BAB I
PENDAHALUAN

1.1 Latar Belakang

Teknologi terus berkembang pesat dan menjadi dasar dalam kehidupan sehari-hari. Dalam era ini, keterampilan yang lebih tinggi dalam pemanfaatan teknologi menjadi suatu keharusan. Teknologi tidak hanya mempermudah tugas-tugas sehari-hari, tetapi juga dapat meningkatkan produktivitas secara signifikan. Peningkatan produktivitas memiliki dampak positif pada kinerja perusahaan, pendapatan, dan keuntungan, sambil mengurangi biaya operasional. Kemajuan teknologi memudahkan proses kerja, yang pada gilirannya berkontribusi pada pertumbuhan ekonomi dan peningkatan daya saing nasional. Investasi dalam teknologi juga menjadi kunci untuk mengembangkan perusahaan dan industri, menciptakan pasar yang lebih kompetitif dan dinamis. Semua ini mencerminkan dampak positif dari *revolusi* industri 4.0 pada berbagai sektor kehidupan dan bisnis[1]. Semakin berkembang, pertumbuhan yang signifikan dalam pertukaran dan pemanfaatan data telah menimbulkan tantangan serius terkait dengan keamanan dan *privasi*. Data yang disimpan, diproses, dan dikirim melalui aplikasi dan *infrastruktur digital* menjadi rentan terhadap ancaman seperti pencurian data, serangan siber, dan pelanggaran *privasi*. Dampak dari pelanggaran keamanan data dapat mencakup kerugian *finansial*, reputasi yang rusak, dan pelanggaran *privasi individu*[2].

Keamanan data menghadapi risiko serius, di antaranya serangan *Brute Force* yang merupakan metode peretasan dengan mencoba *login* berulang hingga berhasil menebak *password*, baik melalui upaya manual maupun *otomatis*. Hal ini mengatasi keberadaan masalah keamanan yang perlu diperhatikan. Serangkaian hasil serangan menunjukkan seriusnya eksploitasi terhadap keamanan data, dengan peretas berhasil mendapatkan

informasi *login* seperti *username* dan *password*. Peningkatan keamanan data menjadi sangat penting untuk mengatasi proses potensi kerugian[3].

Dengan ini menggunakan JSON Web Token (JWT) dan juga *Two Factor Authentication* (2FA). Dimana, sebuah token dalam format string JSON yang memiliki efisiensi tinggi. JWT digunakan sebagai mekanisme autentikasi dan pertukaran informasi. Struktur JWT terdiri dari tiga segmen yang dibedakan oleh tanda titik (.), yaitu *header*, *payload*, dan *signature*[4]. *Header* berisi informasi *algoritme* dan jenis token yang dienkripsi menggunakan *base*64. *Payload*, bagian kedua, mengandung data yang dikirim melalui token dan juga dienkripsi dengan *base*64. Biasanya, *payload* berisi informasi autentikasi seperti *email*, ID, dan data otorisasi seperti peran pengguna. Bagian ketiga, *signature*, adalah nilai hash gabungan dari *header*, *payload*, dan *secret-key* yang harus dirahasiakan[5]. Selain itu, *Two Factor Authentication* (2FA) adalah metode ganda yang umumnya digunakan untuk meningkatkan keamanan sistem. Pendekatan 2FA ini bersifat ramah pengguna dan melibatkan penggunaan dua lapisan *otentikasi*, seperti kata sandi. Tujuan keamanan komputer, yaitu menjaga *integritas*, ketersediaan, dan *privasi* informasi yang dipercayakan kepada sistem, dapat dicapai dengan menerapkan teknik otentikasi ini[6]. *One Time Pad* (OTP) adalah jenis algoritma *simetris* yang ditemukan oleh *Major Joseph Maugborne* dan *Gilbert Vernam* pada tahun 1917. Setiap kunci hanya digunakan untuk satu pesan, sehingga keamanannya lebih tinggi. Dalam konteks keamanan percakapan *WhatsApp*, penggunaan *One Time Pad* bersama *dengan Two Factor Authentication* (2FA) meningkatkan tingkat keamanan dengan pengamanan ganda[7].

