IoT 단말 인증 시스템 구현

강동연* · 전지수 · 한성화

동명대학교

Implement IoT device Authentication System

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

TongMyong University

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

요 약

스마트 팜이나 스마트 해양, 스마트 홈, 스마트 에너지 등 많은 분야에서 IoT 기술을 사용하고 있다. 이러한 IoT 서비스에는 다양한 IoT 단말이 이용된다. 여기서 IoT 단말은 물리적으로 다양한 장소에 설치된다. 악의적 공격자는 인가되지 않은 IoT device를 사용하여 IoT 서비스 접근하여, 인가되지 않은 중요 정보에 접근 후 이를 변조할 수 있다. 본 연구에서는 이러한 문제점을 개선하기 위하여 IoT 서비스에서 사용하는 IoT device의 단말 인증 시스템을 제안한다. 본 연구에서 제안하는 IoT device 인증 시스템은 IoT device에 탑재된 인증 모듈과 IoT 서버의 인증 모듈로 구성된다. 본 연구에서 제안하는 IoT device 인증 기능을 사용하면, 인가된 IoT Device만 서비스에 접근할 수 있으며 인가되지 않은 IoT device의 접근을 차단할 수 있다. 본 연구는 기본적인 IoT device 인증 메커니즘만을 제안하므로, 보안 강도에 따른 추가적인 IoT device 인증 기능의 추가 연구가 필요하다.

ABSTRACT

ogy is being used in many fields, such as smart farms, smart oceans, smart homes, and smart energy. Various IoT terminals are used for these IoT services. Here, IoT devices are physically installed in various places. A malicious attacker can access the IoT service using an unauthorized IoT device, access unauthorized important information, and then modify it. In this study, to solve these problems, we propose an authentication system for IoT devices used in IoT services. The IoT device authentication system proposed in this study consists of an authentication module mounted on the IoT device and an authentication module of the IoT server. If the IoT device authentication system proposed in this study is used, only authorized IoT devices can access the service and access of unauthorized IoT devices can be denied. Since this study proposes only the basic IoT device authentication mechanism, additional research on additional IoT device authentication functions according to the security strength is required.IoT technol

키워드

IoT, Authentication, Arduino, Raspberry Pi

Ⅰ. 서 론

스마트 팜이나 스마트 해양, 스마트 홈, 스마트 에너지 등 많은 분야에서 IoT 기술을 사용하고 있다. 이러한 IoT 서비스에는 다양한 IoT 단말이 이용된다. 여기서 IoT 단말은 물리적으로 다양한 장소에 설치된다. 악의적 공격자는 인가되지 않은 IoT device를 사용하여 IoT 서비스 접근하여, 인가되지 않은 중요 정보에 접근 후 이를 변조할 수 있다. 그러므로 본 연구에서 진행하는 방법과 같이 보안성을 강화할 수 있는 인증 시스템이 필요하다.

* speaker

II. 관련 연구

1. IoT의 동향

IoT 기술의 발달로 구글과 애플과 같은 대형 업체에서도 스마트홈, 스마트팜, 스마트에너지에 이용하기 위해 운영체제를 기반으로 만든 '위브', '네스트', '홈 킷'을 중심으로 각종 기기를 결합한 IoT 사업을 구축해 나가고 있다[1].

2. IoT 보안 이슈

여러 분야에서 편리하게 사용되는 IoT 기술들은 그만큼 우리 일상에 들어와 있으므로 여러 가지 해킹에 대한 위험이 있다[2]. 2021년 아파트에 설치된 월패드(Wall-pad)를 해킹하여 불법으로 촬영한 영상을 판매 및 협박하는 사례가 있다[3]. 네트워크 접속 요청 시 서버에 등록되어있는 MAC 주소와 장비로부터 요청받은 메시지와 함께 전송된 MAC 주소를 비교해 인증하는 절차를 가진다. 하지만, MAC 주소는 위조할 수 있어 MAC 기반 인증만으로는 공격에 취약하다[4].

III. 인증 메커니즘

본 연구에서는 IoT 장치 인증 문제를 해결하기 위해 그림 1과 같은 장치 인증을 위한 OTP 기반과 MAC 기반의 인증을 병합한 인증 모델을 제안한다.

그림 1. 인증 흐름도

제안한 OTP 및 MAC 기반 IoT 인증 메커니즘의 흐름은 그림 1과 같다.

우선 서버에 장비가 연결되어있고 장비의 고유번호들이 저장되어 있다고 가정한다. 서버에서 IoT 장비에 대한 인증을 요청하고 이에 장비는 자신의 MAC 주소를 전달하고 서버에서 받은 MAC 주소를 통해 해당 장비의 고유번호를 알아내고 OTP를 생성한다. 그리고 서버는 장비에게 OTP를 요구한다. 이에 장비는 OTP를 생성하고 서버에게 전송한다. 서버는 전송받은 OTP를 서버에서 생성한 OTP와 대조하여 일치할 경우, 연결을 유지하고 그렇지 않으면 연결을 해제시킨다.

IV. 결 론

최근 통신 서비스의 다양화와 전자 기기들의 보급이 가속화됨에 따라 개인, 사회기반시설, 기업체에 접목되어서 자동화, 시설관리 및 모니터링과 같은 서비스를 제공한다. 하지만 앞서 언급했던 것과 같이 IoT 기기에 악성코드를 심어 감염시킨 뒤 그것을 이용하여 DDoS 공격을 하는 사례를 볼 수 있다. 그러므로 위와 같은 보안 이슈를 보완하기 위해서는 강한 IoT 인증 시스템이 필요하다.

MAC 기반으로만 인증 시스템을 구축하면 MAC 주소가 위조될 수 있어 하나만으로는 보안성이 취약해진다. 따라서 본 연구에서는 이 취약점을 보완하기 위해 OTP 인증 시스템을 추가하였다. 이는 MAC 주소가 위조 당할 때도 OTP를 통한 2차 인증이 존재하므로 보안성을 더욱 강화할 수 있다.

Acknowledgement

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

References

[1] Tae-Sik Son and Jong-Bin Ko, "Internet of Things (IOT) Security Trends in Cloud Computing", Journal of Information Security, Vol. 22, No. 2, 2, 2012.

[2] Byeong-Joo Park, Tae-Jin Lee, and Jin Kwak. "Blockchain-based IoT Device Authentication Scheme." Journal of Information Security Society, 2017.

[3] In-depth report, "Internet of Things Security Threat Trend", Internet & Security Bimonthly, vol 5, 2014

[4] Si-Jung Kim and Do-Eun Jo, "IOT (Internet of Things) Technology Trends for IOT Security", Korea Contents Association Vol. 13 No. 1