INTISARI

Implementasi pembaruan perangkat lunak melalui OTA (*Over-the-Air*) merupakan aspek yang penting dalam sebuah sistem *Internet of Things* (IoT). Fungsionalitas ini akan digunakan untuk memberikan dukungan kepada sistem perangkat pengguna secara jarak jauh melalui sebuah awan atau *cloud.* Pada suatu sistem *Internet of Things* akan memiliki berbagai macam *end-node* yang memiliki fungsi dan *firmware* masing-masing. Sistem pembaruan *firmware* ini harus dapat mecangkup volume perangkat yang besar dan perangkat akan menerima *firmware* yang sesuai dengan fungsi masing-masing perangkat. Dengan adanya komunikasi nirkabel, keamanan menjadi suatu aspek penting dalam sistem *Internet of Things* ini. Komunikasi antara *cloud* dengan perangkat harus terenkripsi dan apabila tidak, maka seluruh sistem *Internet of Things* akan terkompromi karena pada setiap perangkat akan rentan untuk diretas pihak ketiga.

Penelitian ini bertujuan untuk merancang sistem pembaruan *firmware* melalui *Over-the-Air* berbasis ESP8266 menggunakan sistem operasi Mongoose OS yang bersifat aman. Sistem pembaruan dirancang dapat menggunakan layanan *cloud* berbayar Amazon AWS IoT Platform maupun *cloud* pribadi. Komunikasi antara server dan perangkat akan menggunakan protokol MQTT di mana perangkat akan dikelompokkan pada topik MQTT yang sesuai dengan *firmware* masing-masing.

Hasil penelitian berupa sistem pembaruan *firmware* melalui OTA yang dapat memperbarui suatu grup perangkat yang memiliki *firmware* yang sama. ESP8266 akan diamankan menggunakan *crypto-chip* ATECC508a untuk mengenkripsi *private key* yang digunakan pada MQTT dan tidak akan bisa diakses pada *filesystem*. Sistem ini akan dikemas dalam satu kit prototipe yang memudahkan penggunaan sistem operasi Mongoose OS beserta implementasi pembaruan *firmware* melalui OTA yang bersifat aman ke kit prototipe ini.

Kata Kunci: *Internet of Things* (IoT), *Secure Firmware update Over-the-air* (FOTA), ESP8266, *crypto-chip ATECC508a, Kit Prototipe.*

ABSTRACT

Implementation of OTA (Over-the-Air) firmware update is an important aspect in an Internet of Things (IoT) system. This functionality will be used to provide support to the user's system remotely via a server cloud. An Internet of Things system will have various end-nodes that have their respective functions and firmware. This firmware update system must be able to cover a large device volume and the device must receive the firmware that matches the functions of each device. With wireless communication, security became an important aspect of this Internet of Things system. Communication between the cloud and the device must be encrypted and if not, the entire Internet of Things system will be compromised because every device will be vulnerable to hackers.

This research aims to design a secure firmware update Over-the-Air system based on ESP8266 using the operating system Mongoose OS. This system is designed to on paid cloud services Amazon AWS IoT Platform as well as private cloud. Communication between the server and the device will use the MQTT protocol where the devices will be grouped on MQTT topics that correspond to their respective firmware.

The results of the research are an OTA firmware update system that can update a group of devices that runs on the same firmware. ESP8266 will be secured using the ATECC508a crypto-chip to encrypt the private key used on communicating with MQTT and thus this private key will not be accessible on the filesystem. This system will be packaged in a prototype kit provides a fluent introduction to Mongoose OS operating system along with implementing the secure OTA firmware update system to this prototype kit.

Keywords: *Internet of Things (IoT), Over-the-air (FOTA) Secure Firmware update, ESP8266, ATECC508a crypto-chip, Kit Prototype.*