BAB I
PENDAHULUAN

1.1. Latar Belakang Penelitian

Di era digital yang semakin berkembang, sistem teknologi dan informasi yang aman sekaligus efisien merupakan salah satu prioritas utama di dalam bisnis dan perusahaan. Seiring dengan meningkatnya aktivitas pertukaran data, kebutuhan akan sistem informasi berskala besar (*Enterprise Information System*) merupakan urgensi bagi perusahaan terutama dalam mengintegrasikan berbagai sektor dan divisi di dalamnya (Hindra, dkk., 2023). Salah satu elemen penting dari suatu sistem informasi *enterprise* adalah *Application Programming Interface* (API) dengan arsitektur yang umum digunakan saat ini yaitu *Representational State Transfer* API (RESTful API) (Wijayanti, dkk., 2024). RESTful API banyak digunakan karena mekanisme komunikasinya yang relatif sederhana dan efisien. Selain itu, RESTful API juga merupakan arsitektur yang fleksibel dengan skalabilitas tinggi sehingga memudahkan perusahaan dalam mengintegrasikan berbagai sektor ke dalam satu sistem informasi tunggal berskala besar (Sofyan, dkk., 2024).

Seiring dengan implementasi RESTful API yang semakin luas, keamanan dan integritas menjadi tantangan baru yang krusial. Oleh karena itu, metode keamanan RESTful API yang optimal merupakan urgensi selanjutnya untuk memastikan proses pertukaran data terlindungi dan terhindar dari pihak luar yang tidak memiliki akses terhadap API tersebut (Darmawan, dkk., 2023). Metode keamanan yang optimal akan memastikan operasi dan aktivitas yang melibatkan data-data sensitif melalui API tersebut dapat terjaga sesuai dengan ketentuan akses yang diberikan, terutama pada RESTful API yang diakses melalui konektivitas internet (Senapartha, 2021).

Jenis kerentanan dan resiko yang umum terjadi pada RESTful API diantaranya adalah *Broken Object Level Authorization* dan *Broken Authentication* (Sugara, dkk., 2024; Prasetyo, 2024) . Menurut data yang diterbitkan oleh Open Worldwide Application Security Project (OWASP), *Broken Object Level Authorization* dan *Broken Authorization* merupakan dua resiko kerentanan yang teratas di dalam daftar 10 besar kerentanan dan resiko pada API yang paling signifikan serta banyak ditemukan di tahun 2023 (OWASP, 2023). Kedua resiko

dan kerentenan tersebut dapat terjadi karena beberapa faktor, seperti proses autentikasi dan otorisasi yang tidak sesuai yang memungkinkan pihak luar dapat mengeksploitasi validitas dan hak akses suatu API (Singh & Dandotiya, 2023), ataupun pengelolaan elemen autentikasi dan otorisasi pada sistem yang tidak optimal sehingga data-data kredensial di dalamnya dapat dibaca oleh pihak luar.

Berdasarkan kerentanan dan resiko tersebut, disimpulkan bahwa aspek yang menjadi elemen penting di dalam sistem keamanan pada RESTful API diantaranya adalah proses autentikasi dan otorisasi (Nugroho, dkk., 2023). Autentikasi akan memastikan bahwa pengguna yang mengakses suatu API merupakan pengguna yang valid dan autentik di dalam sistem tersebut sementara otorisasi akan memastikan bahwa pengguna tersebut memiliki hak akses terhadap API tertentu di dalam sistem (Cahyono, dkk., 2023). Autentikasi dan otorisasi pada RESTful API merupakan hal yang sangat krusial di dalam sistem informasi *enterprise* yang di dalamnya memiliki banyak pengguna dengan peran dan hak aksesnya yang berbeda satu dengan yang lain (Yuricha, dkk., 2023).

