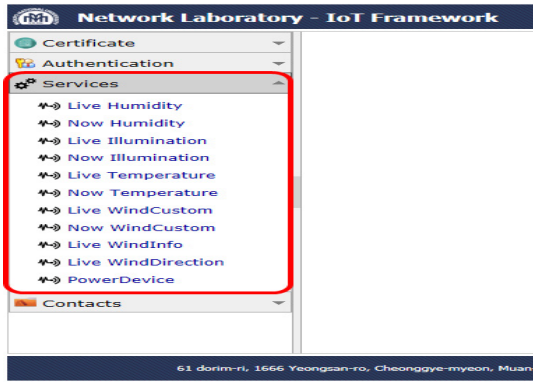

Fig. 12. Resource Services List

제어 서비스를 나타내고 있다. 리소스 서비스는 CapSG의 리소스 모듈에서 서비스 토큰의 URI 정보를 참조하여 서비스를 제공하므로 주체의 플랫폼에 영향을 받지 않고 서비스 할 수 있다.

Fig 13 의 리소스 서비스 구현을 위해 JQuery와 데이터베이스 연결 관리는 스프링 프레임워크 기반 Ibatis 를 이용하였다.

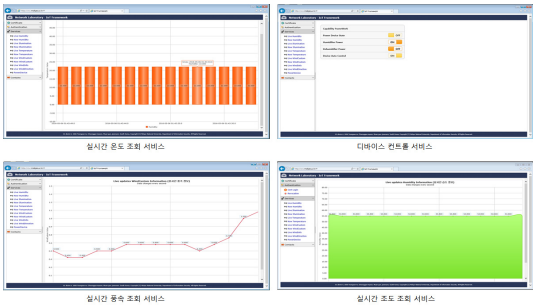

Fig. 13. RIA Based Resource Service

IV. 평 가

4.1 사물인터넷 서비스 접근제어 시스템 평가

본 논문의 CapSG 시스템에 대한 보안성 평가를 위해 시스템 및 서비스 접근에 대한 인증 매체 비교 분석과 사물인터넷 서비스에 대한 주체의 접근제어 관리 방안, 마지막으로 본 논문에서 제시한 사물인터넷 서비스 환경을 대상으로 CVSS 취약점 등급 평가를 실시했다.

4.1.1 공인인증서와 C&C 서비스 토큰 비교 분석

시스템에 대한 사용자 접근제어를 위해 각 시스템에서는 사용자의 아이디·비밀번호 또는 금융기관에서 사용하는 X.509 형식으로 구조화된 공인인증서와 비밀키 파일을 이용하여 별도의 플러그인 프로그램 설치를 통해 인증 절차를 처리한다.

본 논문에서는 인증서를 이용하여 주체의 인증 절차를 처리함에 있어 공인인증서에서 발생 가능한 보안 위험 요소를 살펴보았고, 각 보안 위험 요소를 보완하여 C&C 서비스 토큰 보안성을 높였다. 공인인증서를 사용하여 주체의 인가 여부를 처리하는 사이트는 인증을 위한 별도의 프로그램을 설치하여야 하는 불편함을 줄 뿐만 아니라 악성 코드에 의해 외부 공격자에게 비밀키 정보가 노출 될 위험성이 있다. 일반적인 경우 윈도우 환경에서 인증서와 비밀키는 “c:\Program Files\NPKI” 또는 “c:\NPKI” 와 같은 특정 장소에 위치하고 있기 때문에 디렉토리 복사와 같은 간단한 방법으로 외부 사용자에 의해 유출될 가능성이 있다.

인증서 노출의 위험은 인증을 위한 플러그인 프로그램이 특정 위치의 디렉토리를 참조하고, 인증서가 위치한 특정 디렉토리명이 사용자 계정과 고유키로 구성되어 있는 보안 취약점을 이용한 것이다. 공격자 또는 악성코드는 인증서가 위치한 특정 디렉토리의 개인키를 네트워크를 통해 공격자에게 자동 전송하게 된다. 공격자는 인증서정보, 개인키 정보를 이용하여 별도의 해독 프로그램을 작성하여 사용자의 비밀번호를 획득할 수 있다.

