BAB I

PENDAHULUAN

1.1 Latar Belakang

Internet of Things (IoT) merupakan teknologi di industri 4.0 yang memungkinkan beberapa perangkat dapat saling berkomunikasi satu sama lain melalui internet dan protokol komunikasi tertentu. Perangkat IoT sendiri pada umumnya memiliki beberapa komponen seperti sensor, sistem *processing* data, hingga modul dan protokol untuk melakukan komunikasi. Kehadiran IoT sendiri telah membawa industri dan masyarakat menikmati otomatisasi karena sudah banyak perangkat IoT yang dirancang untuk membantu kehidupan manusia, seperti *smart home*, *smart trash bin*, *smart door*, dan lain sebagainya.

Kapabilitas perangkat IoT yang meliputi perolehan data oleh sensor, pergerakan/ *action* yang dilakukan aktuator, hingga *processing* dan pengiriman data telah membuat perangkat IoT pastinya memiliki sebuah inti atau otak yang mengatur seluruh proses dapat bekerja atau sering kita sebut sebagai *microcontroller*. Perangkat ini memerlukan *logic* untuk dapat bekerja dimana sumber *logic* tersebut berasal dari *firmware* yang di-install sehingga dapat tereksekusi oleh perangkat. Sebuah *firmware* terdiri atas kode yang berisi instruksi khusus sesuai dengan fungsi suatu perangkat IoT. Dalam pemakaian *firmware* tentunya diperlukan pembaharuan baik itu untuk menambahkan fitur atau sekedar memperbaiki *bug* dari versi sebelumnya.

Proses *uploading* sebuah *firmware* dapat dilakukan secara fisik, yakni dengan sebuah kabel data yang dapat menjembatani proses transfer. Namun, hal ini mungkin masih dapat dilakukan saat proses produksi sebelum perangkat digunakan oleh *user*. Hal ini dikarenakan apabila perangkat sudah aktif digunakan oleh *user* maka produsen harus meminta *user* untuk mengantarkan perangkat fisik untuk melakukan pembaharuan

firmware melalui kabel. Maka dari itu, solusi dari persoalan ini adalah dengan menerapkan *remote update* (*over-the-air*) terhadap perangkat IoT dimanapun mereka berada asalkan memiliki kemampuan untuk terkoneksi dengan internet.

Saat ini penerapan *remote update* sudah mulai dilakukan oleh banyak produsen perangkat IoT. Metode yang digunakan berupa pengunduhan data *firmware* ke *server* dari perangkat kemudian di *install* secara otomatis di perangkat. Konsep *centralized* dengan menggunakan *server* memiliki beberapa kekurangan seperti kerentanan terhadap serangan *man-in-the-middle* (MITM) pada sebuah komunikasi yang melalui *insecure channel* karena proses autentikasi hanya dilakukan pada *server* saja sedangkan *client* hanya akan menerima data atau *response* dari *server* sehingga meskipun ada *attacker* yang berperan sebagai pihak ketiga maka *client* akan tetap percaya pada data yang dikirim oleh *attacker*.

[1] Kekurangan dari sistem *centralized* dengan *server* adalah dapat terjadinya IP *Spoofing* yang membuat seseorang atau satu pihak melakukan manipulasi sehingga seolah-olah berperan sebagai pihak yang *valid*. Ini merupakan salah satu dasar dari terjadinya serangan *man-in-the-middle* (MITM) karena paket data yang lewat dapat diubah tanpa sepengetahuan kedua belah pihak yang akan melakukan komunikasi. Selain itu, peluang serangan lain seperti DDoS juga masih kerap terjadi pada *cloud* atau sistem berbasis *server*.

Sedangkan penerapan *blockchain* sebagai pengganti dari *server* di sistem terdistribusi membuat setiap transaksi yang terjadi akan menciptakan suatu blok baru yang berisikan data, *block hash value*, dan *previous block hash* sehingga apabila ada data yang diubah maka akan menghancurkan rantai sehingga terbentuk blok dengan cabang yang baru. Sebagai contoh perbandingan adalah dengan membandingkan verifikasi ataupun autentikasi dengan menggunakan Json Web Token (JWT) di sistem *centralized* dengan *server* dan melakukan verifikasi lewat *smart contract* di dalam jaringan *blockchain*. Dari kedua perbandingan ini dapat diperoleh bahwa verifikasi berbasis JWT tidak dilakukan di *client*

melainkan hanya dapat terverifikasi dengan cara *client* mengirimkan JWT ke *server* kemudian *server* mengecek menggunakan *secret* yang hanya dimiliki oleh *server*. Saat proses ini apabila pihak ketiga masuk dan berpura-pura menjadi *server* akan terlihat seolah-olah *server* memvalidasi JWT dan memberikan *response* data ke *server* padahal data yang diberikan berupa data yang tidak *valid*. JWT sendiri juga dapat di-*encode* sehingga *payload*-nya dapat dilihat sebagai *plain text*. Sedangkan proses validasi ke *smart contract* akan terjadi secara *transaction* dari *address-to-address* sehingga MITM yang mungkin terjadi adalah dengan mengubah tujuan *address* dari pengirim namun di sisi *client* mampu untuk melakukan verifikasi apakah betul yang diajak berkomunikasi lewat transaksi merupakan *address* yang *valid* atau tidak karena *client* terhubung dengan *wallet* atau *Externally Owned Account* (EOA).