Dengan demikian, peneliti mendapatkan isu keamanan pada tahap *login*, yang merupakan dasar dalam perlindungan data dengan nama Cat Point. Penelitian ini berjudul " PENERAPAN JSON WEB TOKEN (JWT) DAN TWO FACTOR AUTHENTICATION PADA API SISTEM PENITIPAN KUCING" bertujuan meningkatkan keamanan *login* dan melindungi data sensitif. Selain itu, penelitian ini juga akan menerapkan

two-factor authentication menggunakan *one-time password* (OTP) melalui *WhatsApp*. Langkah ini diharapkan dapat menambah lapisan keamanan, meningkatkan keamanan sistem, dan melindungi integritas data, sehingga hanya pengguna yang melewati dua faktor otentikasi yang dapat mengakses sumber daya sensitif di API Sistem Penitipan Kucing.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan di atas, permasalahan utama dalam penelitian ini mencakup kebutuhan akan peningkatan integritas, kerahasiaan, dan keaslian token JWT pada *backend* sistem informasi. Dalam rangka mengatasi tantangan ini, penelitian akan memfokuskan *implementasi* JWT sebagai lapisan keamanan *login* secara menyeluruh. Selain itu, penelitian ini juga mengeksplorasi *solusi two-factor authentication* (2FA) dengan menggunakan *one-time password* (OTP) yang disalurkan melalui *WhatsApp*. Dengan demikian, peningkatan keamanan tidak hanya terfokus pada token JWT, tetapi juga mencakup aspek keamanan tambahan melalui 2FA menggunakan OTP melalui *WhatsApp*.

1.3 Pertanyaan Penelitian

Berdasarkan rumusan masalah diatas, maka pertanyaan peneliti dalam melakukan penelitian ini yaitu:

1. Bagaimana langkah-langkah dalam merencanakan dan menerapkan JWT pada API *login* dengan sebuah keamanan, dengan mengambil contoh studi kasus Cat Point di Purwokerto Utara?
2. Bagaimana penerapan *two-factor authentication* (2FA) dalam sistem pendaftaran penitipan kucing melalui *website* dengan keamanan proses pendaftarannya?

1.4 Batasan Masalah

Dari perumusan masalah dan tujuan penelitian, batasan-batasan penelitian diperoleh untuk memastikan kesesuaian penelitian dengan permasalahan yang ada, sebagai berikut:

1. Penelitian ini akan mengeksplorasi kebijakan waktu token dengan tujuan menjaga keamanan sistem dan mengurangi potensi risiko yang mungkin muncul karena penggunaan token yang sudah melewati batas waktu berlakunya.
2. Penelitian ini menerapkan metode *extreme programming* untuk JWT pada API dalam kebutuhan sistem keamanan pada login.

1.5 Tujuan Penelitian

Berdasarkan rumusan masalah, mendapatkan tujuan penelitian Penelitian ini bertujuan untuk:

1. Meningkatkan keamanan *backend* sistem informasi dengan fokus pada token JSON Web Token (JWT). Permasalahan utama yang ingin diatasi meliputi integritas, kerahasiaan, dan keaslian token JWT pada sistem informasi. Selain itu, penelitian ini juga bertujuan untuk mengimplementasikan JWT sebagai lapisan keamanan *login* secara menyeluruh, mencakup aspek-aspek keamanan yang dibutuhkan dalam mengelola akses ke sistem.
2. Menjelajahi dan menerapkan solusi *two-factor authentication* (2FA) dengan menggunakan *one-time password* (OTP) yang disalurkan melalui *WhatsApp*. Penambahan elemen 2FA diharapkan dapat memberikan lapisan keamanan tambahan dalam proses otentikasi, yang pada gilirannya dapat meningkatkan tingkat keamanan secara keseluruhan. Secara keseluruhan, tujuan utama penelitian ini adalah menyediakan solusi yang kokoh dan menyeluruh untuk menjaga keamanan akses ke *backend* sistem informasi.

1.6 Manfaat Penelitian

Berdasarkan rumusan masalah, batasan masalah dan tujuan penelitian yang telah diuraikan diatas, maka dapat diketahui manfaat dari penelitian ini adalah:

1. Penelitian membantu untuk memperoleh pemahaman yang mendalam tentang konsep dan prinsip keamanan *login* terkait dengan JWT. Ini mencakup pemahaman tentang mekanisme kerja JWT, bagaimana cara membuat, memverifikasi, dan menggunakan token.
2. Penelitian ini bertujuan untuk mengidentifikasi dan memahami *implementasi two factor authentication*(2FA) pada sistem penitipan kucing melalui penerapan metode *extreme programming*.