**IoT 하드웨어 보안 모듈을 이용한 secure FOTA 시스템 구축**김선우 박형모 이호재 조민제  
동국대학교 컴퓨터공학부  
swkim@dongguk.edu, gudah1478@dongguk.edu, yslhj93@gmail.com, mnc14231423@hotmail.com   
**Designing Secure FOTA System with IoT Hardware Security Module**Sunwoo Kim Hyungmo Park Hojae Lee Minjae Cho  
  
**요 약**

**1. 서 론**

Internet of things (IoT)가 천천히 세계에 자리를 잡고 있다. 전문가들은 2025년까지 연결된 기계/장치가 1~3조까지 성장할 것을 예측하고 있다. IoT는 컴퓨팅 시스템 및 감지, 작동 기능이 편리함과 경제적 이익을 제공하는 미래 인터넷 비전을 소개한다.

IoT 기술이 상용화되고 발전하기 위해서는 몇가지 문제를 해결해야 한다. IoT는 다른 컴퓨팅 기계와 달리 하드웨어 적으로 성능이 낮다. 그러므로 지속적인 보안 강화와 펌웨어 업데이트를 통해서 보안을 유지를 해야한다. 본 논문에서 이용할 기술은 FOTA(Firmware over the air)이며 이 기술을 통해서 펌웨어 업데이트를 실행할 것이다. FOTA는 현재 휴대폰, 태블릿 등 인터넷에 연결된 디바이스에 이미 자리를 잡고 있다. 이처럼 연결되는 디바이스의 수가 늘어나고 있으며, 꾸준한 업데이트, 보안 강화가 이루어져야 할 필요성이 증가하고 있다. 하지만 FOTA에서 보안에 관한 표준이 아직 자리를 잡고 있지 못하며, 확실한 기준이 존재하지 않는다. 인터넷에 연결된 디바이스가 업데이트 도중, Hijacking의 위협은 존재하며 안전한 통신을 하기 위한 방안이 있어야 한다.

본 논문에서 소개할 내용은 IoT 하드웨어 보안 모듈을 이용한 FOTA이다. IoT는 Raspberry pi와 Cloud server를 이용하여 업데이트를 하게 될 것이다. 암호화, 펌웨어 위변조 방지 등의 기능을 수행하며 펌웨어 업데이트 또한 안정적으로 이루어질 수 있게 만들어 준다.

**2. 관련 연구**

Firmware Over The Air 기술에 대한 Generic Architecture 및 Implementation이 Hesham A. Odat et al.[1]에 의해 제시되었다. 이 논문에 따르면 FOTA 시스템은 다음 4가지로 구성된다.   
a) 업데이트 할 모든 Software들을 하나의 Package로 만들고, 1개 이상의 Vehicle에 각각의 Package를 보내는 “Integrator”,

b) User와 Vehicle의 식별자를 저장하고 Target vehicle과 현재 SW version을 시스템에게 알려주는 “Inventory Database”,

c) Integrator가 보내는 Package를 받고, Inventory Database에 저장된 정보로 Target vehicle에 Target Package를 보내는 “Server”

d) Server가 보내는 Package를 받고 Un-packaging, Installation, Backup, reboot ECU, and ECU initialization을 하는 “Client”.

Krishna Doddapaneni et al.[2]가 Secure Firmware Over The Air에 대한 Architecture를 제안했다. 순서는 다음과 같다.

a) Client가 FOTA image의 download request를 한다.

b) Server가 FOTA image를 정해진 Payload 단위로 자르고, 각각의 Payload에 대한 hash, src/dst address, image size등을 모아 하나의 Object로 만든 뒤 Client에게 전송한다.

c) Client가 정상적으로 파일을 받았으면, acknowledgement를 Server로 보낸다.

d) Server가 마지막으로 보낸 ack를 추적해서, connection이 끊어지면 마지막으로 성공한 ack부터 다시 시작한다.

**3장 시스템 구성**

**3.1 시스템 정의**

Secure FOTA 시스템은 Wi-Fi와 같은 무선 네트워크를 이용해 cloud server와 연결하여 차량의 ECU Firmware를 업데이트를 수행하도록 한다. 여기서 Cloud server는 차량 제조사가 upload한 update SW를 segmentation 하고 순차적으로 차량에게 전송하는 역할을 수행한다. 그리고 차량의 ECU는 Wi-Fi를 이용해 Cloud server가 전송하는 segmentation file들을 다운로드한 후, 통합하여 update를 진행한다.

