BAB I
PENDAHULUAN

1.1 Latar Belakang

Web Service menjadi tren teknologi masa kini dan menjadi bagian penting dari berbagai aplikasi dan sistem yang terhubung pada jaringan. Salah satu arsitektur *web service* adalah *REpresentational State Transfer* (REST). Arsitektur REST diperkenalkan pada tahun 2000 oleh Thomas Fielding dan terus berkembang membuat penerapannya pada *web service* meningkat dan umum dibanding dengan aristektur lainnya (Neumann dkk., 2021). Dalam sistem aplikasi, autentikasi merupakan suatu hal yang esensial yang bertujuan untuk melindungi batasan-batasan sistem serta sumber daya sistem dari pihak yang tidak berwenang (He dan Yang, 2017). Pada sistem RESTful diperkenalkan berbagai metode autentikasi diantaranya adalah autentikasi berbasis token (*Token-based Authentication*) (Ehsan dkk., 2022). Token berbentuk string akan digunakan pada sesi permintaan dan respons. Mekanisme pembuatan dan validasi token bergantung pada pengembang, salah satu konsep yang dapat digunakan adalah JSON Web Token (JWT).

JWT merupakan standar terbuka untuk protokol pertukaran informasi berbasis token yang berfungsi untuk autentikasi dengan menjamin integritas pesan yang dibawanya (lihat lampiran 1 RFC7519). JWT dapat memberikan jaminan keamanan serta hak akses untuk mengelola data pada sistem. Bagian penting dalam JWT adalah menggunakan berbagai algoritma kriptografi tanda tangan (*signing algorithm*) baik algoritma simetris (*secret key*) maupun algortima asimetris (*public key*). Algortima tanda tangan yang umum digunakan antara lain yaitu HMAC (*Hash Message-based Authentication Code*) untuk algoritma simetris, serta RSA (*Rivest Shamir Aldeman*) dan ECDSA (*Elliptic Curve Digital Signature Algorithm*) sebagai algoritma asimetris. Algoritma tanda tangan tersebut juga dilindungi dengan algoritma *hashing* yang umumnya digunakan yaitu SHA (*Secure Hash Algorithm*) (lihat lampiran 1 RFC7519).

Algoritma tanda tangan yang umum digunkan pada JWT memiliki beberapa kerentanan. Algoritma tanda tangan simetris HMAC menggunakan *secret key* yang harus dapat diakses baik pada proses pembuatan token atau proses verifikasi sehingga memberikan kerentanan (Tijms dkk., 2022). *Secret key* yang lemah sangat rentan terhadap serangan *offline brute force* atau *dictionary attack* saat penyerang memperoleh token (lihat lampiran 1 RFC8725). Sehingga saat *secret key* dimiliki oleh pihak yang tidak berwenang penyerang dapat memanipulasi token serta memperoleh hak akses yang ilegal terhadap sistem aplikasi.

Pada algoritma tanda tangan asimetris (RSA dan ECDSA) terdapat kunci privat yang digunakan untuk proses pembuatan token serta kunci publik yang hanya digunakan untuk proses verifikasi, sehingga kedua kunci tidak dapat dipertukarkan. Algoritma tanda tangan asimetris RSA memiliki panjang kunci yang besar serta proses komputasi yang cenderung lebih lambat, sehingga kurang cocok jika digunakan pada sistem yang memiliki sumber daya perangkat yang terbatas. Sementara itu algoritma tanda tangan asimetris ECDSA memiliki panjang kunci yang cenderung lebih kecil serta proses komputasi yang lebih cepat dibanding dengan RSA yang membuat ECDSA cocok untuk sistem yang memiliki sumber daya terbatas (Josias dan Eugène, 2020). Namun demikian ECDSA sangat bergantung pada nilai acak pada setiap pesan yang ditanda tangani (lihat lampiran 1 RFC8725), selain itu juga ECDSA memiliki kerentanan terhadap serangan seperti *fault attack* (Barenghi dkk., 2011) dan *side-chanel attack* (Varchola dkk., 2016) yang memungkinkan penyerang mengeksploitasi kunci privat pada ECDSA.

Dalam hal mencari alternatif lain agar autentikasi menggunakan JWT pada REST *web service* memiliki performa yang lebih baik serta keamanan yang lebih unggul terdapat algoritma tanda tangan asimetris yang dapat digunakan pada JWT salah satunya yaitu EdDSA (*Edwards-Curve Digital Signature Algorithm*). Diluar konteks JWT, EdDSA secara umum memiliki keuntungan dengan performa yang lebih baik pada berbagai platform, tidak bergantung pada nilai acak untuk setiap pesan serta keamanan yang tinggi seperti lebih tahan terhadap *side-channel attack* (lihat lampiran 1 RFC8032). EdDSA juga secara umum memiliki performa yang lebih baik serta

keamanan yang lebih unggul seperti kurva yang lebih aman dibanding dengan ECDSA (Aggarwal dan Kumar, 2021).

