BAB I

PENDAHULUAN

1.1 Latar Belakang

Teknologi informasi terus berkembang dan memberikan pengaruh besar terhadap organisasi maupun individu. Perkembangan teknologi bertujuan untuk memenuhi kebutuhan bagi pemakai. Salah satu teknologi tersebut adalah *Web Service* (*WS)*. Perkembangan bisnis saat ini sangat memerlukan *WS* dalam integrasi sistem karena *WS* dapat bekerja tanpa melihat *platform*, arsitektur maupun bahasa pemrograman yang digunakan oleh sumber berbeda.

Web Service (*WS*) merupakan suatu bentuk perkembangan dari teknologi saat ini yang dapat digunakan untuk integrasi sistem, terutama dalam lingkungan bisnis. Menurut Vasco dan Dustar dalam (Tanaem,dkk.,2016) bahwa manfaat membangun sebuah *WS* untuk kebutuhan bisnis yang berkembang dari waktu ke waktu yaitu untuk meningkatkan jumlah integrasi dan fleksibilitas, untuk pengembangan demi kepentingan dalam mengintegrasikan *service* ke dalam pendekatan manajemen dan proses bisnis yang ada. Keamanan *WS* berada kedalam 10 kerentanan teratas dalam keamanan *Web Application* yang kurang diperhatikan menurut *The Open Web Application Security Project (OWASP). (OWASP, 2017).*

Bentuk nyata dari perkembangan *WS* yaitu hadirnya beberapa *WS* saat ini diantaranya yaitu *Representational State Transfer* (*REST)* atau juga dikenal dengan *RESTful WS*. Menurut Vibha (Kumari,2015) *RESTful* berada pada posisi teratas dalam *protocol* yang sering dipakai dibanding *protocol-protocol* lain. *RESTful* memiliki kinerja yang lebih baik karena dapat menggunakan

berbagai format data diantaranya yaitu *JSON* yang menjadikan proses lebih cepat dan ringan. Kutipan Meng dalam jurnal (Tanaem, dkk., 2016) bahwa *RESTFul WS* sangat baik dalam mengoptimalkan kinerja ketika *RESTFul* diakses dalam skala cukup besar. Keamanan *RESTFul* merupakan salah satu poin penting yang harus diperhatikan. Pengamanan yang dibutuhkan harus mencakup pengamanan data, serta seluruh komunikasi untuk melindungi kerahasiaan dan integritas data. Langkah yang dapat dilakukan dalam mengatasi permasalahan tersebut yaitu dengan menggunakan *JSON Web Token* (*JWT*). *JWT* mendefinisikan cara yang simpel dan independen dari transmisi informasi yang aman antar setiap pihak menggunakan format data objek yang ditransmisikan dengan aman dan dapat diverifikasi karena menggunakan *digital signature. Digital signature JWT* dapat menggunakan kunci rahasia (dengan algoritma *HMAC*) atau sepasang kunci publik dan privat menggunakan *RSA*.

Penelitian (Tanaem, dkk, 2016) bahwa telah diimplementasikan *JWT* dengan algoritma *HMAC SHA*-256 yang masih umum digunakan, sehingga dapat menjadi ancaman tersendiri bagi *RESTful WS*. Penelitian (Rahmatulloh, dkk, 2018) bahwa telah dilakukan uji coba mengenai performa antara *SHA*-256 dan *SHA*-512 di mana *SHA*-256 dan *SHA*-512 menggunakan *symmetric key*.

Penelitian (Lamberger, 2011) menemukan *pseudo-collision attack* pada algoritma SHA-256. Serangan ini dapat juga dilakukan pada SHA-512 yang memiliki struktur yang sama. Penelitian (Khovratovich, dkk, 2011) ditemukan konsep *bicliques* dalam *preimage attacks*. *Bicliques* memiliki potensi besar

dalam serangan pada fungsi *hash* dan *block-chiper*. Konsep ini diuji coba pada algoritma *SHA*-2, yaitu *SHA*-256 dan *SHA*-512. Serangan-serangan ini memungkinkan algoritma *SHA*-256 dan *SHA*-512 dinyatakan tidak aman dan tidak dapat digunakan untuk kedepannya. Penelitian (Oku, dkk, 2018) menghasilkan serangan *Scan-based Side-chanel* yang telah mampu mencuri *secret key* pada *HMAC-SHA*-256 dalam waktu relatif singkat. Hasil ini tentunya menjadi ancaman tersendiri pada *HMAC-SHA*-512 yang menggunakan *symmetric key* seperti *HMAC-SHA*-256

Penelitian kali ini akan dilakukan penelitian mengenai implementasi *JSON Web Token* dengan algoritma *asymmetric RSA*-512 pada arsitektur *RESTful WS* sederhana sebagai alternatif dari algoritma *symmetric SHA*-256 dan *SHA*-512.

