Journal of the Korea Convergence Society
Vol. 8. No. 7, pp. 15-21, 2017
https://doi.org/10.15207/JKCS.2017.8.7.015

파스칼 삼각 이론 기반의 IoT 장치간 효율적인 인증 설립 기법

한군희[1], 정윤수[2*]
[1]백석대학교 정보통신공학과, [2]목원대학교 정보통신융합공학부

Efficient Authentication Establishment Scheme between IoT Device based on Pascal Triangle Theory

Kun-Hee Han[1], Yoon-Su Jeong[2*]
[1]Dept. of Information Communication & Engineeringe, Baeseok University
[2]Dept. of information Communication Convergence Engineering, Mokwon University

요 약 최근 4차 산업 혁명이 사회적으로 대두되면서 IoT 관련 제품에 대한 사용자들의 관심이 증가하고 있다. IoT 장치에 사용되고 있는 센서의 종류와 기능은 점점 다양화되고 있어 IoT 장치의 상호 인증 기술이 요구되고 있다. 본 논문에서는 서로 다른 종류의 IoT 장치들이 서로 상호 연계하여 원활하게 동작될 수 있도록 파스칼 삼각형 이론을 이용한 효율적인 이중 서명 인증 키 설립 기법을 제안한다. 제안 기법은 IoT 장치간 인증 경로를 2개(주 경로와 보조 경로)로 구분하여 IoT 장치의 인증 및 무결성을 보장한다. 또한, 제안 기법은 IoT 장치를 인증할 때 추가적인 암호 알고리즘이 필요하지 않도록 키를 생성하기 때문에 적은 용량을 필요로 하는 IoT 장치에 적합하다. 성능 평가 결과, 제안 기법은 IoT 장치의 지연시간을 기존 기법보다 6.9% 향상되었고, 오버헤드는 기존 기법보다 11.1% 낮은 결과를 얻었다. IoT 장치의 인증 처리율은 기존 기법보다 평균 12.5% 향상되었다.

• 주제어 : RFID, 인증, 사물 인터넷 기술, 키 설립, 4차 산업 혁명

Abstract Recently, users' interest in IoT related products is increasing as the 4th industrial revolution has become social. The types and functions of sensors used in IoT devices are becoming increasingly diverse, and mutual authentication technology of IoT devices is required. In this paper, we propose an efficient double signature authentication scheme using Pascal's triangle theory so that different types of IoT devices can operate smoothly with each other. The proposed scheme divides the authentication path between IoT devices into two (main path and auxiliary path) to guarantee authentication and integrity of the IoT device. In addition, the proposed scheme is suitable for IoT devices that require a small capacity because they generate keys so that additional encryption algorithms are unnecessary when authenticating IoT devices. As a result of the performance evaluation, the delay time of the IoT device is improved by 6.9% and the overhead is 11.1% lower than that of the existing technique. The throughput of IoT devices was improved by an average of 12.5% over the existing techniques.

• Key Words : RFID; Authentication; Internet of Thing; Key Establishment; 4th industrial revolution

*교신저자 : 정윤수(bukmunro@mokwon.ac.kr)
Received May 22, 2017 Revised June 19, 2017
Accepted July 20, 2017 Published July 28, 2017

1. 서론

최근 4차 산업혁명이 사회적으로 대두되면서 사물인터넷(IoT, Internet of Things)에 관한 관심이 꾸준히 증가하고 있다. 사물인터넷은 유·무선 네트워크를 이용해서 사물끼리 실시간으로 데이터를 송·수신하는 기술이다. IoT 장치에 연결되어 있는 사물들은 소규모의 센서들이 내장되어 있어 인공지능 TV, 도어락, 홈 캠, 에어닥터, 스마트 플러그, 헬스바이크, 헬스밴드, 체지방계 등에서 대표적으로 사용되고 있다. 그러나, IoT 장치는 인터넷으로 연결된 외부 환경으로부터 정보를 획득하기 때문에 악의적으로 접근하는 제3자의 접근을 제어하지 못한다면 손쉽게 해킹이 될 수 있는 위험이 존재한다.

