The Journal of The Institute of Internet, Broadcasting and Communication (IIBC)
Vol. 16, No. 6, pp.25-31, Dec. 31, 2016. pISSN 2289-0238, eISSN 2289-0246

https://doi.org/10.7236/JIIBC.2016.16.6.25
JIIBC 2016-6-4

스마트 홈 환경에서 AKI기반 검증 시스템을 활용한 인증관리 및 통신 기법에 관한 연구

A Study on Authentication Management and Communication Method using AKI Based Verification System in Smart Home Environment

진병욱*, 박중오**, 전문석***

Byung Wook Jin*, Jung Oh Park, Moon Seog Jun*****

요 약 최근 IoT 기술의 발전과 ICT 서비스의 확산으로 유·무선 초고속 통신기반의 홈 네트워크 많은 발전과 다양한 서비스가 제공되고 있다. 국내·외 업체는 IoT기반의 기술을 활용하려는 사용자를 위한 혁신기술을 연구하고 있으며, 스마트 홈 환경이 점차적으로 발전하고 있다. 사용자들은 스마트폰의 확산과 발전으로 인해 보다 편리한 생활을 살아하고 있다. 그러나 스마트환경의 통신연결로 인한 다양한 공격기법, 저 전력·경량화 통신의 미흡한 적용, 보안 가이드라인의 문제로 인하여 스마트 홈 네트워크의 보안위협이 발생하고 있다. 또한 악의적인 디바이스의 위장접근 데이터 위변조와 같은 신규·변종 공격사례가 발생하여 해결책이 요구되고 있다. 본 논문에서는 스마트 환경에서 기존 인증 시스템인 PKI의 취약성을 보완한 AKI기반의 인증 관리 기법을 활용한 안전한 통신 프로토콜을 설계한다. ECDSA기반의 서명기법을 활용하여 통신수행의 효율성을 높였으며, 스마트 홈 환경의 보안위협에 대해서 보안성 및 안전성을 분석하였다.

Abstract With the development of IOT technology and the expansion of ICT services recently, a variety of home network services have been advanced based on wired and wireless high speed telecommunication. Domestic and global companies have been studying on the innovative technology for the users using IOT based technology and the environment for the smart home services has been gradually developed. The users live their lives with more convenience due to the expansions and developments of smart phones. However, the threatening on the security of the smart home network had occurred by various attacks with the connection to the smart environment telecommunication, lack of applications on low powered and light weight telecommunication, and the problems of security guideline. In addition, the solutions are required for the new and variant attacking cases such as data forgery and alteration of the device for disguising approach with ill will. In this article, the safe communication protocol was designed using certification management technique based on AKI which supplemented the weakness of PKI, the existing certification system in the smart environment. Utilizing the signature technique based on ECDSA, the efficiency on the communication performance was improved, and the security and the safety were analyzed on the security threat under the smart home environment.

Key Words : Smart Home, AKI Infrastructure, Authentication Protocol

*정회원, 숭실대학교 일반대학원 컴퓨터학과
**정회원, 성결대학교 파이데이아학부 (교신저자)
***정회원, 숭실대학교 컴퓨터학과
접수일자 : 2016년 9월 6일, 수정완료 : 2016년 10월 6일
게재확정일자 : 2016년 12월 9일

Received: 6 September, 2016 / Revised: 6 October, 2016 / Accepted: 9 December, 2016
**Corresponding Author: jopark02@sungkyul.ac.kr
Paideia College Dept, of Paideia Sungkyul University, Korea

Ⅰ. 서 론

사물인터넷의 기술이 급격히 발전되고 정보기술 트렌드의 핵심으로 떠오르면서, ICT 융합기술인 스마트 홈 시장도 점차적으로 넓어지고 있다. 스마트 홈 환경의 IoT Device는 유·무신통신기술의 기반으로 다양한 서비스를 제공하여 사용자들로부터 편의성을 주고 있다[1-2].

