Bab I
PENDAHULUAN

1.1 Latar Belakang

IOT(Internet of Things) adalah sebuah teknologi yang memanfaatkan kemampuan suatu mesin untuk berkomunikasi dengan mesin lainya. IOT terbentuk dari sejumlah perangkat yang saling terhubung dan bekerja bersama-sama untuk mencapai suatu tujuan. Tidak hanya IOT menghubungkan berbagai macam perangkat, tetapi setiap perangkat tersebut dapat mengerjakan tugasnya masing-masing secara mandiri. Sebagai contoh sebuah kendaraan seperti mobil dapat memiliki 40-60 perangkat di dalam jaringan internalnya [1]. Perangkat tersebut dapat terdiri dari sensor, kontroller / mikro-kontroller dan aktuator. Hal ini membuat pembaharuan firmware saat sistem bekerja menjadi semakin populer dan umum digunakan di industri.

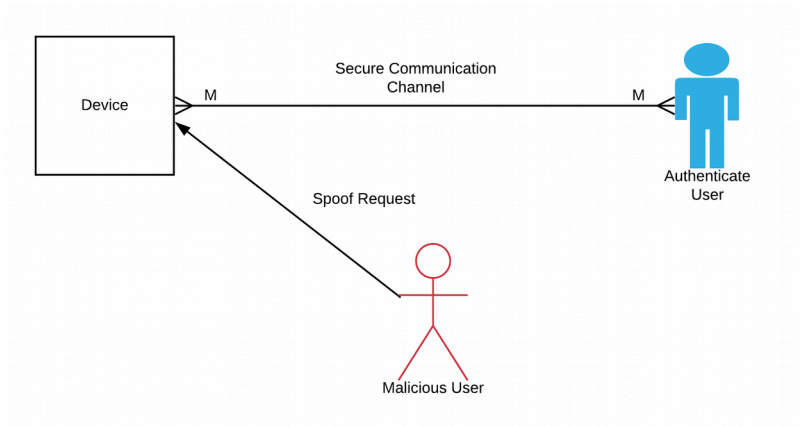
FOTA(Firmware Over The Air) update adalah sebuah metode untuk memperbaharui perangkat-lunak sebuah sistem melalui internet dan dilakukan ketika sistem sedang berjalan. FOTA update membuat perangkat-lunak sebuah perangkat dapat di perbaharui tanpa harus membawa perangkat tersebut ke pusat / tempat perangkat itu dibuat / diperbaiki. Pembaharuan perangkat-lunak dapat bertujuan untuk memperbaiki bug atau menambah fitur baru. Metode ini semakin populer di industri karena dengan FOTA update perusahaan dapat mendistribusikan perangkat lunak mereka secara efektif ke perangkat-perangkat IOT. Hal ini tentu membuat *cost* yang dikeluarkan sebuah perusahaan untuk me-*maintain* perangkat IOT mereka semakin efisien. Dengan meningkatnya penggunaan FOTA update, isu keamanan pada metode tersebut juga semakin meningkat. Salah satu isu keamanan yang penting dalam FOTA update adalah kondisi dimana setiap pihak (perangkat IOT , server , client) yang terlibat dapat proses tersebut dapat saling memverifikasi bahwa mereka berkomunikasi dengan pihak yang benar dan tepat. Ketika perangkat tidak dapat menidentifikasi dan memverifikasi komunikasinya maka agen-agen yang tidak berwenang dapat

berkomunikasi dengan perangkat tersebut dan memberikan pembaharuan perangkat-lunak yang salah / memiliki intensi tidak baik ataupun dapat terjadi kebocoran data. Hal ini dapat membuat kegagalan sistem. Saat melakukan komunikasi, kanal komunikasi perangkat dapat diamankan dengan protokal keamanan yang sudah ada sekarang ini tetapi perangkat itu sendiri belum tentu dapat mengenali dengan siapa dia berkomunikasi. Saat ini ada beberapa metode yang digunakan untuk mengamankan FOTA update. Pada bagian transmisi data, AES dapat digunakan untuk mengenkripsi data. Saat pada kanal komunikasi informaasi yang di transmisikan dapat diamankan menggunakan TLS ataupun IPSec. Doddapaneni mengajukan sebuah standard untuk *secure FOTA object* [2]. Objek ini memiliki sebuah mekanisme *signing* untuk mengecek dan memverifikasi integritas dari data tersebut. Chandra menggunakan *light-weight network* dengan *peer-to-peer connection* untuk melakukan FOTA update [3]. Menurutnya, arsitektur ini meningkatkan portabilitas dan *low-power*. Arsitektur ini cocok untuk daerah *urban*. Pengamanan pada perangkat IOT perlu mempertimbangkan juga kemampuan komputasi perangkat dan kapabilitas perangkat-kerasnya.