IoT 장치와 관련하여 기존 연구에서는 IoT 장치만을 인증하기 위해 사용되는 연구보다는 대부분 하나의 암호화 키로 네트워크 전체에 사용하는 연구를 수행하여 왔다. 이 연구는 네트워크 계층에서 사용되는 초기 보안 프로토콜로써 홉 단위로 데이터를 보호한다[6]. 또한, 통신 전에 IoT 장치에 키가 업데이트되기 때문에 사전에 키가 공유하도록 사용된다. 최근 IoT와 관련된 보안 연구에서는 데이터그램 전송 계층의 보안 프로토콜을 연구하고 있다.

Sahid Raza 기법은 IoT 장치를 위한 경량 보안 솔루션을 제안하였다[11]. 이 기법은 IPSec, DTLS 및 IEEE 802.15.4 보안 등에서 사용할 수 있지만 인증을 수행하기 위해서는 사전에 공유 키를 공유해야 하는 문제점이 존재하였다.

Daniele Trabalza 기법은 CoAPS 프로토콜을 통해 사물의 인터넷에서 센서 노드와 같은 다른 엔드 포인트 사이의 컴퓨터 통신에 기계에 대한 기밀성과 무결성을 제공하였다[13]. 그러나, DTLS의 구현은 표준 사전 키 메커니즘을 공유하는 문제점이 존재하는 단점이 있다.

4차 산업 혁명에서 반드시 필요한 IoT 인증은 사람과 사물이 보다 안전하게 정보를 송·수신할 수 있도록 이기종간 사용될 수 있는 다양한 유·무선 통신에 대해서 보안 취약성을 항시 점검해야 할 필요성이 있다[14].

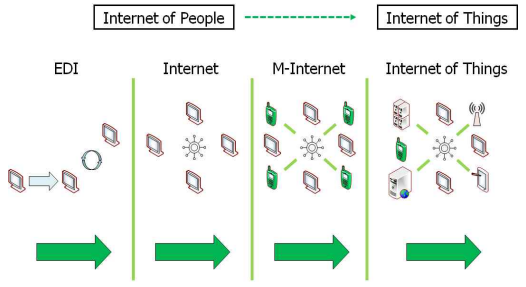
본 논문에서는 이기종간 IoT 장치의 상호 인증을 효율적으로 처리하기 위한 이중 서명 인증 키 설립 기법을 제안한다. 제안 기법은 파스칼 삼각형 이론을 이용하여 이중 서명 인증을 수행하기 때문에 IoT 장치에 추가적인 암호 알고리즘 없이 인증을 수행할 수 있는 키를 손쉽게 생성할 수 있다. 제안 기법은 적은 용량을 가지는 IoT 장치에 적합한 인증 기법을 제시함으로써 IoT 장치의 효율성을 향상시키는 것을 목적으로 한다. 특히, 제안 기법은 IoT 장치들을 서로 상호 인증하기 위해서 인증 경로를 주 경로와 보조경로 등으로 구분하여 IoT 장치들에 대한 인증 및 무결성을 체크한다. 주 경로는 IoT 장치간 연계된 모든 IoT 장치들의 인증을 수행하기 위해서 사용되며, 보조 경로는 IoT 장치간 인증과 무결성을 체크하는 용도로 사용한다. 이 같은 과정을 통해 제안 기법은 IoT장치간 연계 처리되는 정보들의 접근성을 향상시킨다.

이 논문의 구성은 다음과 같다. 2장에서는 IoT 및 기존 연구에 대해서 알아본다. 3장에서는 파스칼 삼각 이론을 이용한 IoT 장치간 효율적인 인증 기법을 제안하고, 4장에서는 제안 기법과 기존 기법과 비교 평가하고 마지막으로 5장에서 결론을 맺는다.