스마트 홈 환경에서는 IoT기반의 기술의 특성을 계승하고 있어 Device 및 네트워크 환경에서 취약점을 이용한 공격기법이 존재하고 있다. 스마트 홈 환경에서 비 인가된 접근으로 인한 해킹사고, 악성코드에 대한 피해사례가 발생하고 있다. 기존의 데이터 위변조, 정보유출. DDoS 공격, 스마트 폰 해킹 공격에 대한 보안위협이 있다[2-3]. 그러므로 본 논문에서는 스마트 홈 환경에서 AKI 기반 시스템을 활용한 인증관리 및 통신기법을 설계한다. 기존의 PKI기반 인증시스템과 AKI기반의 인증시스템의 보안성과 서명기술에 대한 효율성을 분석하며, 스마트 홈 환경에서 발생하는 보안위협에 대해서 안전성을 분석하였다.

본 논문은 5장으로 구성되어 있으며 2장에서는 자가인증 및 스마트 홈 환경 보안위협 및 요구사항에 대해서 관련연구를 수행하였다. 3장에서는 제안된 인증 관리 및 통신 기법에 대해서 서술하였으며, 4장에서는 성능 평가를 수행하였다. 5장에서는 결론을 서술하며, IoT기반의 융합 환경 연구기술에 대해 연구 및 방향성을 제시하여 논문의 결론을 제시한다.

Ⅱ. 관련연구

1. 자가인증 및 AKI 공개키 검증 인프라

자가 인증 인프라란 공개키를 인터넷 개체의 주소로 사용하면서 제3자의 도움 없이 자기 자신의 인증할 수 있는 “self-certifying Address”체계를 말한다[2]. 기존의 주소체계의 IP는 식별자와 위치자 역할을 동시에 담당하게 되면서 스마트 홈 환경에서 적용하기에 문제성이 발생하였다. 또한 주소체계에서 보안성을 지원할 수 있는 기능이 부족하여 다양한 보안위협들이 발생하고였다. 기존의 인증체계의 보완성을 내재하기 위해서 식별자에 자가 인증을 적용하는 Accountable Internet Protocol(AIP), Accountable Key Infrastructure(AKI), Shut Off Protocol와 같은 연구를 수행하고 있다[2][4].

Accountable Internet Protocol(AIP)는 호스트 및 도메인 주소의 위변조를 막기 위해서 제 3자의 도움 없이 객체의 인증을 수행한다. 라우터에 유입된 패킷의 근원지를 검증 후 검증된 패킷만 포워딩할 수 있다. 기존의 패킷마킹이나 패스 핑커 프린터와 같은 방식에 비해 효율적이나 네트워크에 내재적으로 수행할 수 있는 매커니즘이라 할 수 있다. 하지만 사용되는 공개키가 호스트의 것인지에 대한 메커니즘이 제공되지 않으므로 비인가 된 접근과 중간자공격과 같은 취약성이 존재한다. 이에 대한 대응방안으로 Accountable Key Infrastructure(AKI)이 제안되었다. AKI는 기존의 PKI의 취약성인 “single point failure”를 극복하기 위한 기반환경에서 각 영역의 구성요소 간 발생하는 트랜잭션을 감시하고 있다[2][6].

AKI 인프라는 기존의 인증체계의 CA 이외의 Integrity Log Server와 Validator가 구성되고 있다. Integrity Log Server는 인증서를 해쉬트리 기반으로 인증서를 저장하며 그 상위 노드는 아래의 자식 노드 데이터 값을 해쉬값으로 결정하는 특징이 있다. 인증서를 효과적으로 관리할 수 있으며 데이터 변조에 대해서 빠르게 대처할 수 있다. 그러므로 AKI는 분산 구조를 통하여 개인키에 대한 위협이 발생하더라도 인증서에 대한 신뢰성을 보장할 수 있다[2-3][6].

2. 스마트 홈 환경 보안위협 및 요구사항

IoT기반기술을 적용하고 있는 스마트 홈 환경에서는 인증·인가, 암호화, 프라이버시 침해 및 정보노출, 웹·앱·소프트웨어 취약점 등과 같은 보안위협에 노출될 수 있다. 대표적인 사례에서는 홈서비스 환경에서 네트워크에 연결된 Device의 관리부족으로 인하여 다양한 공격기법들이 발생할 수 있으며, 비인가 된 접근으로 인한 악성코드 트래픽 공격으로 취약점이 발생할 수 있다. 그리고 스마트 Device에서 수집된 Gateway의 정보관리의 미흡으로 인한 사용자 신원정보 유출이 발생하고 있다. 스마트 홈 환경의 구성도는 그림 1과 같으며, ICT기반의 서비스를 안전하게 수행하기 위해서는 스마트 기기 및 정보에 대한 서비스 운영, 접근 권한 관리, 종단 간 통신 보안, 무결성/인증제공에 대한 보안요구 사항이 제공되어야 한다[4].