Pada praktik terbaiknya, ada beberapa metode yang dapat diimplementasikan untuk meningkatkan keamanan autentikasi dan otorisasi pada RESTful API. Secara umum, metode autentikasi dan otorisasi pada RESTful API terbagi menjadi dua jenis utama, yaitu autentikasi berbasis *session* dan autentikasi berbasis *token* (Habibullah, dkk., 2024; Rasyada, 2022). Dibandingkan dengan metode berbasis *session*, metode berbasis token lebih umum diimplementasikan karena beberapa keunggulan yang dimiliki dibandingkan dengan metode berbasis *session*. Adapun keunggulan dari metode berbasis token, diantaranya fleksibilitas algoritma yang dirancang, kemudahan integrasi dengan platform atau sistem lain, dan kompatibilitas yang lebih baik terutama di dalam komunikasi *client-server* (Shikhverdiyev, dkk., 2024).

Salah satu contoh metode autentikasi berbasis token yang populer adalah metode autentikasi berbasis *JSON Web Token* (JWT). Di dalam metode ini, token JWT digunakan sebagai lapisan keamanan tambahan untuk mengakses suatu RESTful API yang terproteksi. Token JWT akan menjadi elemen utama yang harus dikirim ketika sebuah API yang terproteksi diakses sehingga sistem dapat memastikan bahwa API tersebut diakses oleh pengguna yang valid dan autentik

(Purnama, 2023). Dibandingkan dengan metode autentikasi berbasis token lainnya (seperti OAuth 2.0), metode autentikasi berbasis JWT lebih populer digunakan terutama dalam mengoptimalkan keamanan sistem informasi berbasis *enterprise*. Metode autentikasi berbasis JWT memiliki keunggulan pada fleksibilitasnya, dimana algoritma yang dirancang dapat disesuaikan dengan kebutuhan sistem yang akan dibuat. Selain itu, berbeda dengan metode berbasis token lainnya seperti OAuth 2,0, metode berbasis JWT memiliki keunggulan dalam kemudahan konfigurasi karena tidak melibatkan akses pihak ketiga (Matias, dkk., 2024).

Keunggulan-keunggulan tersebut menjadikan metode autentikasi berbasis JWT sebagai metode yang dinamis dan dapat diimplementasikan pada berbagai sistem informasi atau aplikasi. Pada penelitan yang dilakukan oleh Astowo, U. B., & Sujarwo, A. (2023) dalam jurnalnya yang berjudul "Penerapan JSON Web Token sebagai Strategi Pengamanan Data pada Aplikasi MultiMasjid", metode autentikasi JSON Web token digunakan sebagai strategi dalam proses autentikasi dan otorisasi API pada aplikasi MultiMasjid. Pada penelitian tersebut, ketika API untuk *login* diuji dengan data pengguna yang autentik, sistem akan mengirimkan respon berupa token JWT. Token tersebut menjadi elemen autentikasi dan otorisasi untuk API selanjutnya yang terproteksi. Misalnya, Ketika API untuk menampilkan data jamaah diuji dengan menyertakan token JWT tersebut, sistem memberikan respon berupa seluruh data jamaah yang ada di *database*. Tetapi ketika API yang sama diakses tanpa menyertakan token JWT, sistem memberikan respon pesan *unauthorized*. Hal ini mengindikasikan bahwa metode autentikasi berbasis JWT dapat meningkatkan keamanan API sehingga aksesnya terlindungi dari pihak luar yang tidak terautentikasi dan tidak terotorisasi.

Berdasarkan penelitian tersebut, dapat disimpulkan bahwa metode autentikasi yang diimplementasikan menggunakan satu jenis token JWT untuk satu pengguna pada setiap sesinya. Oleh karena itu, dapat disimpulkan juga bahwa satu token JWT yang sama digunakan untuk mengakses API lainnya di dalam aplikasi tersebut (token tunggal). Meskipun metode ini cukup efektif dalam meningkatkan keamanan, tetapi metode autentikasi JWT dengan token tunggal masih memiliki kelemahan. Salah satu kelemahan dari token tunggal adalah tidak adanya batasan waktu terhadap token yang digunakan sehingga selama pengguna masih terhubung

dengan sistem, token tersebut akan tetap valid (Bucko, dkk., 2023). Hal ini dapat meningkatkan risiko terjadinya pencurian token, terutama apabila token disimpan di dalam *cookies* yang tidak terproteksi. *Broken Object Level Authorization* dan *Broken Authorization* salah satunya diakibatkan dari pencurian token ini sehingga API yang seharusnya terproteksi dapat diakses oleh pihak luar dengan menggunakan token dari pengguna yang menjadi korban (Compagna, 2021).