2. 관련연구

2.1 IoT

IoT 기술은 4차산업 혁명이 대두되면서 가장 인기있는 서비스 기술 중 하나이다[21,22,23,24]. IoT 기술은 기존 인터넷 표준과 상호 호환 가능한 통신 프로토콜들을 이용하여 네트워크 인프라를 동적 글로벌화가 가능하도록 확장되고 있다[1,14,15,16,17]. IoT 기술은 시기에 따라 다양하게 사용되었다. IoT 서비스가 초기였을 때는 M2M(Machine to Machine) 즉, 교통카드, 택배배송 추적 시스템, 공장/설비관리, ATM, 내비게이션, 바코드 등에 활용되었다. 최근 무선 통신 기술이 발전하면서는 스마트폰, e-book 단말기 그리고 테블릿 등과 같은 장치를 사용한 서비스(스마트그리드, 지능형 차량 서빗, 헬스케어, 스마트홈 등)에서 활용 가능하다.



[Fig. 1] Process of IoT change due to evolution of communication environment

2012년 9월 한국인터넷진흥원은 [Fig. 1]처럼 통신환경 진화에 따른 IoT 변화 과정을 분석하였다[25,26]. [Fig. 1]처럼 IoT는 통신망 연결(Internet)에서 시작하여 컴퓨터와 커넥티드 단말기를 연결(M-Interent)하도록 변화하였고, 최근에는 주변의 모든 기기들이 통신 기능을 부착하여 서비스를 제공할 수 있도록 연결 범위가 확장되고 있다.

2.2 기존 연구

IoT 에서 사용되고 있는 초기 보안 프로토콜은 홉 단위로 홉 데이터의 보안성을 고려하고 있다. 대부분의 경우 하나의 암호화 키는 네트워크 전체에 사용된다[6,18,19,20].

IoT 에서 사용되는 보안 프로토콜의 대부분은 키 노드에 배포되는 적절한 메커니즘 방법이 없다. 대부분의 경우 키는 통신 전에 노드에 업데이트되는 키 분배의 사전 공유 메커니즘을 사용한다[7].

IoT 분야에 종사하는 연구자는 이미 IP를 기반으로 자원이 제한된 장치의 보안을 향상시키기 위한 해결책을 제시하고 있다[8]. 최근 많은 연구자들은 IoT를 고려한 데이터그램 전송 계층의 보안 프로토콜을 연구하고 있다. Sahid Raza는 [11]에서 IoT에 사용하기 위한 경량 보안 솔루션을 제안했다. 이 솔루션은 IoT에서 보안 통신을 위해 IPSec, DTLS, 및 IEEE 802.15.4 보안의 사용을 조사하였지만 여전히 이 방식은 인증을 위한 사전 공유 키에 따라 달라지는 문제점을 가지고 있다.

Sahid Raza는 [12]에서 헤더 압축에 의해 DTLS의 오버 헤드를 줄일 수 있는 가능성을 시사하고 있다. 그러나 [12]는 IoT에서 효율을 증가시키는 목적으로 사용한 헤더 압축이 보안에 문제가 있다는 것을 보여주었다.

Daniele Trabalza은 안드로이드 장치와 같은 CoAPS 프로토콜을 통해 사물의 인터넷에서 센서 노드와 같은 다른 엔드 포인트 사이의 컴퓨터 통신에 기계에 대한 기밀성과 무결성을 제공했다[13]. 그러나, DTLS의 구현은 표준 사전 키 메커니즘을 공유하는 문제점이 존재한다.

3. 파스칼 삼각형 이론 기반의 키 설립 기법

이 절에서는 이기종간 IoT 장치의 상호 인증을 효율적으로 처리하기 위해서 파스칼 삼각형 이론을 이용한 이중 서명 인증 키 설립 기법을 제안한다. 제안 기법은 IoT 장치의 추가적인 암호 알고리즘 없이 적은 용량으로 IoT 장치를 인증할 수 있는 키를 생성함으로써 IoT 장치의 효율성을 향상시키는 것을 목적으로 한다.

