BAB I

PENDAHULUAN

1.1 Latar Belakang

Pada era perkembangan teknologi seperti saat ini, sistem informasi dan komunikasi memberikan manfaat dan kemudahan dalam kehidupan sehari-hari. Diantaranya adalah untuk mendapatkan informasi yang akurat, menentukan keputusan, ataupun memecahkan suatu permasalahan. Untuk bisa melakukan komunikasi jarak jauh (Telekomunikasi) maka memerlukan teknologi Internet dalam pengiriman pesan dan pertukaran data. Sistem informasi dan komunikasi saat ini semakin berkembang dengan pesat, dan banyak terdapat data-data penting didalamnya, maka dari itu diperlukannya sistem pengamanan agar keamanan data pada sistem informasi dan komunikasi tersebut terjaga, sehingga dapat mencegah hal-hal yang tidak diinginkan terjadi seperti, pencurian data, perusakan pada data, dan memanipulasi data.

Sistem informasi tentunya sangat menguntungkan dan dapat meningkatkan kinerja diberbagai komponen organisasi, akan tetapi di sisi lain Sistem Informasi yang berbasis web sangat rawan untuk disadap oleh pihak yang tidak berwenang. Banyak *hacker* yang melakukan segala cara untuk mendapatkan *username* dan *password* pada suatu akun (*Account*). Akun yang dimaksud ini dapat berupa akun apa saja diantaranya akun email, akun media sosial, akun messenger, dan akun berbasis web lainnya.

JSON Web Token (JWT) dapat menjadi solusi menggantikan username dan password. JWT adalah token berbentuk string panjang random yang gunanya untuk melakukan autentikasi system dan pertukaran informasi. JWT mengamankan informasi menjadi sebuah klaim yang di encode ke dalam bentuk JSON dan menjadi payload dari JSON Web Signature (JWS) (Bradley, 2015). Alasan penggunaan autentikasi JWT yang berbasis token adalah adanya expiration. Ukuran JWT yang kecil memungkinkannya dapat dikirimkan melalui URL, parameter HTTP POST, atau header HTTP POST. Token disimpan disisi klien sebagai

cookies sehingga server tidak harus meyimpan token. Karena token sudah ditandatangani secara digital maka dapat diketahui siapa yang melakukan request, karena isi dari tanda tangan pada JWT merupakan gabungan dari isi header dan payload, jika terjadi perubahan maka signature akan menjadi tidak valid.

Setelah melihat dan mengamati permasalahan tersebut maka penulis tertarik untuk merancang dan mengambil topik laporan akhir ini dengan judul ***"Implementasi Sistem Pengamanan Autentikasi Akses Web Pada Website Arsip Politeknik Negeri Sriwijaya dengan JSON Web Token (JWT)"*** dimana penulis akan membuat sebuah website arsip sebagai sarana mahasiswa mengumpulkan tugas kepada dosen secara daring yang proses autentikasinya dilindungi oleh *username* dan *password* untuk menjamin keamanan data yang ada didalamnya menggunakan algoritma kriptografi dengan teknik yang dinamakan *JSON Web Token*.

1.2 Perumusan Masalah

Adapun berdasarkan latar belakang masalah yang telah diuraikan sebelumnya, maka penulis mengemukakan rumusan masalah sebagai berikut:

1. Bagaimana cara membuat website arsip dengan berbagai fitur pengguna?
2. Bagaimana cara membuat sistem pengamanan dan membatasi sebuah akses web dengan menggunakan algoritma *JSON Web Token*?
3. Bagaimana prinsip kerja dari metode *JSON Web Token* yang diterapkan pada website arsip?
4. Apakah *website* arsip dapat beroperasi dengan baik di *Smartphone* Android dan IOS maupun PC / Laptop?
5. Bagaimana tingkat keamanan *website* setelah menggunakan sistem pengamanan *JSON Web Token*?

