# 1. Pendahuluan

**Latar Belakang**

*Internet of Things* (IoT) merupakan kumpulan perangkat yang terdistribusi, saling terhubung dan bertukar data pada suatu jaringan untuk mengubah kondisi fisik menjadi digital atau pun sebaliknya sehingga menghasilkan suatu layanan. Layanan ini dapat dimanfaatkan pada banyak domain seperti *smart home*, *smart city*, layanan kesehatan, kendaraan tanpa awak, pertanian, industri, hingga *retail-sector*[1].

Pemanfaatan perangkat IoT mengalami peningkatan jumlah instalasi setiap tahunnya[2], hal yang sama dialami juga oleh produk *smart home*, dimana pada 2017 *market share smart home* mencapai 76.6 milyar USD dan diperkirakan akan mencapai 151.4 milyar USD pada tahun 2024[3].

Peningkatan instalasi perangkat IoT merupakan salah satu faktor kriteria sebagai perangkat dengan resiko keamanan yang tinggi berdasarkan klasifikasi Ivan Cvitić et al[4]. Karakteristik terdistribusi pada perangkat IoT juga memiliki tantangan dan risiko pada keamanan perangkat, salah satu tantangan tersebut merupakan hak akses[5]. Perangkat IoT seharusnya hanya dapat diakses oleh organisasi tertentu yang memiliki kewenangan.

Banyak metode untuk mengamankan perangkat IoT, kebanyakan metode tersebut memiliki karakteristik *centralized* yang mana alur lalu lintas jaringan mengarah dari banyak ke satu entitas sehingga berisiko terhadap *single-point-of-failure*[6], oleh karena itu dibutuhkann metode keamanan yang *decentralized* dan terdistribusi. Salah satu teknologi yang umum diketahui memiliki karakteristik terdistribusi dan *decentralized* adalah *Blockchain*[7][8][9].

Perangkat IoT memiliki penyimpanan dan sumber daya yang terbatas, hal ini bertolak belakang dengan kebutuhan Blockchain[10][11]. Blockchain harus menyimpan seluruh transaksi dari awal Blockchain dijalankan, dan melakukan komputasi untuk memenuhi kriteria konsensus[12], sehingga memerlukan suatu pendekatan sebagai perantara antara Blockchain dan perangkat IoT.

Penulis merancang dan mengimplementasikan perantara berupa middleware sebagai kontrol akses berbasis Blockchain untuk mengontrol komunikasi perangkat IoT. Blockchain ditempatkan pada perangkat dengan sumber daya dan penyimpanan yang tinggi dan besar, biasanya berupa komputer *server*, sehingga dapat mempertahankan karakteristik *decentrilized* dan terdistribusi dari Blockchain.

**Topik dan Batasannya**

Berdasarkan latar belakang di atas penulis merancang dan mengimplementasikan *middleware* sebagai perantara antara Blockchain dan perangkat IoT. Agar penulisan ini dapat dilakukan lebih fokus dan mendalam, penulis merumuskan beberapa batasan sebagai berikut:

- Protokol komunikasi antara *middleware* dan IoT menggunakan HTTPS.
- Komunikasi antara *middleware* dan Blockchain menggunakan *library* web3 yang menggunakan protokol RPC
- Penulis memakai Ethereum sebagai Blockchain.
- Melakukan serangan *Sniffing* untuk menguji kerahasiaan data dan *Denial-of-service* untuk menguji karakteristik *decentrilized*.

**Tujuan**

Penulis merancang dan mengimplementasikan perantara berupa *middleware* antara Blockchain dan perangkat IoT sebagai kontrol akses untuk mengontrol komunikasi perangkat IoT sehingga dapat mempertahankan karakteristik *decentrilized* dan terdistribusi dari Blockchain.

**Organisasi Tulisan**

Penulisan ini dirumuskan menjadi beberapa bagian. Pendahuluan memuat latar belakang dan batasan dari sistem. Studi Terkait memaparkan tulisan yang berkaitan dengan sistem. Perancangan dan implementasi dirumuskan pada bagian Sistem yang dibangun. Penulis melakukan analisis pada bagian Evaluasi dan memaparkan kesimpulan pada bagian Kesimpulan.