본 논문에서 사용되는 C&C 서비스 토큰에 대한 인증서 정보와 개인키의 보안 안전성 확보를 위해 주체가 별도의 플러그 인 프로그램을 설치하지 않고 특정 위치에 인증서 정보가 위치해 있지 않아도 인증과정에 문제가 없도록 하였다. 주체의 인증서 정보와 비밀번호로 암호화된 개인키는 C&C 서비스 토큰 객체를 이용하여 객체 직렬화를 하였고 역직렬화를 위해서는 C&C 서비스 토큰의 객체 정보가 필요하다.

Table 3.은 기존의 공인인증서 방식과 본 논문에서 제시한 C&C 서비스 토큰의 보안 취약점을 비교한 분석한 것이다. C&C 서비스 토큰의 객체 정보는 서버 사이드 언어에서만 정의되고 사용되기 때문에 공격자에게 노출되지 않는다. 또한 서비스 토큰 객체는 고정적 길이로 계산된 직렬화가 아닌 유동적 직렬화를 이용하였기 때문에 공격자가 파일의 구조를

Table 3. Difference between C&C Token and Certificate Token

	Certificate Token	C&C Token
Location	Fixed a specific location	User Settings
Serialization/ De-Serialization	None	Support
Source Analysis	Possible	Not Possible
Plug-in Installation	Require	Not Require

파악하기 어렵다.

X.509기반의 공인인증서를 재구조화 시키고 기존의 공인인증서와 차별화된 방안으로 매체를 관리함으로써 인증 매체에 대한 보안성을 향상시켰으나, 주체의 리소스 서비스 접근 권한이 과다하게 부여될 경우 매체의 정보 시스템에 자원을 과하게 사용할 수 있는 단점이 있다.

4.1.2 CVSS 보안 위협 평가

사물인터넷 시스템은 다양한 장치들로 구성된 환경으로 인해 디바이스 보안, 암호·보안 프로토콜, 데이터베이스 보안, 프라이버시 관리, 접근제어/권한관리, ID관리 및 서비스 보안 등 여러 요소에 취약점이 노출된다.

정보시스템의 보안 취약점 평가는 시스템 구성과 해당 시스템에서 제공하는 서비스에 대한 보안 취약점 평가로 분류할 수 있으며, 서비스에 대한 보안 취약점은 어떠한 서비스를 대상으로 평가하느냐에 따라 보안 취약점 평가가 서로 상이하다.

본 논문에서는 CVSS 평가를 위해 모든 리소스 서비스에 대해 각각 평가 하려고 하였으나, 주체의 인증을 위한 C&C 서비스 토큰과 리소스 URI를 관리하는 CapSG에 대한 CVSS 평가는 동일한 인터페이스에서 수행되기 때문에 대표적인 디바이스 제어 서비스를 대상으로 평가를 실시하였다.

4.1.2.1 기본 메트릭스

4.1.2.1.1 Attack Vector

공격 수행 위치에 대한 평가 등급은 “Network”로 평가 하였다. 관제를 통해 특정 주체에게 한정된 서비스를 제공하는 방안도 있지만 사물인터넷 특성인 모든 사물이 인터넷에 연결되어 있는 환경에서의 서비스는 네트워크에 대한 공격 가능성을 완전히 배제할 수는 없기 때문이다.

4.1.2.1.2 Attack Complexity

사물인터넷 서비스에 접근하고자 하는 경우 C&C 인증서를 발급받고 인증 과정을 거친 주체만이 서비스에 접근할 수 있다. 사물 디바이스는 직접 데이터베이스에 접속하여 정보를 저장하는 것이 아니라 리소스 게이트웨이의 인터페이스를 통해 데이터베이스에 저장되므로 직접적으로 접속을 시도할 수 없기에 “High” 이다.

4.1.2.1.3 Privileges Required

CapSG에 접속을 위해서는 C&C 인증서를 통한 인증 후 연결세션을 통해 주체를 재 인증하여 리소스 서비스에 대한 접근이 가능하므로 공격자가 두 번 이상 인증 과정을 통해야 하므로 “Low” 이다.