Dalam sebuah sistem IOT, kondisi *environment* perangkat dapat berubah-ubah secara dinamis. Perubahan ini dapat dipengaruhi oleh beberapa faktor, bisa dari arsitektur sistem tersebut ataupun kebutuhan *client* yang harus di penuhi sistem. Oleh karena itu, perangkat IOT harus dapat "beradaptasi" mengikuti perubahan yang terjadi tetapi, perangkat IOT umumnya memiliki keterbatasan terutama dalam hal *storage* dan kemampuan komputasi. Menurut Kolehmainen, FOTA *update* memiliki banyak metode tetapi tidak ada yang men-*standard*-kan cara tersebut [4]. Dari survey yang dia lakukan, banyak peneliti membuat sebuah metode untuk *secure* FOTA tetapi masih bergantung pada kondisi tertentu atau perangkat tertentu secara spesifik. Kurangnya standarisasi membuat metode-metode tersebut cenderung sulit untuk di implementasikan pada sistem yang sudah ada. Terdapat sebuah standar bernama SUIT dari IETF SUIT *working group*. Mereka mendefinisikan sebuah *security model* untuk *firmware updates*. Dalam model tersebut ketika ada *firmware update*, *firmware* tersebut akan melalui

untrusted storage. *Untrusted storage* dapat berupa server atau *removeable media* seperti flashdisk. Hal tersebut berkerja sebagai kanal yang menghubungkan *firmware vendor* ke perangkat yang akan di perbaharui. Dengan melihat dari model tersebut, komunikasi pada FOTA *update* akan selalu melalui *untrusted media.* Hal ini menunjukan dalam *firmware update* dibutuhkan *end-to-end secure communication*. Kolehmainen juga mengatakan pada *automotive network*, mobil dapat terhubungan dengan *mission-critical system*.

Dalam penelitian ini, penulis mengajukan sebuah metode untuk mengidentifikasi pengguna yang melakukan FOTA *update* agar unik dan aman. Hal tersebut membuat perangkat dapat mengautentikasi pengguna. Metode ini berguna agak perangkat tidak menerima *request* dari *client* yang tidak berwenang seperti yang di tunjukan pada gambar 1. Perangkat akan memiliki sebuah *secret key* yang digunakan untuk membuat token. Agen yang melakukan FOTA *update* membutuhkan token ini untuk melakukan pembaharuan perangkat-lunak. Algoritma yang akan digunakan adalah HMAC-SHA256. SHA256 digunakan untuk *signing secure FOTA object* dengan *secret key*. Dengan menambahkan proses keamanan tersebut, perangkat akan memiliki lebih banyak beban sehingga dapat membuat perangkat menjadi lebih lambat. Oleh karena itu, penelitian yang diajukan ini untuk memberikan metode yang dapat membuat FOTA *update* aman tetapi juga tidak memakan waktu yang terlalu lama untuk menyelesaikan proses tersebut.



Gambar 1: Ilustrasi Masalah

1.2 Rumusan Masalah

Masalah dalam penelitian ini adalah:

1. Bagaimana metode autentikasi dalam penelitian ini dapat mengautentikasi *client* yang ingin melakukan FOTA *update* ke perangkat secara tepat ?
2. Bagaimana perangkat dapat tahan dari serangan oleh pihak yang tidak terautentikasi yang ingin melakukan FOTA update ke perangkat ?

1.3 Batasan Masalah

Penelitian ini berfokuskan pada *application layer* dan mekanisme perangkat untuk autentikasi *client*. Oleh karena itu, implementasi dari kanal komunikasi yang aman tidak menjadi topik fokus dari penelitian ini. Yang dimaksudkan sebagai implementasi kanal komunikasi yang aman adalah SSL/TLS. *Attacker* juga diasumsikan tidak dapat mengakses perangkat secara fisik.

1.4 Tujuan Penelitian

Penelitian ini memiliki tujuan untuk :

1. Mengajukan sebuah metode yang dapat digunakan perangkat untuk memverifikasi pengguna.
2. Mengajukan sebuah protokol yang dapat digunakan sebuah sistem IOT untuk melakukan FOTA *update* dengan aman.

1.5 Manfaat Penelitian

Dengan penelitian ini, FOTA *update* dapat dilakukan dengan lebih aman. Perangkat dapat mengenali siapa yang akan melakukan FOTA *update* dan apakah pengguna tersebut memiliki wewenang untuk melakukan hal tersebut. Hal ini juga mencegah perangkat dimasuki *malicious code* yang dapat membahayakan sistem atau membuat sistem gagal. Penelitian ini juga memberikan peforma sebagai pertimbangan untuk mencapai proses autentikasi yang efisien dan tepat. Peforma tersebut adalah lama waktu proses autentikasi sampai pembaharuan *firmware*.