

BAB I

PENDAHULUAN

1.1. Latar Belakang

Teknologi *websocket* berkembang sebagai salah satu metode komunikasi yang layak dipertimbangkan untuk membangun aplikasi yang membutuhkan komunikasi *realtime*. Teknologi ini sering dipertimbangkan sebagai sebuah alternatif metode komunikasi karena memiliki keunggulan dibandingkan dengan komunikasi *request-respon* biasa seperti *Hyper Text Transfer Protocol* (HTTP) yang ada saat ini. Keunggulan-keunggulan tersebut antara lain adalah komunikasi *realtime* dan dapat mengurangi tingkat keterlambatan pengiriman pesan dari pengirim ke penerima (*Latency*) [1]. Teknologi *websocket* diperkenalkan pada bulan September 2012. *websocket* dirancang untuk dapat diimplementasikan pada *web browser* dan *web server* juga dapat digunakan untuk keperluan-keperluan lainnya seperti pada aplikasi *instant messaging* berbasis Android [2].

Meskipun teknologi *websocket* belum dibakukan, namun diharapkan bahwa penggunaan teknologi *websocket* akan meningkat secara signifikan dalam waktu dekat [2]. Dengan fitur komunikasi *full-duplex* tidak menutup kemungkinan akan sangat banyak aplikasi-aplikasi yang akan memanfaatkan *websocket* sebagai teknologi komunikasi mereka. Fitur-fitur *websocket* akan sangat lebih efektif diterapkan pada aplikasi yang membutuhkan waktu respon cepat seperti *instant messaging*, *game realtime* dan pengiriman data multimedia [1].

Namun dengan menerapkan teknologi *websocket* ancaman keamanan akan lebih kongkrit, seperti serangan *pasif monitoring packet*. Karena teknologi *websocket* tidak sepenuhnya menangani masalah komunikasi secara keseluruhan melainkan hanya masalah konektivitas, tidak dalam masalah keamanan. Teknologi *websocket* tidak menyediakan mekanisme keamanan seperti autentikasi koneksi atau enkripsi pesan [3]. Oleh karena itu aplikasi yang memanfaatkan teknologi *websocket* akan sangat rentan terhadap serangan seperti *sniffing* dan lainnya yang dilakukan oleh pihak-pihak yang tidak berkepentingan.

Berdasarkan permasalahan teknologi *websocket* di bidang keamanan, maka akan dilakukan penerapan metode enkripsi untuk mengamankan aliran data pada jalur komunikasi protokol *websocket* yang akan digunakan untuk mengirimkan pesan dari aplikasi *instant*



messaging. Sehingga dengan diterapkannya metode enkripsi, nantinya pesan yang dikirimkan akan lebih sulit untuk dibaca oleh penyerang atau *cracker*. Dengan adanya metode enkripsi kerahasiaan pesan dari aplikasi *instant messaging* yang dikirimkan melalui protokol *websocket* akan lebih aman dan terjaga kerahasiaannya.

Pada penelitian ini digunakan algoritma *Rivest Code 6* (RC6) sebagai metode untuk penyandian paket data *websocket* atas dasar dari berbagai pertimbangan yang telah dilakukan yang diantaranya adalah algoritma RC6 memiliki performa yang bagus dalam proses penyandian. Hal ini karena algoritma RC6 penggunaan operasi-operasi primitif yang telah diimplementasikan secara efisien pada prosesor modern. Algoritma RC6 juga mengadopsi tiga operasi primitif yang digunakan dalam RC5, juga menggunakan operasi perkalian 32-bit yang telah dapat diimplementasikan pada prosesor modern saat ini. Operasi primitif ini sangat efektif untuk menghasilkan efek “*diffusion*” atau efek penyebaran yang lebih efisien, operasi tersebut mengakibatkan algoritma RC6 menjadi lebih aman dibandingkan dengan RC5, serta operasi perkalian tersebut digunakan untuk menghitung jumlah bit yang dirotasi sehingga konsep *data-dependent rotations* dapat diimplementasikan dengan lebih sempurna oleh algoritma RC6 [4]. Berdasarkan uraian-uraian tersebut, maka algoritma RC6 akan diterapkan sebagai algoritma untuk penyandian paket data pada protokol *websocket*.

Dengan menerapkan metode enkripsi *Rivest Code 6* (RC6) diharapkan aliran data pada jalur komunikasi protokol *websocket* yang akan digunakan untuk mengirimkan pesan dari aplikasi *instant messaging* mengalami proses penyandian, sehingga pesan rahasia lebih sulit untuk dimengerti maknanya oleh pihak selain pengirim dan penerima juga terjaga keaslian dan kerahasiaan pesan tersebut.

1.2. Perumusan Masalah

Berdasarkan latar belakang yang telah dipaparkan diatas, maka di dapat rumusan masalah yaitu :

1. Seberapa baik performa kecepatan algoritma *Rivest Code 6* (RC6) dibandingkan dengan *Transport Layer Security* (TLS) dalam mengirimkan pesan melalui protokol *websocket*?
2. Seberapa aman metode enkripsi *Rivest Code 6* (RC6) dibandingkan dengan *Transport Layer Security* (TLS) dalam mengamankan data yang dikirimkan melalui protokol *websocket*?



