BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Pada pertengahan abad ke-20 ini, teknologi informasi semakin berkembang pesat seiring berjalannya waktu untuk mempermudah pekerjaan manusia. Semakin berjalannya waktu kebutuhan manusia di masa yang akan datang membuat peran komputer sangat penting dalam pekerjaan manusia seperti mengendalikan alat elektronik dari jarak jauh menggunakan internet. Manusia memiliki keinginan untuk semua aktivitasnya dapat terhubung dengan internet sehingga dapat mempermudah segala kebutuhannya. Seiring berkembangnya teknologi internet dan perangkatnya, semua perangkat elektronik di sekitar kita dapat dikendalikan dan dapat saling berkomunikasi dengan alat elektronik lainnya melalui internet. Hal ini dapat kita kenal dengan istilah *internet of things* (IoT).

Internet of Things (IoT) merupakan suatu perkembang internet yang sedang ramai pada saat ini, dimana alat-alat elektronik dapat berkomunikasi dan dapat memberikan informasi data yang *real time*. Saat ini *Internet of Things* (IoT) ini menggunakan sebuah perangkat yang sudah tertanam dan telah dikonfigurasi sesuai kebutuhan kita, misalnya *smartwatch*, e-tilang , dan *smarthome*. Hampir semua perangkat *Internet of Things* (IoT) memiliki fungsi untuk merekam atau menyimpan data tertentu, sehingga memerlukan suatu authentikasi pada data tersebut agar terhindar dari penyadapan dan modifikasi data oleh pihak yang tidak bertanggung jawab. Tetapi hal penting yang menjadi perhatian adalah authentikasi yang digunakan, dikarenakan perangkat *Internet of Things* (IoT) pada umumnya memiliki kemampuan komputasi yang rendah. Karena hal tersebut enkripsi yang digunakan harus cukup ringan secara komputasi, dan untuk memenuhi kebutuhan tersebut maka enkripsi yang akan digunakan adalah *Elliptic Curve Cryptography* (ECC).

Menurut penelitian yang dilakukan oleh Koblitz [2] dan Miller [3] pada pertengahan tahun 1987, *Elliptic Curve Cryptography* (ECC) telah diterapkan secara luas dalam kriptografi kunci publik, terutama dalam menghubungkan beberapa kriptosistem[4][5]. Hal tersebut dikarenakan *Elliptic Curve Cryptography* (ECC) menggunakan ukuran kunci yang lebih pendek dan juga memiliki tingkat keamanan yang cukup tinggi dibandingkan kunci publik lainnya. Misalnya, *Elliptic Curve Cryptography* (ECC) kunci 160 *bits* setara dengan *Rivest Shamir Adleman* (RSA)

kunci 1024 *bits*, *Elliptic Curve Cryptography* (ECC) kunci 224 *bits* setara dengan *Rivest Shamir Adleman* (RSA) kunci 2048 *bits*, dan *Elliptic Curve Cryptography* (ECC) kunci 256 *bits* setara dengan *Rivest Shamir Adleman* (RSA) kunci 3072 *bits*[6].

Karena panjang kunci yang lebih pendek, kecepatan yang tinggi dan konsumsi daya yang lebih rendah, sehingga *Elliptic Curve Cryptography* (ECC) banyak diterapkan pada perangkat *wireless* yang memiliki penyimpanan dan *bandwidth* yang terbatas[7], hal tersebut membuat algoritma *Elliptic Curve Cryptography* (ECC) sangat sesuai digunakan pada perangkat *Internet of Things* (IoT) yang memiliki komputasi yang rendah. Meskipun ada pengoptimalan terbaru pada *Elliptic Curve Cryptography* (ECC) yaitu pengurangan kompleksitas komputasi, *Elliptic Curve Cryptography* (ECC) tetap kompleks dan membutuhkan pengoptimalan lebih lanjut. Hal terpenting dan inti dari operasi di *Elliptic Curve Cryptography* (ECC) untuk *encryption, decryption, digital signature, key exchange*.