4.1.2.1.4 Interact User Interaction

리소스 서비스에 대한 권한 요청은 서비스 요청자에 의해 요구 되고, 리소스 관리자에 의해 정의된다. 제안 시스템은 서비스 요청자와 리소스 관리자의 상호작용에 의해 생성 및 관리되므로 “Required” 이다.

4.1.2.1.5 Scope

주체가 요청하는 리소스 서비스 정보는 주체마다 별도의 리소스 매핑 테이블로 관리되어 지고, 이는 다른 리소스 서비스에 영향을 리소스 서비스에 영향을 미치지 않기 때문에 “Unchanged” 이다.

4.1.2.1.6 Confidentiality Impact

기밀성 영향에 대한 평가는 “None”으로 CapSG는 센싱 데이터를 수집하여 저장하는 데이터베이스와 인터페이스 역할을 수행한다. 센싱된 데이터는 유·무선망을 통해 인가된 디바이스에서 발생되는 데이터만 수집하므로 시스템의 기밀성에 영향을 미치지 않는다.

4.1.2.1.7 Integrity Impact

주체의 인증서 및 리소스 서비스 토큰에 대한 무결성과 안전성 확보를 위해 CapSG는 인증서와 리소스 서비스 토큰에 대한 폐기목록리스트를 관리한다. 주체의 인증서 및 리소스 서비스 폐기 시 폐기 된 정보를 폐기목록에 등록하여 무결성을 확보하였기 때문에 영향을 주지 않는 “None” 이다.

4.1.2.1.8 Availability Impact

가용성 영향에 대한 평가 등급은 “Low” 로 CapSG를 이용한 인증 및 리소스 서비스 제공은 주체의 로컬에서 데이터를 재구성하여 서비스를 제공하는 방식이 아닌 모든 리소스 서비스는 서버 측에서 이루어 질 수 있도록 구성하였다.

주체가 리소스 서비스 인증 및 리소스 서비스 요청 시 주체의 C&C 토큰 정보를 서버 측에 전송한다. 서버는 전송 된 토큰 정보를 가지고 분석하여 URI 정보를 추출한다. 이러한 과정 중에 시스템에 대한 성능은 영향을 받는다.

4.1.2.2 시간 메트릭스

4.1.2.2.1 Exploit Code Maturity

본 논문에서 인증서는 X.509 형식으로 인증서와 서비스 토큰 정보가 직렬화 된 C&C 서비스 토큰을 가지고 정보를 처리한다. 공격자가 C&C 서비스 토큰을 획득할 경우 전문적 지식을 가진 공격자는 토큰에 대한 구조 정보를 수정하여 공격 시연이 가능할 수 있어 “Proof-of-Concept” 이다. 공격자의 공격에 대해 CapSG는 인증서에 대한 형식 유효성 검토 및 인증서 폐기 목록을 통해 공격에 대한 응답 처리를 하지 않고 변조된 인증서의 시그니처 정보를 관리하여 서비스에 대한 접속을 차단한다.

4.1.2.2.2 Remediation Level

C&C 서비스 토큰의 구조가 변경될 경우 주체는 공식 패치를 하지 않고 접속할 경우 기존의 인증서를 폐기하고 신규 C&C 서비스 토큰을 발급 받아야 한다. 시스템 및 서비스에 대한 패치는 서버 측에서 이루어지므로 대응 수준에 대한 평가는 본 논문의 사물인터넷 서비스 시스템에 영향을 주지 않는다.

4.1.2.2.3 Report Confidence

C&C 서비스 토큰과 리소스 서비스 관리 모델에 대한 인터페이스 역할을 하는 CapSG는 외부로 정보 누출을 하지 않기 때문에 해당 평가에 영향을 미치지 않는다.

4.1.2.3 환경 메트릭스

4.1.2.3.1 Confidentiality Requirement

사물인터넷 서비스는 다양한 서비스의 종류에 따라 직접적 피해 대상과 크기가 서로 상이하므로 완전한 수익의 잠정적 손실이 없다고 할 수 없다.