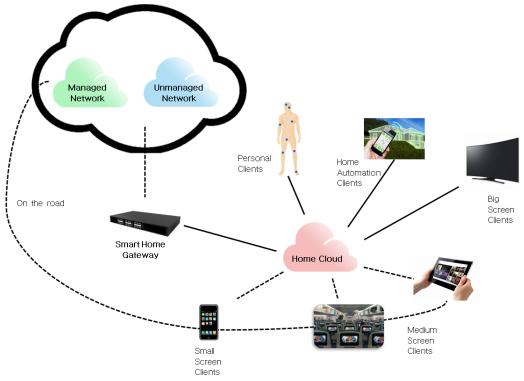

그림 1. 스마트 홈 환경의 구성도
Fig. 1. Configuration of Smart Home Environment

ICT기반의 서비스에서는 디바이스, 네트워크 플랫폼/서비스 단계로 나누어 보안 요구사항을 정리하고 있다. 디바이스영역에서는 무결성 검증/보장이 되어야 하고 D2D 상호인증이 제공되어야한다. 네트워크 영역에서는 IoT Device가 통신을 수행할 때 데이터가 모니터링 되어야 하고 Device도 관리되어야 한다. 또한 종단과 종단간의 보안, 통신보안 및 침입탐지가 수행되어야 한다. 마지막으로 서비스/플랫폼에서는 상호인증이 수행되어야 하고. 경량 암호, 키 관리, 접근제어 및 데이터 누출방지 및 관리가 제공되어야 한다[4][7][8].

Ⅲ. 제안프로토콜

본 논문에서는 스마트 홈 환경에서 AKI 기반의 인증체계기반으로 안전한 통신 시스템을 설계하였다. 기기등록 및 인증서 발급과정, 인증 및 메시지 통신 과정, 인증서 발급 프로토콜을 설계한다. 사용자는 Smart Home based Device를 스마트폰을 활용하여 등록 및 인증하여 Device에서 수신된 데이터를 안전하게 통신 할 수 있다. 제안된 시스템의 전제 조건은 다음과 같으며, 본 장에서 나오는 약어는 표 1과 같으며 전제조건은 아래와 같다.

1. 제안된 Smart Home환경의 인증체계는 AKI기반의 인증 시스템을 수행한다.
2. Certificate Agency와 Integrity Log Server는 SHA1withECDSA기반의 암호체계를 활용하여 서명 값을 생성한다.

표 1. 약어표
Table 1. abbreviation

Symbol	Description
$Device_{SN}$	Serial Number of Device
T_{Device}	Generated TimeStamp of Device
$Device_{Signature}$	Signature Value of Device
$User_{Signature}$	Signature Value of User
$Phone_{nonce}$	Generated nonce of Smart Phone
$Phone_{IMEI}$	IMEI of Smart Phone
$User_{PWD}$	Password of User
$User_{info}$	Information of User
$Gateway_{notation}$	notation of Gateway
$Gateway_{nonce}$	Generated nonce of Gateway
$Gateway_{cert}$	AKI Infrastructure Based Certification of Gateway
$ILS_{Signature}$	Signature Value(ECDSA) of Integrity Los Server
$Device_{Data}$	Data of Device
$Time_{Current\ Time}$	Current Time

1. 기기 등록 및 인증 발급 절차

사용자는 Smart기반 Iot Device를 등록하기 위해서 스마트폰을 활용하여 게이트웨이를 거쳐서 Certificate Agency로 AKI기반 인증서를 발급받는다. 이후 Integrity Log Server에서 AKI기반의 인증서를 검증 후 Device를 등록한다.