**그림 1**는 Secure FOTA 시스템의 구성을 도식화한 것이고 **그림 2**는 흐름표이다.

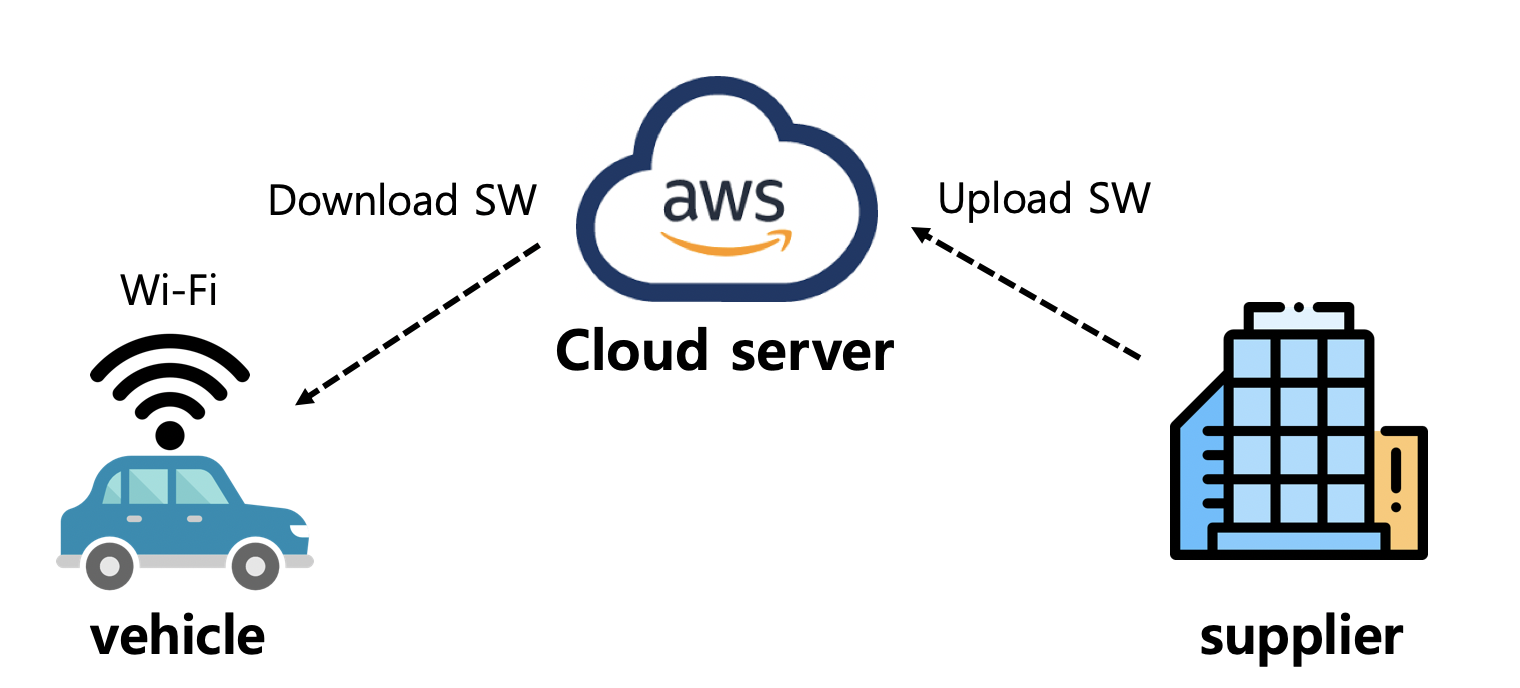


그림 1. Secure FOTA 시스템 구성도

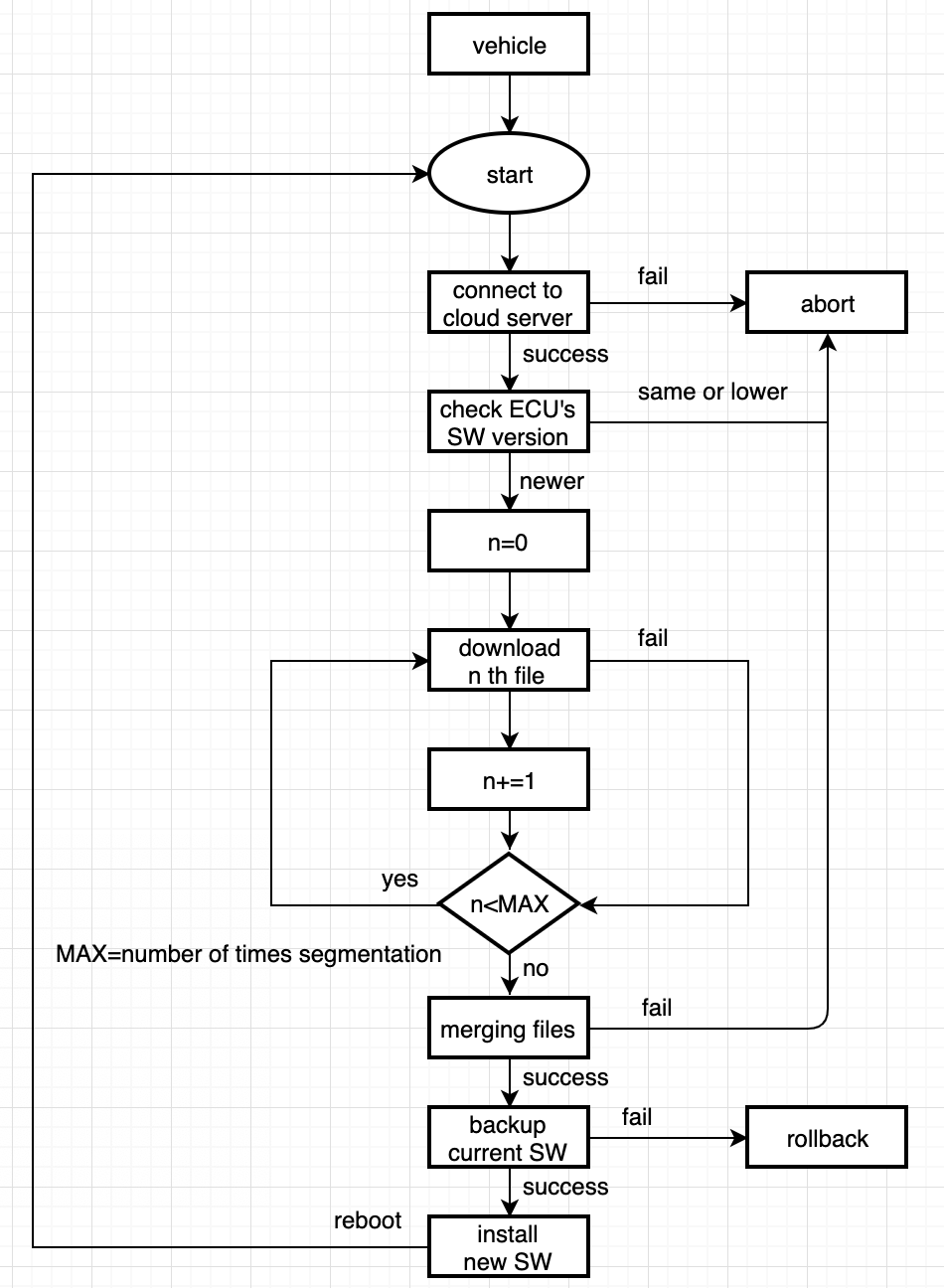


그림 2. Secure FOTA 흐름표

**3.2 개발 환경**

- Raspberry Pi

차량의 ECU 역할을 수행하며 OS는 Raspbian을 사용한다.

**-AWS**

Amazon 사에서 제공하는 클라우드 컴퓨팅 서비스로서, 본 논문에서는 main server를 AWS에서 구축할 것이다. OS는 ubuntu를 사용한다.

**-Linux**

대표적인 오픈 소스 C 프로그래밍 운영체제이다. ECU에서 사용하는 Raspbian과 서버에서 사용하는 Ubuntu 모두 Linux 기반 운영체제이다.

**-C++**

절차지향 프로그래밍 언어인 C언어에 객체지향 프로그래밍을 지원하기 위해 만들어졌다. ECU에서 구동할 Client program 구현 시 사용할 것이다.

**-Apache**

Web server의 한 종류로써, 본 논문에서는 Apache를 이용해서 제조사가 update SW를 upload하고 client program이 download 할 수 있는 main server를 구현할 것이다.

**4장 구현 및 실험**

**5장 결론**

**참고 문헌**

[1] : Hesham A. Odat and Subra Ganesan, “Firmware Over the Air for Automotive, FOTAMOTIVE”, in 978-1-4799-4774-4/14/$31.00 ©2014 IEEE

[2] : Krishna Doddapaneni∗, Ravi Lakkundi†, Suhas Rao†, Sujay Gururaj Kulkarni†, Bhargav Bhat†, “Secure FoTA object for IoT”, in 2017 IEEE 42nd Conference on Local Computer Networks Workshops