CapSG를 기반으로 한 리소스 서비스 중 습도에 따라 자동으로 디바이스를 제어하는 서비스를 기준으로 평가할 경우 약간의 물리적인 손실이나 자산에 대한 손실이 발생할 수 있으므로 “Low” 이다.

4.1.2.3.2 Integrity Requirement / Availability Requirement

C&C 서비스 토큰이 공격자에 의해 조작될 경우, 이는 전체 주체가 아닌 인증서를 소유한 주체에게만 제한적으로 서비스 이용에 제한이 따른다. 그리고 C&C 서비스 토큰 정보가 누출되었을 경우에는 노출된 C&C 서비스 토큰은 주체의 요청에 의해 폐기 목록에 등록되어 사용할 수 있고 제안 시스템에 영향을 주지 않기 때문에 “Not Defined” 이다.

Table 4.는 CVSS 보안 취약점 등급표를 이용하여 본 논문에서 제시한 CapSG 시스템에 대해 발생 할 수 있는 중간자 공격, 악성코드를 이용한 공격, DDoS 공격을 자가 진단한 결과이다.

Table 4. CVSS 3.0 Rating System Proposed

Group	Metric Name	Values
Base	Attack Vector	Network
	Attack Complexity	High
	Privileges Required	Low
	User Interaction	Required
	Scope	Unchanged
	Confidentiality	None
	Integrity	None
	Availability	Low
Temporal	Exploit Code Maturity	Proof-of-Concept
	Remediation Level	Not Defined
	Report Confidence	Not Defined
Environmental	Confidentiality Req	Low
	Integrity Req	Not Defined
	Availability Req	Not Defined
	Modified Attack Vector	Not Defined
	Modified Attack Complexity	Not Defined
	Modified Privileges Required	Not Defined
	Modified User Interaction	Not Defined
	Modified Scope	Not Defined
	Modified Confidentiality	Not Defined
	Modified Integrity	Not Defined
	Modified Availability	Not Defined

CapSG 기반의 사물인터넷 서비스 시스템에 대한 자가 진달 결과 CVSS의 기본 메트릭스 2.6점을 기반으로 시간, 환경 메트릭스 평가 항목과 영향 항목별 점수를 반영한 결과 2.5점을 기록했다.
Fig 14 는 본 논문에서 제시한 사물인터넷 서비스에 대한 CVSS 온라인 시뮬레이션[10]을 수행한 것으로 보안 취약점 위협 평가 등급은 "낮음" 이다.

CVSS 보안 취약점 평가를 통해 CapSG를 이용한 사물인터넷 서비스 접근제어에 대한 평가가 사물인터넷 서비스 시스템에 대한 완전한 보안 취약점 평가가 될 수는 없지만 이를 통해 신규 서비스 개발 시 보안성을 확보하는 방안이 될 수 있을 것이다.

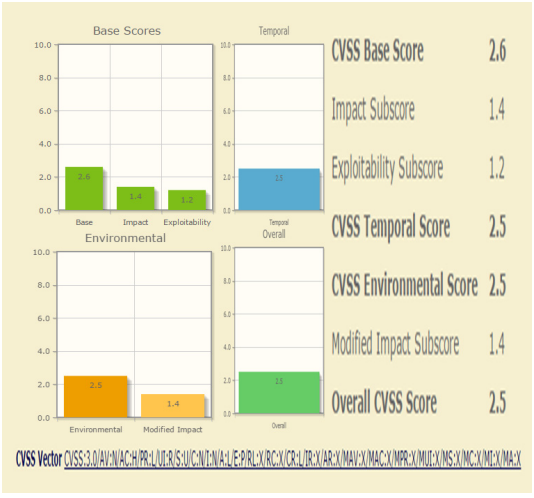

Fig. 14. CVSS 3.0 Online Calculator

V. 결 론

사물인터넷의 편리성을 제공하기 위한 서비스가 개별적이고 독자적인 방식으로 개발 될 경우 인터넷의 장점인 다양한 서비스로의 확장이 어렵고, 다른 기기 및 서비스와 연동됨에 따라 보안 취약점이 발생하고 있다. 서비스에 대한 편리성과 효율성만을 강조한 나머지 서비스 공격에 대한 보안 안전성 확보가 어렵다.