Berdasarkan permasalahan tersebut, penggunaan metode autentikasi berbasis JWT dengan token tunggal masih memiliki kerentanan dalam hal keamanan autentikasi dan autorisasi pada RESTful API yang mengimplementasikannya. Oleh karena itu, penelitian ini akan mengembangkan metode autentikasi dan otorisasi RESTful API berbasis JWT dengan mekanisme token ganda sehingga token yang digunakan tidak hanya satu, melainkan dua jenis token dengan fungsi dan batas waktu (kadaluarsa) yang berbeda. mekanisme token ganda yang dirancang diharapkan dapat meningkatkan keamanan autentikasi dan otorisasi RESTful API yang lebih optimal serta mencegah terjadinya pencurian token. Selain itu pada penelitian ini metode autentikasi dan otorisasi yang dikembangkan juga divariasikan dengan *one time token* sehingga token yang digunakan untuk akses API hanya dapat digunakan satu kali untuk satu aksesnya.

Berdasarkan latar belakang yang telah dijelaskan, penelitian ini diharapkan dapat memberikan konstribusi yang positif terhadap pengembangan keamanan pada RESTful API yang lebih optimal. Oleh karena itu, penelitian ini berfokus untuk mengembangan metode autentikasi dan autorisasi RESTful API berbasis JWT token ganda dengan variasi *one time token*, yang akan diuji ke dalam aplikasi *Product Management* berbasis web. Aplikasi ini dipilih untuk menguji metode yang akan dikembangkan terhadap sistem informasi yang memiliki banyak pengguna dengan role yang berbeda-beda (Abhishek, dkk., 2019)

1.2. Rumusan Masalah Penelitian

Berdasarkan latar belakang yang telah dijelaskan, adapun rumusan masalah di dalam penelitian ini sebagai berikut:

1. Bagaimana mengembangkan metode keamanan RESTful API berbasis JWT token ganda dengan variasi one time token?

2. Bagaimana kinerja dari metode autentikasi dan otorisasi dengan variasi *one time token* seteleh diimplementasikan di dalam RESTful API

1.3. Tujuan Penelitian

Berdasarkan rumusan masalah yang telah dijelaskan, adapun tujuan dari penelitian ini sebagai berikut:

1. Mengembangkan metode keamanan RESTful API berbasis JWT token ganda dengan variasi one time token.
2. Melakukan uji kinerja dari metode autentikasi dan otorisasi dengan variasi *one time token* setelah diimplementasikan di dalam RESTful API

1.4. Manfaat Penelitian

Berdasarkan tujuan penelitian yang telah dijelaskan, diharapkan penelitian ini dapat memberikan kontribusi positif serta bermanfaat dalam pengembangan bidang *Network and Security*, khususnya dalam keamanan RESTful API. Adapun manfaat dari penelitian ini sebagai berikut.

1.4.1. Manfaat Teoritis

Dalam ranah pengembangan keilmuan, penelitian ini diharapkan mampu memberikan kontribusi teoritis yang relevan terhadap studi autentikasi dan otorisasi pada sistem RESTful API. Adapun manfaat teoritis dari penelitian ini sebagai berikut:

1. Melalui perancangan dan pengembangan mekanisme token ganda, penelitian ini dapat memberikan wawasan mengenai metode yang dapat diimplementasikan dalam meningkatkan autentikasi dan otorisasi pada RESTful API.
2. Melalui pengembangan mekanisme token ganda dengan variasi *one time token*, penelitian ini dapat membuka wawasan baru mengenai pengembangan metode autentikasi JWT untuk sistem autentikasi dan otorisasi API yang lebih optimal.
3. Penelitian ini dapat memberikan kontribusi dalam meningkatkan keamanan RESTful API, khususnya pada autentikasi dan otorisasi dengan berbasis JWT.