3.1 IoT 키 생성 과정

제안 기법에서는 수 많은 이기종간 IoT 장치를 서로 인증하기 위해서 바로 이웃하지 않은 IoT 장치에 인증 정보를 전달하도록 해쉬 체인을 구성한다. 제안 기법에서 해쉬체인 형태로 인증 정보를 구성하는 이유는 통신 상태나 환경에 따라 IoT 장치 중 인증에 참여하지 못하는 IoT 장치를 통해 발생할 수 있는 안전성을 보장하기 위해서이다.

제안 기법은 IoT 장치 사이에서 실시간으로 이루어지기 위해서 인증에 사용되는 첫 번째 IoT 장치와 마지막 IoT 장치에 전자 서명을 생성하여 인증과 부인방지를 모두 제공하고 있다. 제안 기법은 인증에 참여하는 IoT 장치 중 일부 IoT 장치에 한해서 전자 서명으로 인증을 수행하기 때문에 기존 기법보다 IoT 장치 간 오버헤드를 최소화 할 수 있다. 제안 기법은 다음과 같은 4단계를 거쳐 인증키를 생성하는 과정을 수행한다.

- 단계 1 : 인증 키를 생성하기 위한 IoT 장치 수가 k이고, IoT 장치의 시드가 s 라고 할 때, 첫 번재 IoT 장치는 ${}_R\{0,1\}^k$으로부터 임의로 안전하게 선택한 시드 s를 선택하여 식 (1)을 생성한다.

$$h^k(s) = \begin{cases} a_{(s-1)(k-1)} + a_{(s-1)k} & , \text{if } s,k > 1 \\ 1 & , otherwise \end{cases} \quad \text{식 (1)}$$

- 단계 2 : 제안 기법은 이중 서명을 위해 ${}_R\{0,1\}^k$로부터 개인키 역할을 수행하는 2개의 램덤 수 x_1^0, x_1^1를 식 (2)처럼 선택한다.

$$x_i^{\zeta[i]} = \begin{cases} x_i^0 & , \text{if } \zeta[i] = 0 \\ x_i^1 & , \text{if } \zeta[i] = 1 \end{cases} \quad \text{식 (2)}$$

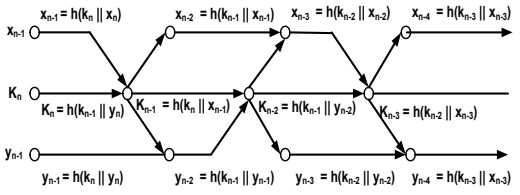
여기서, ζ의 i번째 이진 값에서 선택한 $\zeta[i]$은 첫 번째 한 이진 값을 0과 1중에서 하나를 선택하여 개인키 (x_i^0와 x_i^1)를 표시한다.

· 단계 3 : IoT 장치는 두 개의 새로운 개인키 x_{i+1}^{0}와 x_{i+1}^{1}를 생성하여 식 (3)과 같이 개인키와 대응되는 공개키를 생성한다. 이 때, 공개키는 개인키로부터 계산될 수 있기 때문에 IoT 장치에 저장하지 않는다.

$$PK_{i+1}^{\lambda} = h(x_{i+1}^{\lambda}) = \begin{cases} PK_{i+1}^{0} = h(x_{i+1}^{0}) & , \text{if } \lambda = 0 \\ PK_{i+1}^{1} = h(x_{i+1}^{1}) & , \text{if } \lambda = 1 \end{cases} \quad \text{식 (3)}$$

3.2 IoT 장치 연계 과정

제안 기법에서는 이중 서명을 통해 IoT 장치를 인증하기 위해서 [Fig. 2]처럼 IoT 장치에 대한 인증 경로를 사용한다. [Fig. 2]처럼 제안 기법은 IoT 장치가 추가될수록 오버헤드를 최소화하기 위한 인증 경로를 주 경로와 보조 경로로 구분한다. 주 경로는 연계된 모든 IoT 장치들의 인증을 위해 사용되며, 보조 경로는 IoT 장치간 인증과 무결성을 체크하는 용도로 사용한다.