본 논문은 무분별하게 관리되는 사물인터넷 서비스를 효율적으로 관리하고, 사물인터넷 서비스에 대한 접근제어를 위해 리소스 서비스 토큰을 설계 및 구현하였다. 또한, 주체의 사물인터넷 시스템 및 서비스에 대한 접근제어를 위해서 C&C 서비스 토큰을 설계 하고 구현하였다. 구현된 C&C 서비스 토큰을 이용하여 CapSG 기반에서 주체들 간의 리소스 서비스에 대한 접근제어와 서비스에 대한 URI 보안 방안을 제시하여 사물인터넷 서비스의 보안성을 높이고자 하였다.

CapSG는 주체의 인증과 리소스 서비스 접근 권한을 포함하는 토큰을 이용하여 사물인터넷 서비스를 제공하고 서비스 접근제어를 위해 주체들 간의 서비스 토큰 위임, 폐기, 위임 거부 등의 기능을 관리한다. 그리고 각 센싱 데이터 수집을 위한 도메인 그룹에 대해 토큰 관리그룹을 사용함으로써 도메인별 서비스 접근제어가 가능하고, 토큰 그룹내의 특정 서비스 토큰을 이용한 접근제어 수행도 가능하도록 다양한 서비스 요구에 대한 접근제어의 유연성과 효율성을 제공할 수 있게 구현하였다.

LCRS 리소스 모델 관리는 도메인별 서비스에 대한 접근제어를 수행하기 때문에 사물인터넷 장치들에 종속되지 않아 서비스에 대한 관리 및 확장성이 용이하도록 설계하였고, CapSG에서 사용되는 C&C 서비스 토큰은 인증정보 및 접근제어정보를 포함하고 있으므로 서비스 요청 시 매번 장치 및 사용자에 대한 인증 절차 없이 한 번의 인증으로 연결세션을 유지하여, 해당 서비스에 대한 서비스 토큰만으로 접근제어를 수행할 수 있다.

C&C 서비스 토큰은 공개키 기반 구조의 인증서 토큰을 사용하고 있으며, 토큰에 대한 신뢰성을 확보하기 위해 CapSG 내에 자체 인증서폐기목록리스트와 토큰폐기목록리스트 정보를 관리함으로써 폐기인증서에 대한 실시간 모니터링을 할 수 있도록 했다.

CapSG 시스템에 대한 보안 안전성 평가를 위해 미국의 국가인프라검증위원회의 글로벌 취약점 오픈 프레임워크인 CVSS 취약점 등급 평가를 활용하여 C&C 서비스 토큰을 이용한 사용자 및 리소스 서비스 접근제어와 테스트베드에서 구현한 디바이스 제어 서비스에 대한 보안 취약점 등급을 평가를 하였다.

CVSS 보안 취약점 평가는 기본, 시간, 환경 메트릭스 그룹을 활용하여 총 0.0~10.0점으로 구성된다. 본 논문의 사물인터넷 서비스에 대한 자가진단 결과 평가 점수는 2.5점으로 0.0~3.9 구간의 "낮음"으로 보안 취약 등급 점수를 기록했다.

본 논문에서 C&C 서비스 토큰을 이용한 사용자 인증과 리소스 서비스 메핑 테이블을 이용한 CapSG 기반의 접근제어 시스템이 사물인터넷 환경에서 서비스 제공에 대한 보안 안전성이 향상된 것을 확인 할 수 있었다.

본 논문은 단일 도메인 환경에서 센싱 데이터를 이용하여 사물인터넷 서비스를 구축한 것으로 향후 멀티 도메인 환경에서 다양한 서비스 관리 방안과 주체의 인증서 안전성 확보를 위해 제3의 인증기관에서 발급한 인증서 기반의 C&C 서비스 토큰 관리 방안, 암호화된 REST 구조에서 계층간의 이동 시 암복호화 과정에서 발생하는 성능하락에 대한 연구가 필요하다.