3. Seberapa baik *websocket* hasil modifikasi dalam mengirimkan pesan pada jaringan dengan kondisi *packet loss*?

1.3. Tujuan dan Manfaat

Adapun tujuan dan manfaat dari penelitian yang akan dilakukan adalah sebagai berikut:

1.3.1. Tujuan

Adapun tujuan yang ingin dicapai dalam penelitian ini adalah untuk mengetahui pengaruh metode enkripsi terhadap performa dan keamanan protokol *WebSocket* dalam pengiriman pesan dari aplikasi *instant messaging* berbasis Android.

1.3.2. Manfaat

Manfaat dari penelitian ini terbagi menjadi dua, yaitu manfaat secara teoritis dan manfaat secara praktis diantaranya :

1.3.2.1 Manfaat Teoritis

Hasil penelitian ini diharapkan dapat memberikan kontribusi keilmuan dalam bidang keamanan data, khususnya yang berkaitan dalam pengamanan data pada protokol *websocket*.

1.3.2.2 Manfaat Praktis

1. Bagi pengguna, dengan adanya jalur komunikasi yang aman, dapat membantu pengguna untuk mengamankan pesan rahasia mereka.
2. Bagi *developer*, hasil penelitian ini dapat digunakan sebagai acuan untuk membangun aplikasi *instant messaging* dengan jalur komunikasi yang aman.
3. Bagi peneliti selanjutnya, hasil penelitian ini dapat digunakan sebagai bahan referensi untuk pengembangan lebih lanjut melalui kegiatan penelitian selanjutnya yang berkaitan dengan konteks bidang keamanan data.

1.4. Batasan Masalah

Pada penelitian ini terdapat beberapa batasan masalah yang diambil diantaranya sebagai berikut :

1. Protokol *websocket* yang digunakan adalah versi RFC 6455.
2. Bahasa pemrograman yang digunakan adalah *java*.
3. Proses enkripsi dilakukan pada *payload* pada *frame websocket*.
4. Data yang di enkripsi berupa *byte*.
5. Kunci enkripsi ditetapkan pada saat implemtasi *websocket*, baik dari sisi *server* maupun *client*.



6. Panjang kunci enkripsi yang digunakan adalah 16 *byte*.
7. Aplikasi *server messaging* berbasis java.
8. Aplikasi *client messaging* berbasis Android.
9. Pengujian dilakukan di jaringan *wifi* lokal.

1.5. Metodologi Penelitian

1.5.1. Tahap Pertama (Studi Pustaka)

Pada tahap ini akan dilakukan pengumpulan informasi yang dibutuhkan. Informasi didapat dari membaca jurnal ilmiah, penelitian, paper, buku serta mencari informasi melalui media internet yang berkaitan dengan permasalahan.

1.5.2. Tahap Kedua (Perancangan Sistem)

Pada tahap ini dilakukan perancangan sistem yang dibangun dengan mengacu pada hasil pemahaman dan studi pustaka.

1.5.3. Tahap Ketiga (Implementasi)

Pada tahap ini dilakukan implementasi sistem ke dalam suatu program sesuai dengan rancangan sistem.

1.5.4. Tahap Keempat (Uji Coba)

Pada tahap ini dilakukan uji coba terhadap *library websocket* hasil modifikasi yang telah dibuat. Pengujian ini bertujuan untuk mengetahui kecepatan pengiriman pesan dan tingkat keamanan metode enkripsi *Rivest Code 6 (RC6)* yang telah diimplementasikan pada *library websocket*.

1.5.5. Tahap Kelima (Penyusunan Laporan)

Pada tahap ini penulis akan melakukan penulisan laporan dari hasil yang telah didapat pada proses analisa sampai pada pengujian dari penelitian yang dilakukan.

1.6. Sistematika Penulisan

Secara garis besar. Sistematika penulisan laporan Tugas Akhir ini adalah sebagai berikut :

BAB I PENDAHULUAN

Bab ini berisikan latar belakang, rumusan masalah, tujuan dan manfaat, batasan masalah, metodologi penelitian, dan sistematika penulisan.



BAB II STUDI PUSTAKA

Pada bab studi putaka dijelaskan mengenai materi-materi yang menjadi dasar pedoman penyusunan penelitian ini.

BAB III PERANCANGAN SISTEM

Bab perancangan sistem dijelaskan mengenai alur dari sistem yang dirancang setelah melakukan analisa permasalahan.

BAB IV IMPLEMENTASI SISTEM

Bab ini menjelaskan implementasi sistem yang telah dilakukan pengkodean sesuai dengan rancangan sistem untuk menambahkan *Rivest Code 6 (RC6)* sebagai algoritma penyandian paket pada *library websocket* serta hasil pengujian kecepatan dan *avalanche effect*.

BAB V PENUTUP

Bab penutup berisi kesimpulan dari hasil uji coba sistem dan saran untuk pengembangan penelitian selanjutnya



[HALAMAN INI SENGAJA DI KOSONGKAN]