[Fig. 2] Multipath Hash Chain of Proposed Scheme

식 (4)은 IoT 장치를 병합하기 위해 수행되는 IoT 장치의 해쉬체인 값을 나타내고 있다. 이 때, 해쉬 체인 값은 IoT 장치 수 n에 따라 식 (4)와 같이 짝수와 홀수로 나누어 해쉬 값을 생성한다.

$$k_n = \begin{cases} h(k_{n-1} \parallel y_n) & n\text{=짝수} \\ h(k_n \parallel x_{n-1}) & n\text{=홀수} \end{cases} \quad \text{식 (4)}$$

이 때, x_n과 y_n이 보조 경로인 경우 $n-1$번째 키 값을 식 (5)~식 (6)과 같이 해쉬 함수를 통해 구한다.

$$x_n = h(k_{n-1} \parallel x_{n-1}) \quad \text{식 (5)}$$

$$y_n = h(k_{n-1} \parallel y_{n-1}) \quad \text{식 (6)}$$

3.2 IoT 장치 인증과정

제안 기법에서 IoT 장치간 인증을 수행하기 위해서 사용되는 생성자(generator)는 다음의 4단계 과정을 통해서 n의 값이 0일 될 때까지 반복적으로 수행한다.

- 단계 1 : IoT 장치간 인증에 필요한 생성자를 구하기 위해서 IoT 장치로부터 전달된 n의 값을 순차적으로 감소(n>0)시킨다.
- 단계 2 : 첫 번째 IoT 장치로부터 전달된 n의 값은 식 (4)와 같이 짝수와 홀수로 구분하여 생성자를 계산한다.
- 단계 3 : IoT 장치간 인증과 무결성을 체크하기 위해서 k_{n+1}를 해쉬 함수에 적용하여 이전 IoT 장치와 연결된 보조 경로 x_n를 계산한다. 생성된 보조 경로 x_n는 IoT 장치간 인증에 사용되는 키를 생성할 때 사용한다.

$$x_n = h(k_{n+1}) \quad \text{식 (7)}$$

- 단계 4 : 생성자는 이중 서명 인증에 필요한 인증 정보를 계산하기 위해서 주 경로 k_n을 보조 경로 x_n와 y_n을 이용하여 식 (8)와 같은 해쉬 값을 계산한다.

$$k_n = h(x_{n-1} \| y_n) \quad \text{식 (8)}$$

4. 평가

제안 기법의 성능평가는 IoT 장치의 인증 지연시간, IoT 장치 간 오버헤드, IoT 장치당 처리되는 인증 처리율 등을 기존 기법과 비교 평가한다.

4.1 실험환경

제안 기법은 IoT 장치의 인증 지연시간, IoT 장치 간 오버헤드, IoT 장치당 처리되는 인증 처리율 등을 평가하기 위해서 <Table 1>과 같은 실험 환경을 설정하여 객관적인 평가가 나타나도록 시뮬레이션을 수행하였다. <Table 1>처럼 IoT 장치는 {1, 3, 5, 10, 25, 50, 100}으로 설정하고, threshold 는 {1, 3, 5}로 설정한다. IoT 장치간 거리는 $1m$로 설정 한 후, 초기 인증 데이터 설정 시간과 인증 데이터 생성 시간은 각각 $0.01ms$와 1 sec로 가정한다.

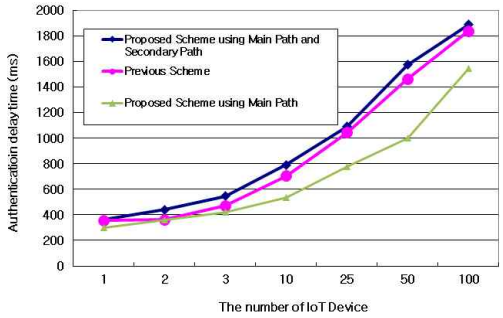
<Table 1> Parameter Setup

Parameter	Setting
Number of IoT devices	N = {1, 3, 5, 10, 25, 50, 100}
threshold	Th = {1, 3, 5}
Transmission of IoT device	1m
Authentication data generation interval	0.01 ms
Initial authentication data set time	1 sec

4.2 성능평가

4.2.1 IoT 장치의 인증 지연시간

[Fig. 2]은 IoT 장치 수에 따른 IoT 장치간 전달되는 인증 정보를 처리하는데 필요한 지연시간을 기존기법과 비교 평가하였다.

