1 PENDAHULUAN

1.1 Latar Belakang

Autentikasi identitas pengguna komputer atau jaringan berperan melindungi keamanan informasi. Sistem autentikasi tradisional yang menggunakan *trusted third-party authentication* memiliki masalah yang terpusat seperti *single point of failure*, transparansi yang buruk dan masalah keamanan yang serius. Penggunaan *blockchain* menjadi solusi untuk keamanan informasi yang bisa diandalkan [1].

Penggunaan *identity-based cryptography* dibandingkan dengan sisem autentikasi tradisional salah satunya SSL *authentication protocol* lebih cepat 58%, sehingga *identity-based cryptography* lebih cepat dan lebih efisien dibandingkan dengan SSL *authentication protocol* yang merupakan sistem autentikasi tradisional [2].

Skema autentikasi yang aman berdasarkan *blockchain* dan *identity-based cryptography* dapat mengatasi permasalahan pengelolaan sertifikat yang rumit, perlindungan privasi, dan keamanan pada sistem autentikasi tradisional. Hal ini dilakukan dengan memanfaatkan *Private Key Generator* (PKG) terdesentralisasi untuk menghindari manajemen sertifikat yang kompleks, meningkatkan perlindungan privasi, meningkatkan keamanan dan lebih efisien, namun membutuhkan biaya yang tinggi karena overhead yang tinggi [3].

Untuk penerapan autentikasi dengan *identity-based* pada *blockchain* secara tradisional, hal yang perlu diperhatikan adalah penyimpanan dan penyebaran identitas pribadi yang digunakan sebagai *public key* agar tetap aman karena bisa berpotensi terjadi pencurian dan penyalahgunaan identitas pribadi, yang kemudian data tersebut dapat digunakan untuk mengakses data lainnya di *blockchain*, selain itu ada juga kemungkinan gangguan saat pembaruan atau pencabutan jika diterapkan akses dengan anonimitas total. Tetapi, penggunaan *identity-based* ini lebih baik karena menggunakan *short term key* yang tidak ditautkan dan tidak mengungkapkan *public key* pada skema autentikasinya [4].

Salah satu contoh penerapan *identity-based* pada *blockchain* yaitu E-residency, menyediakan layanan autentikasi universal tanpa batas yang menyimpan data kependudukan menggunakan *blockchain* dan menerapkan *single identity credential*. Hal ini memudahkan akses, manajemen data dan penelusuran historis data serta tidak membutuhkan lagi dokumen fisik dalam kepentingan administrasi, tetapi dapat menimbulkan pencurian dan penyalahgunaan identitas serta juga bertentangan dengan hukum perbankan internasional dan hukum negara Uni Eropa dan Estonia [5].

Selain itu, penerapan *blockchain* untuk autentikasi juga bisa digunakan untuk biometrik seperti *face recognition*, salah satunya dengan metode *fuzzy extractor* yang datanya disimpan di *blockchain*, sehingga kontrol informasi pribadi lebih baik, rendah biaya, dan data *face recognition* lebih aman karena disimpan secara terdesentralisasi. Namun, jika terjadi kebocoran atau ada data *face recognition* yang identik, untuk nilai kemiripan tertentu akan terjadi kekeliruan akses data, hingga penggunaan data oleh pihak yang bukan seharusnya [6].

Penggunaan *identity-based cryptography* yang merupakan penerapan *asymmetric cryptography* membutuhkan kompleksitas komputasi dan biaya komputasi yang tinggi. Sehingga dibutuhkan optimalisasi dalam proses tersebut. Metode *cryptography* yang ringan secara komputasi namun kecepatan komputasinya tinggi adalah *symmetric cryptography*, salah satunya *lightweight cryptography*.

1.2 Perumusan Masalah

Berdasarkan latar Belakang yang telah diuraikan, permasalahan yang menjadi dasar pengerjaan tugas akhir adalah bagaimana menerapkan komputasi yang efisien dalam penerapan *identity-based cryptography* dalam proses autentikasi *blockchain* pada perangkat dengan komputasi rendah dari segi waktu komputasi.

1.3 Tujuan

Tujuan yang akan dicapai pada tugas akhir ini adalah menganalisa performa *identity-based cryptography* dari segi waktu komputasi pada setiap proses pada *blockchain*

serta memberikan rekomendasi batasan yang paling efektif dengan komputasi paling rendah.

1.4 Hipotesis

Penerapan *identity-based cryptography* konvensional memiliki kompleksitas yang tinggi dan mengakibatkan biaya yang tinggi pada blockchain, maka perlu adanya efisiensi proses komputasi salah satunya dari segi waktu komputasi. *cryptography* yang rendah komputasi yaitu *light-weight identity based cryptograpy* dapat menurunkan komputasi dan dapat diterapkan pada perangkat dengan daya komputasi terbatas.

1.5 Rencana Kegiatan

Dalam pelaksanaan tugas akhir ini terdapat beberapa proses untuk mecapai tujuan analisa sebagai berikut:

1. Kajian Pustaka

   Tahap ini dilakuan dengan menelaah referensi dan membuat *literatur review* dari jurnal atau buku referensi yang sesuai dengan topik yang diambil. Adapun referensi yang digunakan yaitu jurnal 10 tahun terakhir. Salah satunya adalah jurnal utama yang digunakan untuk adopsi pengembangan aspek lain dari studi kasus yang sama pada jurnal tersebut dan satu jurnal pendukung utama.
2. Rancangan penelitian

   Menghitunng waktu komputasi *light-weight cryptography* untuk *identity-based cryptography* pada *blockchain* pada kasus yang sama dengan jumlah data yang berbeda kemudian membandingkan hasilnya dengan hasil uji penggunaan teknik autentikasi lain dari penelitian yang sudah pernah dilakukan.
3. Cara pengujian

   Menghitung waktu komputasi pada *light-weight identity-based cryptography* menggunakan simulasi dengan jumlah data berbeda kemudian membandingkan waktu komputasi yang terdapat pada paper acuan kedua.