Contoh di atas dapat terjadi dalam konteks *remote update* yang membutuhkan validasi sebuah data *firmware*, apabila diartikan ke konteks yang berbeda seperti MITM pada [2] jaringan *Bitcoin* dengan mengubah tujuan *address* yang ingin dikirimi *cryptocurrency Bitcoin* tentu akan berbahaya karena transaksi *cryptocurrency* memakai mekanisme *one-way transaction* sehingga apabila sudah terkirim tidak dapat dikembalikan dan yang dikirim merupakan langsung nominal *cryptocurrency*.

Pada penelitian ini penulis akan melakukan implementasi teknologi *blockchain* pada proses *remote update* dengan melibatkan teknologi tambahan *InterPlanetary File System* (IPFS) sebagai tempat penyimpanan. Penelitian ini akan mengambil dasar perbandingan terhadap sistem *remote update* yang berbasis *centralized* atau menggunakan server. Dengan melibatkan teknologi ini, proses pengecekan data akan menjadi lebih aman karena mengimplementasikan sifat dasar dari *blockchain* dimana data tidak dapat di ubah (*immutable*). Proses pengiriman data yang melibatkan perangkat dan penyimpanan mungkin masih bisa saja diretas dan peretas berperilaku layaknya pengirim yang *valid* namun dengan adanya sistem yang dirancang ini akan membuat mekanisme autentikasi data berdasarkan

content identifier (CID) yang merupakan hash dari data yang disimpan di dalam IPFS.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang sudah dijabarkan di atas, ada beberapa rumusan masalah yang diperoleh, yaitu :

1. Bagaimana kemampuan sistem untuk melakukan verifikasi file pada perangkat?
2. Apakah proses verifikasi file yang dilakukan oleh perangkat ke *smart contract* dapat terbebas dari serangan *man-in-the-middle* yang memotong komunikasi dan memodifikasi *response* dari *smart contract* ?

1.3 Batasan Penelitian

Dalam penelitian ini, penulis menetapkan batasan masalah sebagai berikut:

1. Performa kecepatan komunikasi tidak menjadi fokus pada penelitian ini, baik komunikasi antara halaman tampilan (*frontend*) dengan *smart contract* di dalam jaringan *blockchain* serta antara perangkat dengan penyimpanan IPFS dan *smart contract*.
2. Peneliti tidak melakukan proses *deployment* terhadap jaringan *blockchain* ke *main network* ataupun *test network* melainkan dijalankan secara lokal *peer-to-peer* dengan bantuan *virtual machine* (VM).
3. Proses transaksi ke *blockchain* yang akan memakan *gas fee* tidak dipertimbangkan dalam penelitian ini.
4. File yang dianggap sebagai file *firmware* untuk dikirimkan ke perangkat merupakan file teks biasa.
5. Keseluruhan penelitian berfokus pada proses komunikasi antar entitas, sehingga proses pembuatan *account* di halaman *dashboard* tidak menjadi perhatian penulis melainkan penulis sudah

mempersiapkan beberapa *account address* yang sudah bisa digunakan.

1.4 Tujuan Penelitian

Berdasarkan pertanyaan rumusan masalah diatas, maka tujuan dari penelitian ini adalah sebagai berikut:

1. Mengetahui perbandingan keamanan dalam proses komunikasi antara sistem yang dirancang dengan sistem *centralized* yang ada dan banyak digunakan.
2. Mengamati pengiriman informasi *address-to-address* yang dimiliki *Blockchain* serta *content identifier* milik IPFS dalam melakukan verifikasi data tanpa mempertimbangkan aspek *secure communication*.

1.5 Manfaat Penelitian

Manfaat dari penelitian ini adalah:

1. Peneliti memperoleh pengetahuan sekaligus pengalaman dalam menggunakan dan berinteraksi secara langsung dengan teknologi *blockchain* dan IPFS yang dapat menjadi bekal bagi peneliti di dunia kerja atau sekedar *general knowledge*.
2. Peneliti dapat memahami proses komunikasi *peer-to-peer* yang menjadi salah satu dasar dari teknologi yang digunakan.
3. Penelitian ini dapat menjadi referensi ataupun bahan perbandingan bagi penelitian-penelitian yang lain dengan topik terkait.