사물인터넷 환경에서의 강화된 보안 아키텍처에 대한 연구

이종원, 김기천*

*건국대학교

Study on Enhancing Security Architecture in Internet of Things Environment

Jong-won Lee, Keecheon Kim*

*Konkuk University

E-mail : ljw4874@konkuk.ac.kr, kckim@konkuk.ac.kr*

요 약

사물인터넷은 우리 주변의 모든 것들을 네트워크로 연결시켜주고 언제 어디서나 쉽게 접할 수 있게 해준다. 사물인터넷은 다양한 스마트기기, 무선 센서 등 여러 단말기들을 네트워크에 연결하여 사용하는데, 각 단말간의 통신 중에 명령이나 결과에 대한 어떤 사소한 정보라도 외부에 노출이 되었을 경우 심각한 위험을 도래할 수 있다. 사물인터넷은 하드웨어적으로 제한된 성능을 가지고 있어 보안성에서도 일반 네트워크보다 훨씬 취약하다는 특성을 가지고 있다. 본 논문에서는 이러한 사물인터넷 하드웨어적 제한을 고려하여 강화된 사물인터넷 보안 아키텍처에 대하여 제안하고자 한다.

ABSTRACT

The Internet of Things allows you to connect everything around you to your network and make it easy to reach anytime, anywhere. The Internet of Things uses various devices such as smart devices and wireless sensors connected to the network. When any small information about command or result is exposed to the outside during communication between each terminal, there is a serious risk. The Internet has a characteristic that it is much weaker than general network in terms of security because it has limited hardware performance. In this paper, I propose an enhanced security architecture of Internet of Things considering the limitation of hardware.

키워드

사물인터넷, 보안, 제한된 환경, IPS, IDS, 사물인터넷 보안 아키텍처

Ⅰ. 서 론

사물인터넷은 4차 산업혁명에서 대두되고 있는 기술 중 하나로 각종 사물에 센서와 통신기능을 내장하여 인터넷에 연결하고 그 정보를 활용하여 사물 본연의 기능을 더 충실히 행하도록 하는 기술을 말한다. 우리가 흔히 접할 수 있는 웨어러블 기기부터 자동차, 공장, 헬스 케어 등 활용 가능한 적용 사례가 매우 광범위 하여 각광 받고 있다.

사물인터넷의 활용은 증가 하고 있지만 그에 대한 보안은 많이 부족한 실정이다. 고도의 보안 솔루션을 도입하기 어렵고 외부에서 해킹 사실을 확인할 수 없으며 복잡한 네트워크 구조로 침투 경로가 다양하다는 점 때문에 보안 위협이 대두되고 있다.[2] 특히 센서나 임베디드 기기와 통신하여 서비스를 제공하는 만큼 하드웨어적 한계

표 1. 사물인터넷을 활용한 분야별 응용사례[1]

구분	분야	사례
개인 IOT	자동차	커넥티드카
	헬스케어	스마트밴드
	생활가전	스마트가전
산업 IOT	농업	스마트팜
	공장	스마트공장
공공 IOT	환경	스마트크린
	에너지	스마트미터

때문에 보안 서비스를 도입하기 어렵고 도입 하더라도 기존의 성능보다 저하되는 경우가 많다. 때문에 단순한 패킷 수집만 하더라도 쉽게 정보를 탈취할 수 있어 각종 보안 취약성은 물론 사물인터넷 서비스에서 실시간으로 수집되는 사용자 데이터는 사생활 침해 문제 또한 유발 가능하다.

이에 본 논문에서는 IPS(Intrusion Prevention System), IDS(Intrusion Detection System)와 단순한 암호화를 이용하여 이러한 사물인터넷 환경에서도 효과적으로 보안을 할 수 있는 방안을 제안하고자 한다.

Ⅱ. 관련 연구

사물인터넷은 모든 사물을 인터넷에 연결하고 그 정보를 활용하는 것인데 그 말은 모든 사물이 해킹 대상이 될 수 있음을 의미한다. 보통 편의를 위해 모두 무선 인터넷 환경에서 사용되므로 그 정보를 가로채기가 매우 쉽다. 이를 막고자 메시지를 암호화 하거나 암호화 프로토콜을 이용하는데 주로 사용되는 기술은 다음과 같다.