Berdasarkan penelitian *elliptic curve cryptography* (ECC) sebelumnya [8], penelitian dilakukan dengan menganalisis pada perangkat yang memiliki spesifikasi rendah. Hasil penelitian tersebut menunjukkan pemakaian energi dari algoritma ECC menggunakan protokol *Schnnor* yang telah diimplementasikan dalam berbagai sistem koordinat, tetapi belum mencoba untuk menggunakan protokol *Zero Knowledge Protocol* (ZKP) lainnya dan belum membandingkan hasil dari penelitiannya dengan algoritma lainnya.

Sehingga pada penelitian Tugas Akhir ini akan menerapkan metode dengan menganalisis kinerja *Elliptic Curve Cryptography* (ECC) berbasis *Fiat-Shamir* dan *Elliptic Curve Diffie-Hellman* (ECDH) pada perangkat *Internet of Things* (IoT). Penelitian ini juga akan membandingkan kinerja *Elliptic Curve Cryptography* (ECC) berbasis *Fiat-Shamir* dengan *Elliptic Curve Diffie-Hellman* (ECDH) pada perangkat *Internet of Things* (IoT) yang bertujuan untuk memaksimalkan kinerja terbaik pada algoritma *Elliptic Curve Cryptography* (ECC) untuk diterapkan sebagai kriptografi pada perangkat *Internet of Things* (IoT) tersebut.

1.2 Rumusan Masalah

Berdasarkan latar belakang diatas, permasalahan yang dapat diangkat adalah:

1. Berdasarkan data yang ada, perkembangan perangkat IoT akan selalu meningkat setiap tahunnya. Oleh karena itu, diperlukan authentikasi untuk mencegah dan memastikan seseorang yang mengakses adalah seseorang yang memiliki otoritas.

2. Perlunya analisis algoritma ECC berbasis *Fiat-Shamir* dan algoritma ECDH-HMAC terhadap perangkat IoT.

1.3 Tujuan dan Manfaat

Tugas Akhir ini bertujuan untuk mempelajari performansi ECC berbasis *Fiat-Shamir* dan ECDH berbasis HMAC, kemudian akan mensimulasikan dan membandingkan kinerjanya untuk mencari hasil terbaik pada perangkat IoT.

Adapun manfaat Tugas Akhir ini adalah memberikan referensi pilihan sistem authentikasi data yang lebih efisien dalam memiliki performansi yang lebih baik saat diaplikasikan pada perangkat IoT.

1.4 Batasan Masalah

Tugas Akhir ini membatasi masalah dengan rincian sebagai berikut:

1. Penelitian ini hanya menggunakan teknik authentikasi ECC.
2. Melakukan simulasi dengan 2 perangkat berbeda yaitu Laptop dengan OS *Windows* dan raspberry pi sebagai IoT dengan OS *Linux*.
3. Melakukan simulasi dengan skema ECC berbasis *Fiat-Shamir* dan ECDH bebasis HMAC.
4. Melakukan perbandingan hanya pada kinerja dari ECC berbasis *Fiat-Shamir* dan ECDH-HMAC.

1.5 Metode Penelitian

Metode penelitian yang diterapkan dalam penyelesaian Tugas Akhir ini adalah sebagai berikut:

1. Studi literatur ECC
   Tahap ini melakukan pengumpulan literatur yang berkaitan dengan ECC, *Fiat-Shamir*, ECDH, dan HMAC. Literatur tersebut dapat berupa buku dan jurnal dari berbagai publikasi nasional maupun internasional.
2. Kinerja sistem
   Tahap ini melakukan simulasi terhadap perangkat IoT yang telah diusulkan dengan menggunakan skema ECC yang telah dipelajari.

3. Penarikan kesimpulan

   Tahap ini melakukan penarikan kesimpulan hasil simulasi yang telah diperoleh yang ditentukan dari hasil dan analisis dari ECC berbasis *Fiat-Shamir* dan ECDH-HMAC yang telah disimulasikan pada perangkat IoT.