1.4.2. Manfaat Praktis

Selain memberikan kontribusi secara teoritis, penelitian ini juga memiliki manfaat praktis yang dapat diterapkan dalam pengembangan sistem keamanan API di lingkungan profesional maupun akademik. Adapun manfaat praktis dari penelitian ini sebagai berikut:

1. Bagi praktisi dan professional, rancangan mekanisme token ganda pada penelitian ini dapat diimplementasikan ke dalam pengembangan RESTful API pada sistem informasi berbasis enterprise atau sistem berbasis client-server lainnya untuk keamanan RESTful API yang lebih optimal.
2. Bagi peneliti, melalui penelitian ini peneliti dapat mengimplementasikan ilmu yang diperoleh selama masa kuliah. Peneliti dapat melakukan eksplorasi dan pengembangan terhadap metode yang telah ada sebelumnya agar menghasilkan metode baru yang lebih optimal.

1.5. Ruang Lingkup Penelitian

Berdasarkan tujuan penelitian yang telah dijelaskan, adapun ruang lingkup pada penelitian ini sebagai berikut:

1. Penelitian ini akan fokus pada pengembangan metode keamanan RESTful API berbasis JWT token ganda dengan variasi *one time* token.
2. Algoritma enkripsi yang digunakan dalam membuat token JWT adalah algoritma HMAC SHA256.
3. Aspek yang dievaluasi pada penelitian ini meliputi aspek keamanan, efisiensi, dan kinerja API ketika mekanisme token ganda diimplementasikan.
4. Hasil evaluasi pada aspek efisiensi dari penelitian ini akan dibandingkan dengan sistem autentikasi dan otorisasi RESTful API berbasis JWT yang telah diimplementasikan pada penelitian sebelumnya.
5. Penelitian ini menggunakan aplikasi *product management* berbasis web hanya sebagai studi kasus untuk menguji implementasi metode token ganda pada autentikasi dan otorisasi RESTful API berbasis JWT, tanpa membahas aplikasi secara keseluruhan.

6. Pengembangan mekanisme token ganda dan *enterprise product management information system* sebagai studi kasus dilakukan dengan menggunakan bahasa pemrograman Java dan Spring *framework*.

1.6. Struktur Organisasi Skripsi

Skripsi pada penelitian ini disusun dengan sistematika berdasarkan Pedoman Penulisan Karya Ilmiah Universitas Pendidikan Indonesia 2024. Adapun sistematika pada skripsi ini sebagai berikut.

1. BAB I PENDAHULUAN

   Bab I menjelaskan tentang latar belakang, rumusan masalah, tujuan, dan manfaat dari penelitian yang dilakukan.

2. BAB II TINJAUAN PUSTAKA

   Bab II menjelaskan dasar-dasar konsep dan teori, yang menjadi landasan dari penelitian yang dilakukan. Pada bab ini juga mencekup penelitian-penelitian yang telah dilakukan sebelumnya dan kerangka pemikiran.

3. BAB III METODE PENELITIAN

   Bab III menjelaskan metode serta langkah-langkah yang dilakukan pada penelitian ini. Bab ini mencakup rancangan dari API Web Service serta metode autentikasi dan otorisasi yang akan dikembangkan.

4. BAB IV HASIL DAN PEMBAHASAN

   Bab IV menjelaskan hasil yang diperoleh dari penelitian ini yang mencakup hasil pengembangan API Web Service dan metode autentikasi otorisasi serta hasil pengujian yang telah dilakukan. Pada bab ini juga dijelaskan analisis dari keseluruhan hasil pengujian yang telah dilakukan

5. BAB V KESIMPULAN DAN SARAN

   Bab V menjelaskan kesimpulan berdasarkan hasil yang telah diperoleh dari penelitian ini. Pada bab ini juga dijelaskan saran-saran yang dapat dilakukan untuk pengembangan selanjutnya.