1. CoAP (Constrained Application Protocol)

CoAP의 같은 경우 저전력, 저용량, 소형 센서나 임베디드 기기같이 사물인터넷처럼 제한적인 환경에서 사용될 수 있는 웹 전송 프로토콜이다. UDP 기반에 신뢰성을 위해 재전송과 타이머 관리 기능을 옵션으로 가지며, 보안적 요소를 위해 DTLS(Datagram Transport Layer Security)를 사용할 수 있다. CoAP의 보안모드는 4가지로 분류되는데 기본 방식인 NoSec 모드를 제외한 3가지 모드의 경우는 DTLS가 적용되어 강력한 보안성이 제공된다.[3]

2. MQTT (Message Queue Telemetry Transport)

MQTT는 제한된 네트워크에서 비동기 통신을 가능하게 해주는 경량 메세징 프로토콜이다. Publish/subscribe 모델을 사용하며, 브로커가 네트워크 노드간에 메시지를 관리하고 라우팅한다. TCP를 사용하여 높은 신뢰성을 특징으로 하는데 기존의 TCP와는 달리 암호화 되지 않은 상태로 사용된다.[4] 이와 같은 특성 때문에 패킷 페이로드 암호화가 추가적으로 필요하다.

3. 암호화

암호화는 평문으로 전송되는 데이터를 암호화 알고리즘을 이용하여 알아볼 수 없는 상태로 데이터를 전송하고 사전에 협의된 방법으로만 복호화 하여 해당 데이터를 읽을 수 있도록 하는 방법이다. 해당 장의 1절 과 2절 같은 경우 사물인터넷의 하드웨어 성능이 충분치 못할 경우 평문으로 전송될 수 있는데 이와 같은 경우에 개인정보가 유출되거나 조작되기 쉬우므로 암호화를 사용한다. 하지만 암호화 알고리즘을 사용하는 데에도 하드웨어 성능이 좋지 않으면 사물인터넷이 제 성능을 발휘하지 못할 수 있다. 이런 경우 연산 과정을 줄이고 별도의 알고리즘을 도입하여 경량 암호화 알고리즘을 사용할 수 있는데 이에 대해서는 다양한 연구가 진행되고 있다.

Ⅲ. 강화된 사물인터넷 보안 아키텍처

1. 기존 연구의 제한점

기존의 사물인터넷 보안에 대하여 다양한 표준 암호화 프로토콜이나 가이드라인, 공통 보안 원칙 등이 제시되고 있고, 그에 대하여 다양한 연구가 진행되고 있다. 하지만 사물인터넷 환경에서는 하드웨어 성능이 매우 제한적이기 때문에 이에 대한 고려도 이루어 져야한다. 사물인터넷 표준 프로토콜인 CoAP의 경우 제한된 환경에서는 NoSec 모드를 제외한 모드는 사용하기 어렵고 NoSec 모드의 경우는 보안적인 기능을 제공하지 않으며[3], MQTT의 경우는 패킷 페이로드 암호화를 추가로 해주지 못 할 경우에는 패킷이 평문 형태로 전송되어 보안 성능이 취약하다. 이와 같이 기존에 제시되어있는 많은 보안 해결책이 제한된 환경에서는 제 성능을 발휘하지 못하여 사물인터넷 환경이 보안에 매우 취약한 상태가 된다.

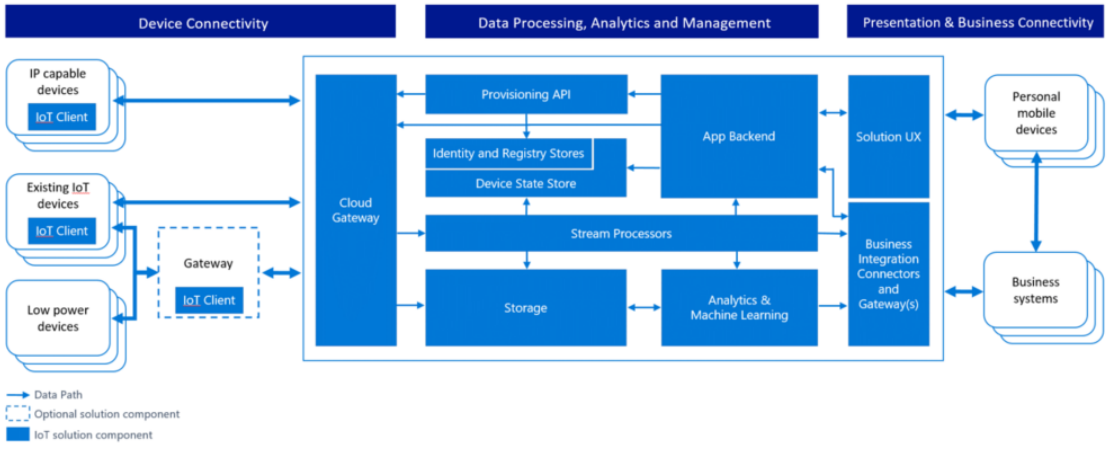

그림 1. IoT Archetecture[5]