Pemaparan tersebut dijadikan dasar oleh penulis untuk melakukan penelitian mengenai pengujian performa algoritma EdDSA sebagai algoritma tanda tangan asimetris pada JSON Web Token dalam mekanisme autentikasi pada aplikasi berbasis REST. Pada penelitian ini aplikasi REST yang diuji berupa *E-Commerce*. Penelitian ini akan melakukan proses pengujian performa dengan melakukan perbandingan antara algoritma EdDSA dan ECDSA pada JWT. Parameter atau metrik pengujian performa RESTful *web service* yang digunakan pada penelitian ini adalah waktu respons, *throughput* dan *utilization* (CPU dan memori) (Wang dan Wu, 2019). Dalam konteks mekanisme autentikasi JWT pada RESTful *web service* metrik-metrik tersebut akan di uji pada saat generasi token dan waktu verifikasi token (Rahmatulloh dkk., 2019).

1.2 Rumusan Masalah Penelitian

Berdasarkan latar belakang di atas, penelitian ini dirumuskan dengan beberapa masalah sebagai berikut:

1. Bagaimana proses pengujian performa berdasarkan waktu respons, *throughput* dan *utilization* algoritma EdDSA dan ECDSA pada JSON Web Token dalam mekanisme autentikasi aplikasi RESTful *web service*?
2. Bagaimana analisa performa berdasarkan waktu respons, *throughput* dan *utilization* algoritma EdDSA dan ECDSA pada JSON Web Token dalam mekanisme autentikasi aplikasi RESTful *web service*?

1.3 Tujuan Penelitian

Tujuan dari penelitian ini yaitu:

1. Menerapkan pengujian performa berdasarkan waktu respons, *throughput*, dan *utilization* algoritma EdDSA dan ECDSA pada JSON Web Token dalam mekanisme autentikasi aplikasi RESTful *web service.*

2. Menganalisa performa berdasarkan waktu respons, *throughput*, dan *utilization* algoritma EdDSA dan ECDSA pada JSON Web Token dalam mekanisme autentikasi aplikasi RESTful *web service.*

1.4 Manfaat Penelitian

Manfaat dari penelitian ini adalah sebagai berikut:

1. Secara akademis, penelitian ini dapat dijadikan acuan untuk penelitian selanjutnya yang terkait.
2. Secara praktis, penelitian ini diharapkan memberi kontribusi pada pengembang atau ahli yang terkait agar dapat mengembangkan sistem autentikasi yang lebih optimal dan aman.
3. Hasil penelitian ini diharapkan juga dapat digunakan dalam industri sebagai acuan penggunaan algoritma alternatif yang didasari pada performa algoritma asimetris pada mekanisme autentikasi menggunakan JSON Web Token yang bisa digunakan pada sistem dengan sumber daya yang terbatas.

1.5 Batasan Masalah Penelitian

Ruang lingkup dari penelitian ini diperlukan agar tujuan penelitian tidak melebar dan lebih terperinci. Adapaun batasan penelitian ini:

1. Implementasi algoritma EdDSA menggunakan bahasa pemrograman *Javascript* NodeJs yang akan diterapkan pada sisi server serta dibatasi pada lingkup *backend*.
2. Implementasi JSON Web Token menggunakan pustaka yang tersedia pada *Node Packet Manager* (NPM).
3. Pengujian performa akan membandingkan algoritma EdDSA dengan ECDSA berdasarkan parameter waktu respons, *throughput*, dan *utilization.*
4. Pengiriman data pada REStful *Web service* dilakukan dengan protokol HTTP.

1.6 Sistematika Penulisan Skripsi

Dalam bagian ini dibahas urutan penulisan dari setiap bab dan bagian bab dalam skripsi.

BAB I PENDAHULUAN

Pada bagian ini dijelaskan mengenai gambaran umum dari penelitian yang akan dilakukan. Pendahuluan bersisi latar belakang penelitian, rumusan masalah penelitian, tujuan penelitian, manfaat penelitian, batasa penelitian serta sistematika penulisan skripsi.

BAB II KAJIAN PUSTAKA

Bagian ini berisi kajian pustaka yang meliputi kerangka pemikiran, teori-teori terkait yang mendukung penelitian serta keadaan penelitan sebelumnya yang relevan dengan penelitan yang akan dilakukan.

BAB III METODOLOGI PENELITIAN

Bagian ini akan menguraikan metode dan prosedur yang akan digunakan untuk memecahkan masalah penelitian. Beberapa aspek yang akan dijelaskan termasuk desain penelitian yang akan digunakan, alat dan bahan penelitian, instrumen penelitian, hipotesis, analisis data.

BAB IV TEMUAN DAN PEMBAHASAN

Bagian ini akan memaparkan hasil penelitian disertai analisisnya sesuai dengan tujuan dan masalah penelitian yang telah diuraikan sebelumnya. Bagian ini mencakup proses pengujian performa pada algoritma EdDSA dan ECDSA yang diimplementasikan pada aplikasi RESTful *web service* serta analisis perbandingan hasil antara kedua algoritma tersebut.

BAB V SIMPULAN, IMPLIKASI, DAN REKOMENDASI

Bagian ini berisi kesimpulan dan saran. Dalam bagian ini disajikan penafsiran dan pemaknaan peneliti terhadap hasil ananlisis temuan penelitian. Saran dan rekomendasi ditulis setelah simpulan.