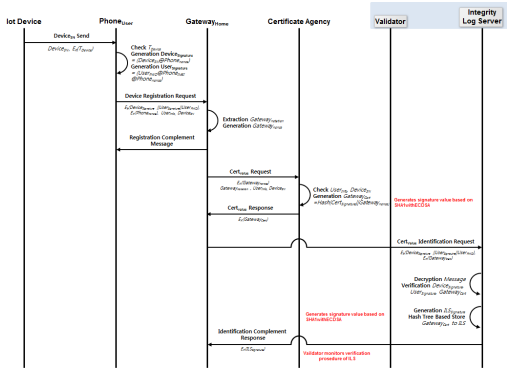

그림 2. 디바이스 등록 및 인증서 발급 과정
Fig. 2. Device Registration and Certificate Issue Phase

1. IoT Device를 등록하기 위해서 사용자는 IoT Device를 이용하여 디바이스의 Serial Number를 Smart Phone으로 발송한다.
$Device_{SN}, E_k(T_{Device})$

2. Smart Phone에서는 수신된 메시지의 타임스탬프를 검증한다. 이후 난수를 생성하고 Device, 사용자의 서명 값을 생성한다.

$Device_{Signature} = (Device_{SN} \oplus Phone_{nonce})$

$User_{Signature} = (User_{PWD} \oplus Phone_{IMEI} \oplus Phone_{nonce})$

3. 사용자는 Gateway로부터 디바이스 등록 요청 메시지를 발송한다.

$E_k(Device_{Signature} \| User_{Signature} \| User_{PWD})$,
$E_k(Phone_{nonce})$, $User_{Info}$, $Device_{SN}$

4. Gateway에서는 표기 값을 추출하고 이후 난수를 생성한다. 그리고 Smart Phone으로 등록 완료 메시지를 전송 후 Certificate Agency로부터 인증서 발급 요청을 전송한다.

$E_k(Gateway_{nonce})$, $Gateway_{\text{ation}}$, $User_{\infty o}$, $Device_{SN}$

5. Certificate Agency에서는 사용자의 정보, Device Serial Number를 체크 후 인증서를 발급한다. (Certificate Agency에서는 Sha1 with ECDSA기반으로 서명 값을 생성한다.)

$Gateway_{Cert} =$
$Hash(Cert_{Signature} \| Gateway_{nonce})$

6. Certificate Agency는 Gateway로 발급된 인증서를 발송한다.

$E_k(Gateway_{cert})$

7. Gateway에서는 발급된 인증서와 Gateway를 검증하기 위해서 식별 요청 메시지를 전송한다.

$E_k(Device_{Signature} \| User_{Signature} \| User_{Pwd})$,
$E_k(Gateway_{cert})$

8. Integrity Log Server는 수신된 메시지를 복호화 후 디바이스, 사용자 서명값, 인증서를 검증한다. 이후 Integrity Log Server서명 메시지를 생성 후 해쉬 트리기반으로 Integrity Log Server에 인증서를 저장한다.

9. Integrity Log Server는 Gateway로부터 식별 완료 메시지를 전송한다. (Integrity Log Server로 검증을 수행할 때 Vaildator로 통하여 감시한다.)

$E_k(ILS_{Signature})$

2. 인증 및 메시지 프로토콜 설계

본 절에서는 앞 절에서 생성된 인증서를 기반으로 사용자가 통신을 수행한다. 인증서를 검증 후 디바이스와 Gateway에서 TLS를 설립하여 데이터를 전송한다. Gateway는 사용자는 데이터를 전송함으로서 제안된 프로토콜을 마무리한다.

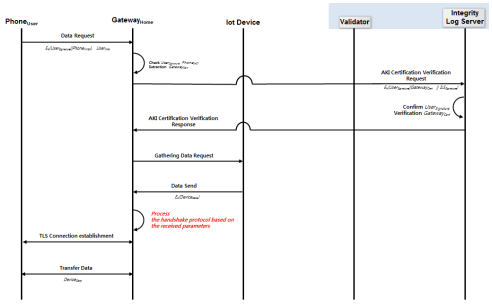

그림 3. 인증 및 메시지 통신 설계
Fig. 3. Authentication and Message Communication Protocol

1. 사용자는 Smart Phone을 활용하여 Gateway로 데이터 요청 메시지를 전송한다.