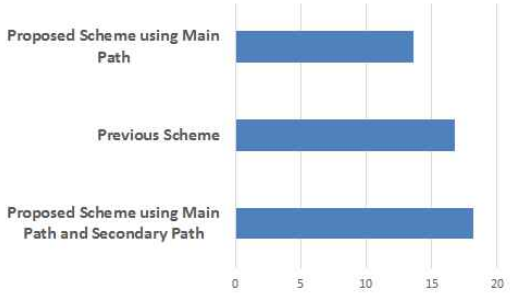


[Fig. 2] Delay time of IoT device

[Fig. 2]처럼 이중 서명을 위해 필요한 2개의 경로(주 경로와 보조 경로) 값을 통해서 IoT 장치의 인증 키 설립을 수행했을 경우, 기존 기법보다 IoT의 인증 지연시간은 평균 6.9% 낮게 나타났다. 주 경로만을 이용한 IoT 인증 지연시간은 기존 기법보다 9.2% 낮은 결과를 얻었지만 주 경로와 보조 경로를 모두 사용한 IoT 인증 지연시간에서는 기존 기법보다 지연시간이 1.5% 낮은 결과를 얻었다. 이 같은 결과는 IoT 장치 사이에서 실시간으로 인증을 이루어지기 위해서 사용된 키가 다중 해쉬 체인을 사용하여 생성되었기 때문에 나타난 결과이다.

4.2.2 IoT 장치 간 인증 처리 오버헤드

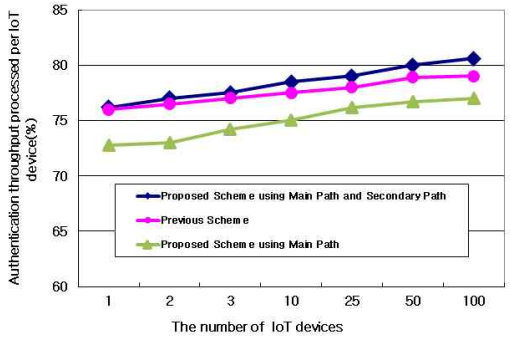
[Fig. 3]은 IoT 장치 간 인증을 수행할 때 사용되는 키가 IoT 장치가 처리할 때 발생되는 오버헤드를 IoT 장치 수 증가에 다라 비교 평가하고 있다. [Fig. 3]의 실험 결과, IoT 장치의 오버헤드는 기존 기법에 비해 11.1% 낮은 결과를 얻었다. [Fig. 3]처럼 제안 기법은 IoT 장치 수가 증가할수록 오버헤드 변화의 크기가 기존 기법보다 낮게 나타났다. 특히, 제안 기법은 파스칼 삼각형 이론을 이용하여 추가적인 암호 알고리즘을 사용하지 않았고, 적은 용량으로 IoT 장치를 인증할 수 있도록 키를 생성하였기 때문에 오버헤드의 변화가 기존 기법보다 높지 않았다.



[Fig. 3] Authentication process overhead between IoT devices

4.2.3 IoT 장치당 처리되는 인증 처리율

[Fig. 4]은 단위 시간당 IoT 장치의 인증 처리율을 나타내고 있다. [Fig. 4]의 결과, 다중 해쉬 체인으로 파스칼 삼각 이론을 적용한 제안 기법이 기존 기법보다 평균 12.5% 높게 나타났다. 이 같은 결과는 제안 기법이 이중 서명을 위해서 2개의 키를 생성하여 사용하더라도 추가적인 암호 알고리즘 없이 다중 해쉬 체인으로 다중의 IoT 장치를 인증 처리하기 때문이다. 특히, 제안 기법은 IoT 장치 수가 많더라도 인증 지연시간이 적게 사용되기 때문에 적은 수의 IoT 장치를 사용할때보다 많은 수의 IoT 장치를 인증 처리할 때가 인증 처리율이 높게 나타났다.



