BAB I

PENDAHULUAN

1.1 Latar Belakang

Sistem akses kontrol merupakan salah satu faktor yang penting dalam keamanan. Sistem asked kontrol memberikan keamanan berupa pembatasan bagi pengguna untuk mengakses ruangan ataupun suatu ruang dengan sebuah kunci [1]. Sistem akses kontrol sendiri sudah digunakan dari zaman dahulu. Beberapa contoh dari sistem akses tradisional adalah kunci pintu, gerbang pintu dan sebagainya. Seiring dengan berkembangnya zaman, Sistem akses kontrol tradisional sering juga disebut dengan *physical access control.* Seiring dengan berkembangnya teknologi, sistem akses kontrol juga ikut berkembang. Sistem akses kontrol yang sering ditemukan pada saat ini disebut dengan *electronic access control.* Sistem *electronic* merupakan sistem yang merupakan gabungan dari koneksi antar komputer (*cyber)* dengan sistem fisik (*physical)* [2]. Beberapa contoh dari *electronic access control* adalah sistem akses dengan menggunakan biometric, sistem akses dengan menggunakan *smart card*, dan sebagainya.

Electronic access control memiliki beberapa kelebihan dari *physical access control*, namun juga memiliki beberapa kekurangan. Salah satu kekurangan dari sistem ini adalah sistem yang digunakan masih tersentralisasi. Sistem yang tersentralisasi ini dapat memungkinkan adanya beberapa kekurangan seperti, *single point of failure. Single point of failure* merupakan suatu kekurangan pada sistem dimana jika sistem gagal untuk bekerja, maka sistem tersebut menjadi tidak dapat bekerja [3]. Selain itu *single point of failure* juga membuat *attacker* dapat menyerang sistem dan sistem akan terkompromi. Beberapa contoh dari *single point of failure* adalah kebakaran pada Gedung Cyber 1 yang menghentikan beberapa layanan [4] serta kebocoran data BPJS [5]. Kelemahan *single point of failure* umumnya dapat diatasi dengan sistem komputasi awan atau *cloud.*

Selain *Single point of failure,* sistem akses kontrol *electronic* yang memiliki data yang tersentralisasi juga menyimpan data pada suatu server yang disebut

dengan *Log*. Sistem *Logging* merupakan suatu sistem yang mencatat tentang siapa saja yang melakukan akses ke suatu ruangan. Sistem *log* ini dapat digunakan sebagai salah satu cara untuk melakukan *tracing* terhadap siapa saja yang melakukan akses, namun sistem *log* ini juga memiliki salah satu kekurangan yaitu *Log Tampering*. *Log Tampering* merupakan salah satu teknik dimana *attacker* menyerang sistem *log* pada sistem dengan cara menginjeksi, memanipulasi atau mengubah entri *log* sehingga memungkinkan *attacker* untuk menghilangkan jejak dari penyerangan maupun untuk menyesatkan *log* ketika audit *log* dijalankan [6]. *Log tampering* pada sistem akses kontrol *electronic* digunakan untuk menghilangkan jejak akses seseorang dari sebuah ruangan ataupun ruang.

Salah satu cara untuk mengatasi kedua masalah tersebut adalah dengan menggunakan sistem terdistribusi atau yang disebut dengan *distributed system.* Sistem terdistribusi adalah sistem dimana data yang ada tidak disimpan tidak berada pada satu komputer atau satu *server* saja, namun terdistribusi diantara beberapa komputer maupun client [7]. Salah satu contoh sistem terdistribusi adalah sistem *peer-to-peer* seperti Torrent. Sistem terdistribusi lainnya yang sedang berkembang dan banyak digunakan adalah *Blockchain*. *Blockchain* merupakan sistem terdistribusi dimana setiap transaksi yang terjadi akan dicatat dalam sebuah *block*, *block* tersebut kemudian disimpan oleh banyak komputer, selain itu *block* yang telah dibuat dienkripsi menggunakan *hash*, sehingga jika terjadi perubahan pada data maupun serangan akan sulit dilakukan, karena data yang ada berada pada jaringan dari komputer yang ikut serta ke dalam *blockchain* tersebut. Sistem terdistribusi juga digunakan karena lebih aman dan lebih transparan daripada sistem yang terpusat [7].

Dengan adanya sistem terdistribusi, maka diharapkan kelemahan *single point of failure* dapat dihilangkan, karena sistem yang ada terdistribusi, sehingga jika salah satu *server* mati, *server* lainnya masih dapat digunakan untuk pemrosesan data dan sistem. Selain itu dengan adanya *hash* pada transaksi pada *blockchain*, maka diharapkan dengan penyimpanan data *logging* pada *blockchain* dapat memitigasi serangan terhadap *log tampering* dikarenakan dengan *hash* data pada *blockchain* tidak dapat diubah-ubah.

Selain hal tersebut, sistem akses kontrol elektronik umumnya menggunakan sistem kartu pintar berbasis RFID, *numpad password* dan *biometrics* seperti sensor sidik jari. Sistem akses kontrol berbasis teknologi memiliki kelebihan seperti memiliki waktu pemberian akses yang cepat maupun *power* yang digunakan untuk memproses data cukup rendah. Namun teknologi-teknologi akses kontrol tersebut juga memiliki beberapa kekurangan, seperti mudah untuk diserang serta melakukan penduplikasian identitas yang lebih mudah. Sebagai contoh untuk melakukan duplikasi kartu pintar RFID hanya dibutuhkan RFID *reader* yang digunakan untuk membaca isi konten dari kartu, dan kemudian isi konten kartu tersebut dapat diduplikasi ke kartu lainnya, atau untuk mendapatkan password dari *numpad*, penyerang dapat menggunakan teknik forensik untuk mendapatkan sidik jari dari *password* yang biasanya digunakan. Untuk mengatasi kekurangan ini, maka dapat digunakan sistem biometrik baru seperti *face recognition.*