$E_k(User_{Signature} \| Phone_{IMEI})$, $User_{info}$

2. Gateway에서는 사용자의 서명 값과 스마트폰의 IMEI를 검증 후 저장된 인증서를 추출하여 Integrity Log Server로 인증서 검증 요청 메시지를 전송한다.

$E_k(User_{Signature} \| Gateway_{cert} \| ILS_{signature})$

3. Integrity Log Server는 사용자의 서명 값, 자신에서 생성된 서명 값을 확인하고 해쉬트리 기반의 저장된 인증서를 비교분석 및 검증한다.

4. Gateway로 AKI 인증 검증 응답 메시지를 전송한다. 이후 Gateway에서는 IoT Device 로 수집된 데이터를 요청한다.

5. IoT는 수집된 데이터를 Gateway로 전송한다. Gateway는 Smart Phone과 앞 절 등록과정에서 수신된 파라미터를 기반으로 TLS Connection을 설립한다.

$E_k(Device_{Data})$

6. Gateway에서 수집된 데이터는 Smart Phone으로 TLS 안전하게 설립된 채널로 데이터 전송을 한다.

3. 인증서 관리 프로토콜 설계

Certificate Agency에서 발급된 인증서를 관리하는 프로토콜을 수행한다. 기존의 PKI 인증서 체계와는 달리 Vaildator에서 Integrity Log Server로 인증서 유효성을 요청한다. 이후 Certificate Agency와 Gateway를 검증하여 발급된 인증서의 유효성 검사를 수행하여 갱신한다. 제안된 인증서 관리 프로토콜 절차는 그림 4와 같다.

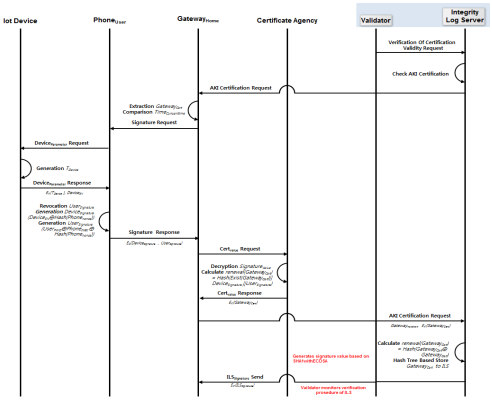

그림 4. 인증서 발급 관리 프로토콜 설계
Fig. 4. Design of Authentication Certification Management Protocol

1. Validator는 Integrity Log Server로 인증서 유효성 검증 요청 메시지를 전송한다.

2. Integrity Log Server 해쉬트리 저장된 AKI기반의 인증서를 검증 후 Gateway로 인증서를 요청한다.

3. Gateway에서는 인증서를 추출하고 저장된 시간과 현재시간을 비교분석 후 등록된 Smart Phone으로 서명 값을 요청한다.

4. Smart Phone에서는 IoT Device로 서명값을 요청 메시지를 전송한다. 이후 IoT Device에서는 TimeStamp를 생성한다.

5. IoT Device에서는 Smart Phone으로 Device Parameter를 전송한다.
$E_k(T_{Device}), Device_{SN}$

6. Smart Phone에서는 메시지를 수신하고 사용자의 서명 값을 갱신한다. 이후 디바이스 서명 값, 사용자 서명 값을 갱신한다.
$Device_{Signature} = (Device_{SN} \oplus Hash(Phone_{nonce})$
$User_{Signature} = (User_{PWD} \oplus Phone_{IMeI} \oplus Hash(Phone_{nonce})$

7. Smart Phone에서는 Gateway로 서명 값을 전송한다.
$E_k(Deivce_{Signature}, User_{Signature})$

8. Gateway에서는 Certificate Agency로 인증서 갱신을 요청한다.
$renewal(Gateway_{cert}) = Hash(Exist(gateway_{cert}) \| Device_{Signature} \| User_{Signature})$

9. Certificate Agency는 갱신된 인증서를 Gateway로 전송한다.
$E_k(Gateway_{cert})$

10. Gateway에서는 갱신된 인증서를 Integrity Log Server로 전송한다.
$Gateway_{notation}, E_k(Gateway_{cert})$

11. Integrity Log Server에서는 갱신된 인증서를 검증 후 해쉬 트리기반으로 인증서를 저장한다.
$renewal(Gateway_{cert}) = Hash(Gateway_{cert} \oplus Gateway_{cert})$

12. 등록과정과 마찬가지로 Sha1withECDSA기반으로 서명 값을 생성 후 Gateway로 전송한다. (등록과정과 마찬가지로 Integrity Log Server로 검증을 수행할 때 Vaildator로 통하여 감시한다.)
$E_k(ILS_{Signature})$

Ⅳ. 성능평가

1. 보안성 및 효율성 평가

본 절에서는 기존의 PKI기반 CA가 발급한 인증 시스템과 제안한 방식의 AKI시스템의 인증시스템의 보안성을 비교분석하였다. 수행과정, 발급기관의 작업량, 인증서 관리사항, 공격기법, 특징에 대해서 분석한 결과는 표 2와 같다.