[Fig. 4] Authentication throughput processed per IoT device

5. 결론

4차 산업혁명과 함께 사물인터넷 서비스가 대중화되면서 사물인터넷과 연관된 많은 응용분야가 개발되고 있다. 본 논문에서는 서로 다른 종류의 IoT 장치들이 손쉽게 인증할 수 있도록 파스칼 삼각형 이론 기반의 이중 서명 인증 기법을 제안하였다. 제안 기법은 IoT 장치의 인증 부하를 최소화하기 위해서 첫 번째와 마지막 IoT 장치에 인증 정보를 이용하여 이중 서명이 가능하도록 하였다. 특히, 제안 기법은 IoT 장치간 인증 경로를 2개(주 경로와 보조 경로)로 구분하여 IoT 장치의 인증 및 무결성을 보장할 수 있도록 키를 생성하였다. 성능 평가 결과, 제안 기법은 기존 기법보다 IoT 장치의 지연시간은 6.9% 향상되었고, 오버헤드는 기존 기법보다 11.1% 낮은 결과를 얻었다. IoT 장치의 인증 처리율은 기존 기법보다 평균 12.5% 향상되었다. 향후 연구에서는 본 연구의 결과를 기반으로 실제 사물 인터넷 환경에 적용하여 IoT 장치의 성능평가를 비교 평가할 계획이다.

REFERENCES

[1] S. Haller, S. Karnouskos, and C. Schroth, "The Internet of Things in an Enterprise Context," in Future Internet – FIS 2008 Lecture Notes in Computer Science Vol. 5468, pp. 14-28, 2009.

[2] S. Raza, H. Shafagh, K. Hewage, R. Hummen, and T. Voigt, "Lithe: Lightweight Secure CoAP for the Internet of Things," IEEE Sensors Journal, Vol. 13, No. 10, 2013.

[3] R. Roman, J. Zhou, and J. Lopez, "On the Features and Challenges of Security and Privacy in Distributed Internet of Things," Computer Networks, Vol. 57, Elsevier, pp. 2266-2279, July 2013.

[4] W. Trappe, R. Howard, and R. S. Moore, "Low-Energy Security: Limits and Opportunities in the Internet of Things," IEEE Security & Privacy, Vol. 13, No. 1, pp. 14-21, 2015.

[5] K. Jaffr'es-Runser, M. R. Schurgot, Q. Wang, C. Comaniciu and J M. Gorce, "A Cross-layer Framework for Multiobjective Performance Evaluation of Wireless Ad Hoc Networks," Ad Hoc Networks, Vol. 11, No. 8, pp. 2147-2171, 2013.

[6] D. R. Raymond and S. F. midkiff, "Denial of service in wireless sensor Networks: Attakcs andDefenses", Pervasive Computing, Vol. 7, No. 1, pp. 74-81, Jan-Mar, 2008.

[7] Gupta, M. Wurm, Y. Zhu, M. Millard, S. Fung, N. Gura, H. Eberle and S. C. Shantz, "Sizzle : A standards - Based End to End Security Architecture for the Embeded Internet", Pervasive mobile computing, Vol. 1, pp. 425-446, Dec. 2005.

[8] T. Heer, O. Garcia-Morchon, R. Hummen, S. L. Keoh, S. S. Kumar and K. Wehrle, "Security challenges in the ip based interent of things", Wireless Personal Communications, Vol. 61, No. 3, pp. 527-524, 2011.

[9] R. H. Weber, "Internet of Things: New Security and Privacy Challenges," Computer Law & Security Review, vol. 26, no. 1, pp. 23-30, 2010.

[10] R. Roman, P. Najera, J. Lopez, "Securing the Internet of Things," Computer, vol.44, no.9, pp.51,58, Sept. 2011

[11] Sahid Raza, "Lightweight security solutions for the Internet Of Things", Malardalen University Sweden, 2013.