1.3 Pembatasan Masalah

Dalam penulisan laporan akhir ini penulis hanya membahas mengenai hal-hal sebagai berikut:

1. Penulis hanya membahas keunggulan dan kelemahan *JSON Web Token* dibandingkan dengan metode lain pada umumnya seperti *Simple Web Token* (SWT) dan *Security Assertion Markup Language Tokens* (SAML) yang bisa juga digunakan untuk mengamankan akses web.
2. Fitur-fitur yang terdapat di website arsip memungkinkan pengguna untuk membuat pengumuman, mengupload file, dan mengirim file langsung ke email.
3. Sistem autentikasi pada website hanya menggunakan *JSON Web Token* saja yang bekerja pada saat *user* memasukkan *username* dan *password*.

1.4 Tujuan dan Manfaat

1.4.1 Tujuan

Tujuan yang ingin dicapai dari pembuatan aplikasi ini adalah

1. Membuat website arsip yang proses autentikasinya menggunakan algoritma *JSON Web Token*.
2. Mengembangkan sistem arsip yang dapat membantu mahasiswa dan dosen dalam mengumumkan atau mengumpulkan tugas secara online.

1.4.2 Manfaat

Adapun manfaat dari pembuatan aplikasi ini adalah penulis dapat mengenal unsur-unsur dasar kriptografi, dimana penerapannya adalah pada suatu website yang memiliki sistem autentikasi dan pengaksesan yang terbatas. Penulis juga dapat mempelajari tentang *JSON Web Token* serta mekanisme kerjanya dalam melindungi akun dan data yang terdapat dalam suatu website.

1.5 Metodologi Penulisan

Untuk metode penyusunan Laporan Akhir ini penulis menggunakan metode penulisan sebagai berikut:

a. **Metode Studi Pustaka**

   Melakukan metode pengumpulan materi atau data tentang peran dan cara kerja perangkat lunak dan sistem operasi yang akan digunakan, yang berasal dari jurnal, buku, artikel, dan referensi lain.

b. **Metode Observasi Eksperimental**

   Melakukan pengamatan simulasi dengan mencoba mengenkripsi dan deskripsi algoritma menggunakan metode *JSON Web Token.*

c. **Metode Konsultasi**

   Metode konsultasi, bertanya serta meminta masukan kepada dosen pembimbing dalam menyelesaikan laporan.

d. **Metode Diskusi**

   Melakukan diskusi dan wawancara dengan rekan-rekan yang ahli di bidang program aplikasi berbasis web.

e. **Metode Cyber**

   Mencari informasi dan data yang ada kaitannya dengan masalah yang dibahas dari internet sebagai bahan referensi laporan.

1.6 Sistematika Penulisan

Untuk mempermudah dalam penyusunan laporan akhir yang lebih jelas dan sistematis maka penulis membaginya dalam sistematika penulisan yang terdiri dari beberapa bab pembahasan dengan urutan sebagai berikut:

BAB I **PENDAHULUAN**

Bab ini menjelaskan latar belakang dan alasan pemilihan judul, tujuan penulisan, pembatasan masalah, metodelogi dan sistematika penulisan.

BAB II **TINJAUAN PUSTAKA**

Bab ini menguraikan tentang landasan teori yang mendukung dan mendasari cara kerja dari aplikasi yang akan digunakan.

BAB III RANCANGAN SISTEM APLIKASI

Bab ini menjelaskan tentang proses pembuatan aplikasi yang dibuat, *flowchart*, blok diagram, instalasi, tahapan-tahapan membuat aplikasi.

BAB IV PEMBAHASAN

Bab ini akan membahas tentang cara kerja pembuatan aplikasi dan Analisa aplikasi yang dirancang.

BAB V KESIMPULAN DAN SARAN

Bab ini merupakan bagian akhir dari laporan yang berisi tentang kesimpulan dari pembuatan rancangan sistem aplikasi dan saran yang perlu diperhatikan berdasarkan keterbatasan yang ditemukan dan asumsi-asumsi yang dibuat selamat pembuatan aplikasi.