표 2. 기존 시스템과 제안된 인증시스템 보안성 비교
Table 2. Security Comparison of Exist System and Proposed Authentication System

classification	PKI based Authentication System	Proposed Authentication System
Process of Achieve (Message Communication)	3E+3D+2S+2C	3E+3D+2S+1C
Workload of issuing organization	Overhead High	Overhead Low
Authentication Management	Support (Speed Low)	Support (Speed High)
Attack Technique	MitM Attack Replay Attack Reliability low of CA	-
Feature	PKI Based Authentication System	AKI Based Authentication System

효율성을 평가하기 위해서 본 논문에서 제안된 서명 기법 Sha1 with ECDSA(ECC160)과 기존의 RSA 2048 X.509를 JAVA환경의 JCE의 기반의 Eclipse Tool을 활용하여 비교분석하였다. 서명 수행속도에 대해 대략 41%, 메시지 통신과정에 대해서 대략 85%을 향상된 수치를 확인 할 수 있었다. 효율성 분석에 대한 수치는 그림 5와 같다.

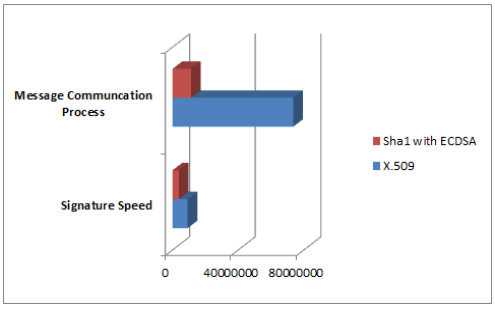

그림 5. 기존 암호시스템과 제안된 시스템의 성능 분석
Fig. 5. Performance Analysis of X.509 Based Cryptosystem And ECDSA based Cryptosystem

2. 안전성 분석

Session Hijacking 에 대한 위협

세션 하이재킹은 서버와 클라이언트가 통신할 때 시퀀스 넘버의 취약성을 이용하여 파고드는 공격으로 Gateway와 Smart Phone간의 통신을 수행할 때 위협을 받을 수 있다. 하지만 통신 프로토콜에서 $Device_{SN}$, $User_{Signature}$, $User_{PWD}$, $Gateway_{\text{ation}}$의 기반으로 시퀀스 넘버와 조합하여 TLS Connection을 설립 후 데이터를 전송함으로써 안전하다.

중간자 공격 및 재전송 공격

Smart Home 환경에서 공격자가 취약한 디바이스에 접근 및 Gateway와 Smart Phone간의 통신과정에서 정보가 누출되는 중간자 공격이 가능하다. 이를 보안하기 위해서 등록과정에서 발급된 AKI기반의 인증서($Gateway_{cert}$)를 활용하여 Integrity Log Server에서 검증 후 Validator에서 트랜잭션을 감시함으로써 보완할 수 있다. 그리고 재생공격에 대한 위협에서는 해쉬트리기반으로 생성 후 ILS가 서명된 $ILS_{Signature}$를 검증함으로써 재생공격은 실패로 끝난다.

비 인가된 접근에 대한 위협

악의적인 사용자가 Smart Home 환경에서 Gateway로 접근하는 사례가 발생하고 있다. 본 논문에서는 Smart Phone의 $User_{Pwd}$, $User_{info}$뿐만 아니라 사용자가 서명한 $User_{Signature}$를 검증함으로써 비인가 된 사용자의 대한 접근이 불가능하다.

프라이버시 위협 및 정보 누출

IoT기반의 융합 환경에서는 프라이버시 위협 및 정보 누출에 대한 논란이 꾸준히 제기되고 있다. 프라이버시의 보안성을 강화하기 위해서 본 논문에서는 인증서 관리 프로토콜을 설계하여 $Device_{Signature}$, $User_{Signature}$, $Gateway_{Cert}$ 주기적으로 갱신하도록 하였다. 또한 AKI 인프라에서 Validator가 Smart Home 환경의 Device, Gateway의 생성된 데이터를 추적 및 감시함으로써 정보 누출에 대한 피해가 감소한다.