2. IPS(Intrusion Prevention System) & IDS(Intrusion Detection System)를 활용한 강화된 사물인터넷 보안 아키텍처 제안

본 논문에서는 경량화 및 모듈화 된 IPS, IDS를 게이트웨이에 탑재하여 저전력 디바이스같이 하드웨어의 성능이 떨어져 네트워크 서버와 통신하기 위해 추가로 게이트웨이가 필요한 디바이스에 적합한 보안 아키텍처를 제안한다. 제안하는 보안 아키텍처는 <그림2>와 같다.

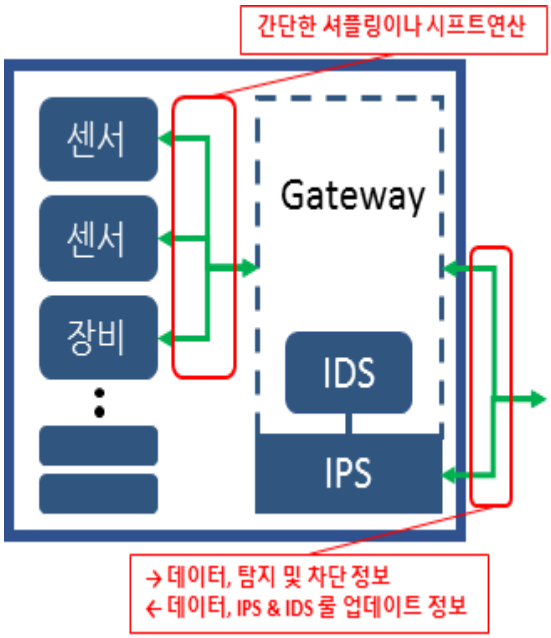

그림 2. Enhanced IoT Security Archetecture

IDS와 IPS를 경량화 및 모듈화 하여 게이트웨이에 탑재하고 네트워크 서버로부터 규칙에 대한 정보를 업데이트 받으며 디바이스와 게이트웨이 사이에 비정상적인 트래픽이나 데이터 변조와 같이 외부로부터 접근이 있을 경우 이를 탐지하고 차단하도록 하여 취약점을 보완한다. 경량화 된 IPS, IDS 모듈이므로 침입 탐지에 반응이 느릴 수 있으므로 바로 정상적인 데이터 형태를 판별할 수는 없지만 제한적인 성능의 장비나 센서도 연산할 수 있도록 간단한 셔플링이나 시프트 연산을 통해 경량화 된 IPS, IDS 모듈의 성능을 보완하고 침입이 탐지 되었을 시 네트워크 서버로부터 새로 적용된 룰 정보를 업데이트 받아 공격을 차단한다.

Ⅳ. 결 론

기존의 사물인터넷 보안 아키텍처의 경우 센서나 저전력 장비 등 제한된 환경에서의 사물인터넷에 대한 보안이 고려되지 않아 주고받는 데이터의 정보가 그대로 드러나는 정도로 보안이 취약했다.

본 논문에서는 하드웨어의 한계를 고려하여 Gateway에 경량화 된 IPS, IDS를 모듈화 하여 탑재하고 경량화 된 IPS, IDS의 성능 또한 고려하여 방지책을 세워 강화된 사물인터넷 보안 아키텍처를 연구, 제안하였다. 추후 강화된 사물인터넷 보안 아키텍처를 세분화하여 설계하고 구현하여 성능을 검증하고자 한다.

ACKNOWLEDGMENT

이 논문은 2017년도 정부(미래창조과학부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임 (No.2017-0-00279,안전한 IoT 전용망 구축을 위한 LPWAN 침해 방지 기술 개발)

참고문헌

[1]KDB 산업은행 - 이정민, 사물인터넷의 국내외 주요 적용사례 분석과 시사점 69P
[2]한국 인터넷 진흥원 - 심층분석 사물인터넷 보안 위협 11P (2014)
[3] RFC 7252 - Z. Shelby, K. Hartke, C. Bormann, The Constrained Application Protocol (CoAP) (2014)
[4] OASIS Standard - Andrew Banks, Rahul Gupta, MQTT Version 3.1.1 (2014)
[5] Microsoft Azure - Yuri Diogenes, Dominic Betts, Internet of Things Security architecture (2017)