1.2 Rumusan Masalah

Berdasarkan uraian pada latar belakang, maka rumusan masalah dari penelitian ini adalah :

1. Bagaimana implementasi *JWT* dengan algoritma *asymmetric RSA*-512 pada arsitektur *RESTful*?
2. Bagaimana hasil proses otentikasi menggunakan *JWT* dengan algoritma *asymmetric RSA*-512 pada arsitektur *RESTful*?

1.3 Batasan Masalah

Batasan pada penelitian ini adalah:

1. Implementasi *JWT* dengan algoritma *asymmetric RSA*-512 dilakukan pada *prototype* arsitektur *RESTful WS* sederhana.
2. Pengujian dilakukan pada *server localhost*.

1.4 Tujuan Penelitian

Tujuan penelitian ini adalah:

1. Mengetahui implementasi *JWT* dengan algoritma *asymmetric RSA*-512 pada arsitektur *RESTful.*
2. Mengetahui hasil proses autentikasi menggunakan *JWT* dengan algoritma *asymmetric RSA*-512 pada arsitektur *RESTful.*

1.5 Manfaat Penelitian

Manfaat penelitian ini adalah:

1. Hasil penelitian ini dapat dijadikan ilmu pengetahuan baru mengenai implementasi mekanisme autentikasi menggunakan *JWT* dengan algoritma *asymmetric RSA-512*.
2. Hasil penelitian ini dapat dijadikan sebuah alternatif pilihan bagi masyarakat dalam membuat mekanisme autentikasi menggunakan *JWT*.

1.6 Metodologi Penelitian

Metodologi penelitian dalam penelitian ini, peneliti membagi menjadi beberapa tahap pengerjaan yang digunakan sebagai acuan dalam penyelesaian

penelitian hingga pembuatan laporan akhir. Tahap-tahap dalam melakukan penelitian ini adalah sebagai berikut:

1. Studi literatur

   Tahap ini dilakukan dengan informasi terkait beberapa hal berikut:

   A. Pengumpulan informasi tentang bagaimana cara membangun *JWT* pada arsitektur *RESTful WS*.

   B. Pengumpulan informasi tentang bagaimana algoritma *asymmetric RSA*-512 yang akan diterapkan pada *JWT*.

   C. Pengumpulan informasi tentang bagaimana cara melakukan *parsing* data *JWT* untuk menguji performa algoritma yang diterapkan pada *JWT*.

2. Perancangan *Prototype*

   Tahap ini mengimplementasikan *JWT* menggunakan algoritma *RSA*-512 pada *RESTful WS* sederhana.

3. Pengujian

   Tahap pengujian dilakukan dengan melakukan uji coba terhadap mekanisme *JWT* dengan algoritma *asymmetric RSA*-512 yang diterapkan pada *RESTful WS* sehingga didapatkan data-data yang dibutuhkan.

4. Analisis

   Tahap analisis dilakukan dengan analisis terhadap data yang dihasilkan pada tahap pengujian.

1.7 Sistematik Penulisan

Sistematika penulisan yang digunakan dalam laporan tugas akhir ini adalah sebagai berikut:

BAB I PENDAHULUAN

Bab ini berisi pembahasan masalah umum, yang merupakan gambaran secara garis besar tentang isi laporan, yang didalamnya memuat latar belakang dilakukannya penelitian, rumusan masalah, batasan permasalahan pada penelitian, tujuan penelitian, manfaat penelitian, metode penelitian dan sistematika penulisan laporan tugas akhir.

BAB II LANDASAN TEORI

Bab ini berisi pembahasan teori - teori yang yang saling berhubungan dengan penelitian dan pembuatan sistem. Mulai dari penjabaran mengenai metode yang digunakan dan teori lainnya yang saling berhubungan serta ulasan mengenai penelitian – penelitian sebelumnya.

BAB III METODOLOGI

Bab ini menjelaskan tentang perencanaan implementasi *JWT* dengan algoritma *RSA-512* pada *RESTful WS*. Dilakukan beberapa tahapan yaitu studi literatur, perancangan *prototype*, pengujian, dan analisis.

BAB IV HASIL DAN PEMBAHASAN

Bab ini menjelaskan hasil analisis terhadap perancangan pada bab sebelumnya, yaitu rancangan yang sesuai dengan metodologi dan implementasi pada sistem yang telah dibuat, dan dilakukan pula pengujian dan perbandingan untuk mendapatkan hasil yang sesuai dengan tujuan awal penelitian.

BAB V KESIMPULAN DAN SARAN

Bab ini merupakan bab akhir dari penulisan laporan yang berisi mengenai simpulan yang merupakan hasil analisis pada bagian sebelumnya serta saran yang perlu diperhatikan berdasarkan keterbatasan yang ditemukan dan asumsi-asumsi yang dibuat selama penelitian.