암호키 기반 IoT 네트워크 보안 시스템 구현

전지수 · 강동연 · 한성화*

동명대학교

Implementation of crypto key-based IoT network security system

Ji-Soo Jeon · Dong-Yeon Kang · Sung-Hwa Han*

TongMyong University

E-mail : ruca1619@naver.com / tmvlem0711@gmail.com / shhan@tu.ac.kr

요 약

IT 융합 연구가 계속 진행되면서 IoT(Internet of Things) 서비스의 범위는 계속 확대되고 있다. IoT 서비스는 목적에 맞는 단말을 사용한다. 이러한 IoT 단말은 단말 자체에 대한 인증 기능이 요구된다. 또, 개인정보 등의 중요 정보를 취급하는 IoT 서비스에서는 전송 데이터의 보안이 필요하다. 본 연구에서는 IoT 서비스에 대하여 단말을 인증하고 단말간 데이터를 안전하게 전송할 수 있는 암호키 기반의 IoT 네트워크 보안 시스템을 구현한다. 본 연구를 통하여 IoT 서비스는 그 자체적으로 단말을 인증할 수 있으며, 전송 데이터의 기밀성을 유지할 수 있다. 다만 IoT 서비스이므로 암호 알고리즘 적용 추가적인 효율 연구가 필요하다.

ABSTRACT

As research on IT convergence continues, the scope of IoT (Internet of Things) services continues to expand. The IoT service uses a device suitable for the purpose. These IoT devices require an authentication function. In addition, in IoT services that handle important information such as personal information, security of transmission data is required. In this study, we implement a crypto key-based IoT network security system that can authenticate devices for IoT services and securely transmit data between devices. Through this study, IoT service can authenticate the device itself and maintain the confidentiality of transmitted data. However, since it is an IoT service, additional research on the application efficiency of the encryption algorithm is required.

키워드

IoT, IT Convergence, Authentication, Secure Network, Cryptography

Ⅰ. 서 론

IT 융합 연구가 계속되면서 IoT 서비스는 스마트 팜이나 스마트 에너지나 스마트 해양 등의 다양한 분야로 확장되고 있다. 보통 IoT 서비스는 CS구조로 제공되고 있다. 다양한 IoT 단말과 연동하는 구조이다. 이러한 상황에서 IoT 단말이 인가되지 않은 상태에서 서버에 접속하여 비정상적인 데이터를 전달할 수 있다. 또 IoT 단말에서 생성한 정보를 서버에 전달할 때, 전달되는 과정에서 중요 정보가 외부에 노출될 수 있는 문제점이 있다.

본 연구에서는 이러한 문제점을 개선하기 위하여 IoT 서버와 연동하는 단말을 인증하고, 인증된 단말이 전송하는 데이터에 대해 기밀성을 유지할 수 있는 암호키 기반 IoT 네트워크 보안 시스템을 제안하고 이를 구현하고자 한다. 제안하는 암호키 기반 IoT 네트워크 보안 시스템을 사용한다면, 많은 IoT 서비스에서 단말 인증뿐만 아니라 안전한 데이터 전송이 가능해질 것이다.

* corresponding author

II. 관련 연구

1. IoT의 동향

IoT 기술의 발달로 인해 라즈베리파이나 아두이노 등 다양한 IoT 단말이 개발되고 있다[1]. 다양한 IoT 서비스에서는 이 단말을 사용하여 IoT 서비스를 구축한다. IoT 단말은 정보의 수집이나 상황에 따라 대응 행동을 한다. IoT 단말에서 수집한 정보는 서버로 전달된다. 보통 유선이나 무선 네트워크를 사용하여 서버로 전달되며, 서버는 전달받은 정보를 저장하거나 분석하여 대응 행동을 결정한다.

2. IoT 보안 이슈

원격지에 위치한 IoT 단말은 물리적으로 취약하다. 이러한 상황에서 IoT 단말은 쉽게 위변조 될 수 있다. IoT 단말 위변조로 잘못된 정보가 IoT 서버로 전달될 수 있다. 이 경우, IoT 서비스는 잘못된 결정을 하여 오동작을 할 수 있다[2].

또 IoT 단말은 네트워크를 통하여 수집한 정보를 서버에 전달한다. 그러나 이 과정에서 수집한 정보가 개인정보 등의 중요 정보일 때에는 네트워크에서 악의적 공격자에게 노출될 수 있다[3].