V. 결 론

본 논문은 스마트 환경에서 AKI기반의 공개키 검증 인프라를 활용하여 인증서 관리 및 안전한 통신 기법에 관하여 연구하였다. 기존의 PKI의 X.509 인증서 관리체계와 대비 AKI기반의 Certificate Agency, Integrity Log

Server, Vaildator의 시스템을 추가적으로 구성한 인증구조, 통신 시스템, 인증서 발급 관리 시스템을 제안하였다.

제안된 시스템은 스마트 환경의 보안위협인 Session Hijacking 에 대한 위협, 중간자 공격 및 재전송 공격, 비인가된 접근에 대한 위협, 프라이버시 위협 및 정보 누출에 관하여 안전성을 분석하였다. 그리고 기존의 PKI 인증 시스템과 제안된 시스템의 보안성 평가와 제안된 암호시스템의 효율성을 분석하였다. 기존 대비 대략 41%의 향상성을 확인할 수 있었다.

향후 본 논문에서 제안된 인증관리 및 통신 기법은 Smart Home 환경뿐만 아니라, IoT기반의 ICT융합 환경에서 다양하게 활용될 것을 기대하고 있다. 그러나 IoT 기기에서 사용자로부터 통신을 수행할 때 안전한 통신뿐 만아니라, 사용자에 대해서 식별 후 등급을 파악하여 알맞은 메시지를 전송하는 통신기법에 대한 연구가 요구될 것으로 예상하고 있다.

References

[1] Ho-Seok Ryu, Jin Kwak, “Analysis of Security Threats and Security Requirements in Smart Home”, No. 10, pp. 113-114, 2014. 10.

[2] Tae-Hwan Kim, Jeong Hwa Hong, Hee Young Jung, “Trend in Trustworthy Communication for the Next-Generation”, ETRI, 2015. 8

[3] Gi-Tae Park, Jae Hwoon, Hee Young Jung, “Improved Accountable Internet Protocol Using Signature”, JKICS, Vol 39B, No. 4, 2014

[4] Seung-su Yang, Jae-Sung Shim, Seog-Cheon Park, “Analysis of Countermeasures and Network Security Vulnerability for IoT Smart Home”, Conference, Vol 23, No 1, 2016. 4

[5] Byung Wook Jin, Jae- Pyo Park, Keun Wang Lee, Moon Seog Jun, “A Study of Authentication Method for Id-Based Encryption Using In M2M Environment”, KAIS, Vol. 14, No. 4, pp 1926-1934, 2013

[6] A. Beimel. Secure Schemes for Secret Sharing and Key Distribution. PhD thesis, Israel Institute of Technology, Technion, Haifa, Israel, 1996.

[7] Kossinets, G. and D.J. Watts, “Origins of Homophily in an Evolving Social Network”, American Journal of Sociology, Vol.115, 2005, 405-500. doi:10.1086/599247 (Downloaded February 28, 2010).

[8] Younghwa An, “A Strong Biometric-based Remote User Authentication Scheme for Telecare Medicine Information Systems with Session Key Agreement”, IJASC, Vol.8 No.3, pp.41-49, 2016

저자 소개

진 병 욱(정회원)

- 2000년 7월 : 청운대학교 멀티미디어학과 졸업
- 2013년 2월 : 숭실대학교 컴퓨터공학 석사
- 2013년 3월 ~ 현재 : 숭실대학교 컴퓨터학과 박사과정

<주관심분야 : 네트워크 보안, 인증 시스템, IoT>

- E-mail : quddnr4511@naver.com

박 중 오(정회원)

- 2000년 7월 : 성결대학교 컴퓨터공학과 졸업
- 2003년 3월 : 명지대학교 전자계산교육 석사
- 2011년 8월 : 숭실대학교 컴퓨터공학 박사
- 2013년 3월 ~ 2016년 2월 : 동양미래대학교 조교수
- 2016년 3월 ~ : 성결대학교 조교수

<주관심분야 : PKI, Network security, 암호학>

- E-mail : jopark02@sungkyul.ac.kr

전 문 석(정회원)

- 1989년 2월 : University of Maryland Computer Science 박사
- 1989년 9월 ~ 1991년 2월 : New Mexico State University Physical Science Lab. 책임연구원
- 1991년 3월 ~ 현재 : 숭실대학교 정교수

<주관심분야 : 정보보호, 네트워크 보안, 암호학>

- E-mail : mjun@ssu.ac.kr