BAB I

PENDAHULUAN

1.1 Latar Belakang

Keamanan kini menjadi kendala yang sangat diperhatikan pada era digital saat ini, hal ini memberikan pengaruh yang besar terutama dalam bidang bisnis(Le, 2022). Sebuah website dituntut untuk memberikan keamanan agar dapat menjaga privasi maupun dokumen rahasia milik pengguna (Setiawan, Lusanjaya and Kurnia, 2019). Melihat dari perkembangan teknologi yang semakin meningkat saat ini, beberapa metode keamanan sudah banyak dikembangkan dan salah satu diantaranya adalah JWT atau JSON Web Token (Rosyada, 2021). Penggunaan JWT kini sudah cukup populer, karena mudah diterapkan namun mampu memberikan perlindungan yang sudah teruji keamanannya (Rahmatulloh, Sulastri and Nugroho, 2018). JWT mampu mengamankan transaksi data antar jaringan dengan melakukan proses autentikasi yang menggunakan sebuah token untuk validasi otorisasi akun pengguna (Peyrott, 2022).

Web service kini sangat diperlukan dalam melakukan integrasi pada sebuah sistem terutama dalam bidang *e-commerce,* karena dapat memudahkan pertukaran data pada berbagai platform yang berbeda (Rosyada, 2021). Web *service* yang saat ini sedang banyak digunakan adalah REpresentational State Transfer (REST). Ukuran pesan pada RESTful Web Service ini terbilang lebih kecil dibandingkan ukuran pesan dari web service berbasis SOAP (Simple Object Access Protocol). Akan tetapi, REST sangat rendah dalam segi keamanannya sehingga rentan terhadap peretasan yang dapat merugikan berbagai pihak (Rahmatulloh, Sulastri and Nugroho, 2018). Salah satu solusi untuk melindungi kerahasiaan dan integrasi

data adalah menggunakan JSON Web Token (JWT) untuk pengamanan yang efektif dan terdistribusi (Rosyada, 2021).

CV Jastra Card saat ini memiliki layanan *e-commerce* yang masih belum menerapkan keamanan khusus terutama pada *web service*-nya. Hal ini menjadi permasalahan akan tingkat kepercayaan pelanggan untuk melakukan pemesanan kartu undangan, kartu nama, buku dan beberapa media cetak lainnya secara online (Abdurrohim, 2019). Dengan masalah tersebut akan menjadi kendala pada pelayanan *e-commerce* percetakan pada CV Jastra Card. Untuk mengatasi masalah ini penerapan keamanan dibutuhkan untuk menjaga keamanan akun pengguna.

Penelitian sebelumnya telah banyak menerapkan berbagai metode dalam pembangunan Web *Service* yang menggunakan JWT sebagai keamanan. Penelitian pertama menerapkan sistem keamanan *web service* (RESTful API) menggunakan JWT untuk mengukur *authentication* dan *authorization* dengan Hashing Algoritma HMAC SHA-512 (Rosyada, 2021). Penelitian tersebut melakukan uji coba perbandingan performa antara algoritma HMAC SHA-256 dan algoritma HMAC SHA-512 yang memperoleh hasil performa HMAC SHA-512 lebih unggul dalam proses eksekusi. Selanjutnya penelitian kedua mengkaji tentang penggunaan JWT untuk Autentikasi pada Introperabilitas Arsitektur berbasis RESTful Web Service (Gunawan and Rahmatulloh, 2019). Penelitian tersebut menggunakan rancangan interoperabilitas sebagai arsitektur sistem yang dibuat. Selanjutnya penelitian ketiga membahas tentang pembangunan RESTful *Web Service* dengan JWT yang menerapkan HMAC-SHA 512 pada arsitektur 64-bit (Rahmatulloh, Sulastri and Nugroho, 2018). Penelitian tersebut memberikan

hasil dari kecepatan dan besarnya data yang dikirim pada JWT dengan menggunakan algoritma HMAC SHA-512 pada arsitektur 64-bit yaitu 50% lebih baik dari algoritma yang lainnya. Selanjutnya penelitian keempat mengkaji tentang penggunaan kriptografi JWT dalam mengimplementasi keamanan API (Rajagukguk, 2018). Penelitian tersebut memberikan batasan contoh dari penggunaan SHA-256 pada JWT. Dan yang penelitian terakhir menerapkan JWT yang digunakan untuk keamanan API yang menggunakan *framework* Django (Wijaya, Jacobus and Sambul, 2021). Penelitian tersebut telah berhasil mengembangkan sebuah sistem yang dapat mengintegrasikan atau bertukar data dari berbagai sistem yang berbeda. Berdasarkan penelitian yang telah dipaparkan diperoleh bahwa penerapan HMAC SHA-512 memiliki keunggulan dalam proses pengamanan maupun peforma eksekusi.

Penelitian ini bertujuan untuk menerapkan JSON Web Token yang menggunakan Algoritma HMAC-SHA 512 dan menggunakan metode *refreshing token authentication* dalam sistem keamanan *Web Service E-commerce* pada CV Jastra Card. Metode pengembangan yang digunakan dalam penelitian ini adalah metode RAD yang meliputi tahapan *Planning*, *User Design*, *Construction* dan *Cutover*. Untuk pengembangan sistem web service digunakan bahasa pemrogramman Phyton yang dipakai pada *framework* Django. Hasil penelitian ini menunjukan JSON *Web Token* mampu melindungi autentikasi akun pengguna. Penggunaan *refreshing token* bekerja lebih baik dari *access token* biasa, dikarenakan *refreshing token* mampu memberikan *access lifetime* serta dapat memblokir token yang sudah *expired*.

1.2 Rumusan Masalah

Rumusan masalah dalam penelitian ini adalah CV. Jastra Card belum memiliki keamanan pada *web service e-commerce* nya sehingga didapat permasalahan yaitu bagaimana memberikan keamanan pada *web service e-commerce*?

1.3 Batasan Masalah

Adapun beberapa batasan masalah pada pembuatan sistem web service pada CV Jastra Card yaitu :

1. Keamanan yang diterapkan hanya berfokus pada sisi *backend system*.
2. Penelitian dilakukan pada perusahaan CV Jastra Card berfokus pada sistem *e-commerce Bussiness to Customers*.
3. Proses implementasi serta pengujian dilakukan pada server localhost.

1.4 Tujuan Penelitian

Tujuan penelitian ini adalah memberikan keamanan pada *web service e-commerce* yang menggunakan JSON *Web Token* dengan algoritma HMAC-SHA 512 serta dikombinasikan dengan metode *refreshing token authentication* pada CV Jastra Card.

1.5 Manfaat Penelitian

Manfaat yang didapat pada penelitian pengamanan sistem *web service* pada CV Jastra Card adalah sebagai berikut :

1. Meningkatkan keamanan pada sistem *Web Service*.

2. Dapat mengetahui cara kerja sistem keamanan *web service* yang menerapkan JSON *Web Token* (JWT) dengan algoritma HMAC-SHA 512 dan *refreshing token authentication* pada RESTful API.