그러므로 IoT 서비스에 대해서는 단말을 인증하고, 암호 기능을 탑재한 네트워크 데이터 전송 기능이 필요하다.

III. IoT 네트워크 보안 시스템

본 연구에서는 IoT 서비스에서 발생하는 단말 인증 및 네트워크에서 전송 데이터의 노출 문제점을 해결하기 위한 암호키 기반 IoT 네트워크 보안 시스템을 제안하고 이를 구연한다.

본 연구에서 제안하는 암호키 기반 IoT 네트워크 보안 시스템의 구조는 그림 1과 같다.

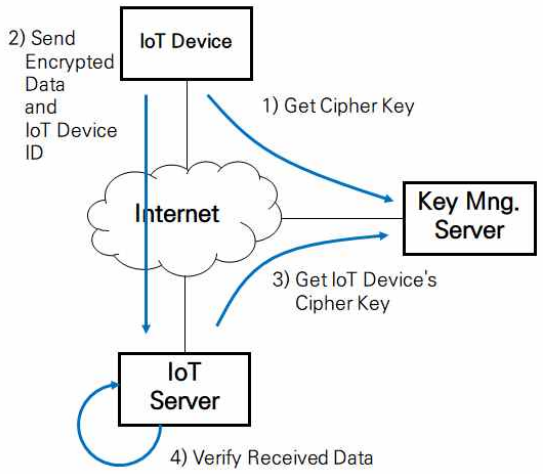

그림 1. 암호키 기반 IoT 네트워크 보안 시스템 구조

본 연구에서 제안하는 시스템은 3개의 컴포넌트로 구성되어 있다. 먼저 IoT Device는 IoT 서비스를 위한 정보의 수집이나 결정된 대응행동을 실행하는 단말이다. Key Mng. Server는 키관리 서버로 IoT 단말에 대한 암호키가 저장되어 있다. IoT 서버는 IoT Device가 전달한 정보를 수신하고 저장하거나 분석한다.

IoT Device는 동작을 시작하면 Key Mng. Server에 접속하여 단말에 대한 암호키를 수신한다. 암호키를 수신하는 과정에서 단말 ID 등의 식별자를 전달한다. 만약 등록되지 않은 단말 ID가 암호키를 요청할 때는 암호키를 전달하지 않는다. IoT Device는 암호키를 수신하면 이를 사용하여 수집/생성한 전송 데이터를 암호화한 다음 서버에 전달한다. 서버는 이를 수신한 다음 검증을 한다. 수신 데이터는 단말 ID에 대한 암호키를 Key Mng. Server로부터 확인하여 복호화된다. 만약 복호화되지 않으면 인가되지 않은 IoT Device가 전달한 것이므로 이를 폐기한다.

IV. 결 론

IoT 서비스는 헬스케어나 환경, 해양, 에너지 분야 등으로 확대될 것이다. 이러한 환경에서 IoT 단말은 매우 중요한 역할을 할 것이며 네트워크 구간에서 전송 데이터의 보호도 강조될 것이다.

본 연구에서는 IoT 서비스에서 요구되는 단말 인증 및 전송데이터의 기밀성을 만족할 수 있는 시스템을 제안하였다.

다만 암호 기능을 사용하는 만큼 무선 환경의 단말의 과도한 전력 소모가 발생할 수 있다. 그러므로 이에 대한 추가 연구가 필요하다.

Acknowledgement

본 연구는 과학기술정보통신부 및 정보통신기획평가원의 SW중심대학지원 사업의 연구결과로 수행되었음(2018-0-018740301001).

References

[1] Kim, D. H., Yun, S. U. and Lee, Y. P., “IoT 서비스를 위한 보안”, Information and Communications Magazine, vol.30, no.8, pp.53-59, 2013.

[2] Pyo, C. S., Gang, H. Y., Kim, N. S. and Bang, H. C., “IoT (M2M) 기술 동향 및 발전 전망”, Information and Communications Magazine, vol.30, no.8, pp.3-10, 2013.

[3] Kim, S. J. and Cho, D. E., “Technology Trends for IOT Security”, Review of Korea Contents Association, vol.13, no.1, pp.31-35, 2015.