[12] Shahid Raza, Hossein Shafagh, Kasun Hewage, Rene Hummen, and Hiemo Voigt, "Lithe: Lightweight Secure CoAP for the Internet of Things", IEEE Sensor Journals, 2013.

[13] Daniele Trabalza, "Implementation and Evaluation of Datagram Transport Layer Security for the android operating system", 2013.

[14] H. S. Ning, H. Liu; Y, L.T. "Cyberentity Security in the Internet of Things," Computer, Vol. 46, No.4, pp. 46-53, Apr. 2013.

[15] T. Heer, O. Garcia-Morchon, R. Hummen, S. L. Keoh, S. S. Kumar and K.laus Wehrle. Security challenges in the ipbased internet of things. Wireless Personal Comomunications, Vol. 61, No. 3, pp. 527-542, 2011.

[16] D. R Raymond and S. F. midkiff, "Denial of service

in wireless sensor Networks: Attacks and Defenses" Pervasive Computing, Vol. 7, No. 1, pp. 74-81, Jan- Mar 2008.

[17] V. Gupta, M Wurm, Y. Zhu, M. Millard, S Fung, N. Gura, H. Eberle and S.C. Shantz, "Sizzle: A standards - Based End to End Security Architecture for the Embeded Internet" pervasive moblie computing, Vol. 1, pp. 425-445, Dec. 2005.

[18] J. W. Jung, J. D. Kim, M. G. Song, Chul-Gu Jin, "A study on Development of Certification Schemes for Cloud Security", Journal of digital Convergence , Vol. 13, No. 8, pp. 43-49, 2015.

[19] S. J. Lee and W. S. Bae, "Inter-device Mutual Authentication and Formal Verification in Vehicular Security System", Journal of digital Convergence, Vol. 13, No. 4, pp. 205-210, 2015.

[20] Y. S. Choo, B. W. Jin, J. P. Park and M. S. Jun, "Design The User Authentication Framework Using u-health System", Journal of digital Convergence, Vol. 13, No. 5, pp. 219-226, 2015.

[21] K. B. Kim and H. J. Cho, "A Study on the Regulation Improvement Measures for Activation of Internet of Things and Big Data Convergence", Journal of the Korea Convergence Society, Vol. 8. No. 5, pp. 29-35, 2017.

[22] J. S. Park, "A Data Driven Index for Convergence Sensor Networks", Journal of the Korea Convergence Society, Vol. 7. No. 6, pp. 43-48, 2016.

[23] D. Y. Jung and Y. Y. Sok, "A Study on the Edu-tainer Convergence App for Young Children's Play learning in Mobile Environments", Journal of the Korea Convergence Society, Vol. 7. No. 5, pp. 23-28, 2016.

[24] S. S. Shin, S. H. Lee, "Security Requirements Analysis and Countermeasures in Cloud Computing," Journal of IT Convergence Society for SMB, Vol. 5, No. 1, pp. 27-32, 2015.

[25] H. G. Hong, "Business Process Support Based on IoT Technology," Journal of Convergence for Information Technology , Vol. 7, No. 1, pp. 75-79, 2017.

[26] B. W. Min, "An Improvement of Personalized Computer Aided Diagnosis Probability for Smart Healthcare Service System," Journal of IT Convergence Society for SMB, Vol. 6, No. 4, pp. 85-91, 2016.

저자소개

한 군 희(Han, Kun Hee) [종신회원]

- 2000년 2월 : 충북대학교 컴퓨터공학과(공학박사)
- 2001년 3월 ~ 현재 : 백석대학교 정보통신학부 교수

<관심분야>
멀티미디어, 정보보호

정 윤 수 (Yoon-Su Jeong) [정회원]

- 2000년 2월 : 충북대학교 전자계산학과 이학석사
- 2008년 2월 : 충북대학교 전자계산학과 이학박사
- 2009년 8월 ~ 2012년 2월 : 한남대학교 산업기술연구소 전임연구원
- 2012년 3월 ~ 현재 : 목원대학교 정보통신융합공학부 조교수

<관심분야>
유·무선 통신 보안, 정보보호, 빅 데이터, 헬스케어 서비스, IoT