References

[1] Ho-won Kim, "Issues of Security/privacy in IoT Enviroment", *TTA Journal* 153, pp, 35-39, 2014

[2] Yun-hee Lee, "Internet of Things for creating economies based on promising market prospects and challenges," *National Information Society Agency*, 2013

[3] JoseL. Hernandez-Ramos,M. VictoriaMoreno, Jorge BernalBernabe, DanGarciaCarrillo and Antonio F.Skarmeta. "SAFIR: Secure access framework for IoT-enabled services on smart buildings," *Journal of Computerand System Sciences*, 81, pp. 1452-1463, 2015

[4] Jayavardhana Gubbi, Rajkumar Buyya, Slaven Marusic and Marimuthu Palaniswami. "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future Generation Computer Systems*, vol. 29, pp.1645-1660, 2013

[5] Jos´e L. Hern´andez-Ramos,Antonio J. Jara,Leandro Mar´ın and Antonio F. Skarmeta. "Distributed Capability-based Access Control for the Internet of Things," *Journal of Internet Services and Information Security*, vol. 3, No 3/4, pp. 1-16, 2013

[6] S. Gusmeroli,S. Piccione and D. Rotondi. "A capability-based security approach to manage access control in the Internet of Things," *Mathematical and Computer Modelling*, vol. 58, pp. 1189-1205. 2013

[7] Common Vulnerability Scoring System, http://first.org/cvss

[8] The Legion of the Bouncy Castle, https://www.bouncycastle.org

[9] National Vulnerability Database, https://nvd.nist.gov/cvss/v3-calculator

[10] Jin-Bo Kim,Deresa Jang,Mi-Sun Kim and Jae-Hyun Seo. "The Access Control platform of the IoT Service using the CapSG," *The Journal of korea Information processing society*. vol. 4, no. 9, pp. 337-346, 2015

[11] Youn-sung Nam,Jin-Bo Kim,Mi-sun Kim and Jae-hyun Seo. "A Study of Capability Token Management for Authentication and Access control in the Internet of Things," *Korea information processing society*. vol. 22, no. 2, pp. 756-758, 2015

[12] Deresa Jang,Jin-bo Kim,Mi-sun Kim and Jae-hyun Seo. "A Study of Resource Service Management Model for IoT Service Access Control," *Korea information processing society*. vol. 22, no. 2, pp. 664-667, 2015

[13] Jong-hyeon Park, Hyo-chan Bang, Se-han Kim,Mal-hui Kim,In-Hwan Lee, Byeong-cheol Choi, Gang-bok Lee, Su-seong Kang and Ho-won Kim. "The Future of the Internet of Things," *The Electronic Times*. 2014

[14] Deresa Jang,Jin-bo Kim,Mi-Sun Kim and Jae-Hyen Seo. "Privacy-preserving Access Control in the IoT Service Platform," *MITA 2016*. pp. 52-54, 2016

[15] Seok-kap Ko, Seung-chul Son, Seung-hoon Oh and Byung-tak Lee. "Internet of Things standards and implementing technical trends CoAP," *IITP*, 2014

〈저자소개〉

김 진 보 (Jin-bo Kim) 정회원
2003년: 국립목포대학교 멀티미디어학과 졸업
2007년: 국립목포대학교 정보보호기술학 협동과정 석사
2016년: 국립목포대학교 정보보호기술학협동과정 박사
〈관심분야〉 정보보호, 웹서비스 보안, 빅데이터, 프로그래밍 언어

김 미 선 (Mi-sun Kim) 정회원
1996년: 국립목포대학교 컴퓨터공학과 졸업
2000년: 국립목포대학교 컴퓨터공학과 석사
2000년: 국립목포대학교 컴퓨터공학과 박사
2012년~현재: 국립목포대학교 정보보호학과 초빙교수
〈관심분야〉 정보보호, 프로그래밍 언어, 컴퓨터 네트워크, 모바일 시스템 보안

서 재 현 (Jae-hyun Seo) 종신회원
1985년: 전남대학교 계산통계학과 졸업
1988년: 중앙대학교 전자계산학과 석사
1996년: 전남대학교 전산통계학과 박사
1996년~현재: 국립목포대학교 정보보호학과 교수
〈관심분야〉 정보보호, 시스템 및 네트워크보안, 컴퓨터 네크워크, 모바일 네트워크 보안