Face recognition merupakan teknologi yang digunakan agar komputer dapat membaca wajah manusia. Sistem *face recognition* akan melakukan identifikasi wajah sesuai dengan data yang terdapat pada *database* dari sistem.*Face recognition* merupakan teknologi biometric yang memiliki sistem identifikasi yang lebih unik dan memiliki sistem yang kuat untuk menahan serangan. *Face recognition* banyak digunakan pada sistem akses kontrol, seperti contohnya adalah sistem akses kontrol untuk membuka kunci pada layar *smartphone.*

Seiring perkembangan teknologi, sistem autentikasi untuk akses kontrol juga ikut berkembang. Pada awalnya, autentikasi sistem akses kontrol hanya memerlukan satu sistem autentikasi, seperti misalnya pintu yang membutuhkan kunci atau pintu yang hanya membutuhkan *password.* Sistem autentikasi yang memakai satu sistem autentikasi disebut dengan *single factor authentication* [8]. Sistem SFA ini memiliki kekurangan seperti dengan mengetahui atau memiliki satu kredensial, maka jika kredensial tersebut dimiliki oleh orang lain, maka orang lain tersebut dapat mengakses seluruh sistem yang menggunakan kredensial tersebut. Oleh karena permasalahan ini, *two factor authentication* dibuat. *Two factor authentication* memakai dua kredensial untuk memberikan akses [9]. Sebagai contoh pada mesin ATM yang memakai kartu dan pin sebagai sistem autentikasi.

Sistem *two factor authentication* ini merupakan sistem yang umum digunakan, namun seiring berkembangnya teknologi sistem ini juga semakin mudah untuk diserang. *Multi factor authentication* dibuat untuk menambah keamanan dari sistem *two factor authentication*. Pada *multi factor authentication,* sistem menggunakan lebih dari dua kredensial sebagai sistem authentikasi [10]. Dengan bertambahnya kredensial, maka akan lebih sulit untuk mendapatkan akses jika penyerang tidak memiliki kredensial yang dibutuhkan.

Berdasarkan latar belakang yang telah disampaikan diatas, maka penulis merancang penelitian dengan judul "Rancang Bangun Sistem Akses Kontrol Elektronik Berbasis Blockchain".

1.2 Rumusan Masalah

Berdasarkan latar belakang yang penulis paparkan diatas, maka rumusan masalah penelitian dapat dibagi menjadi beberapa poin, yaitu:

1.2.1 Apakah sistem dapat mengatasi *single point of failure* dengan menggunakan 2 *node* dan 1 *node*?

1.2.2 Apakah sistem dapat mengatasi *Log Tampering* dengan menggunakan 51% attack?

1.2.3 Bagaimana performa sistem dalam memberikan dan memproses akses kepada *user*?

1.3 Batasan Masalah

Batasan masalah pada penelitian ini adalah sebagai berikut

1.3.1 Sistem yang dirancang akan menggunakan *blockchain* berupa *private* Ethereum *network* yang akan dijalankan menggunakan program Geth serta IPFS pada *virtual machine* dikarenakan pengimplementasian menggunakan Main Net cukup memakan biaya.

1.3.2 Sistem akan menggunakan *blockchain* dan IPFS berupa *virtual machine* dikarenakan keterbatasan perangkat.

1.3.3 Sistem yang dirancang menggunakan Raspberry Pi, karena Raspberry Pi merupakan *single board computer* sehingga dapat memproses data lebih cepat dibandingkan NodeMCU atau Arduino.

1.4 Tujuan Penelitian

Tujuan dari penelitian ini adalah pengimplementasian sistem kontrol elektronik menggunakan *face recognition* berbasis *blockchain* dan IPFS.

1.5 Manfaat Penelitian

Manfaat Penelitian ini adalah

1.5.1 Mendukung perkembangan implementasi *blockchain* pada bidang IoT.

1.5.2 Memperketat keamanan sistem akses kontrol berbasis elektronik

1.5.3 Memberikan alternatif sistem akses kontrol berbasis elektronik

1.6 Sistematika Penelitian

Laporan penelitian ini disusun menjadi 5 bagian untuk mempermudah pemahaman pembaca dalam membaca laporan ini.

Bab I berisi pendahuluan yang menjelaskan tentang latar belakang, rumusan masalah, batasan penelitian, tujuan penelitian dan manfaat penelitian dari penelitian yang diteliti oleh penulis.

Bab II berisi mengenai penelitian-penelitian terkait terdahulu yang dijadikan referensi penelitian, serta poin-poin penting yang dapat diambil dari penelitian-penelitian terdahulu tersebut. Selain itu, pada bab ini juga berisi mengenai deskripsi

mengenai sistem perangkat keras dan perangkat lunak yang digunakan untuk pengimplementasian sistem pada penelitian ini.

Bab III berisi mengenai rancangan umum dari keseluruhan sistem yang diteliti, serta rancangan detail mengenai setiap sub-sistem dari sistem. Selain itu, pada bab ini juga berisi mengenai cara kerja singkat sistem yang diimplementasikan pada penelitian ini.

Bab IV berisi mengenai hasil dan analisis dari implementasi sistem berdasarkan rancangan yang telah dibahas pada bab III. Bab IV juga berisi mengenai kendala dan solusi terhadap masalah yang dihadapi dalam proses penelitian.

Bab V berisi mengenai kesimpulan yang didapat dari penelitian serta saran terhadap penelitian-penelitian yang selanjutnya yang akan diteliti berdasarkan penelitian ini.