BAB I

PENDAHULUAN

I.1. Latar Belakang

Perkembangan teknologi informasi yang begitu cepat berpengaruh besar pada kehidupan manusia. Teknologi mengubah cara hidup baik untuk melakukan *latency* pada transmisi data terenkripsi di protokol *websocket*. Teknologi mengalami perubahan yang sangat cepat untuk mendukung kebutuhan manusia.

Salah satu protokol *Websocket* menyediakan layanan koneksi yang sangat efektif, mengurangi *latency* dan *traffic* jaringan. *Websocket* menjadi solusi yang tepat untuk layanan *web* yang membutuhkan koneksi *real-time*. Protokol yang menekankan pada keterlambatan paket data dari pada kehilangan paket data, Sedangkan UDP merupakan protokol yang bersifat connection lessoriented. Artinya, saat melakukan pengiriman data tidak dilakukan proses handshaking, tidak ada sequencing datagram, dan tidak ada garansi bahwa paket data (datagram) yang dikirim akan tiba dengan selamat.

RC4 dan RC6 keduanya adalah algoritma cipher kunci simetri. Perbedaan mendasar dari keduanya hanyalah pada algoritma yang diimplementasikan. Keduanya memiliki sifat- sifat umum algoritma block cipher, yaitu memiliki fungsi enkripsi dan dekripsi yang diaplikasikan pada 1 blok data dan menghasilkan 1 blok data hasil pemrosesan latency pada transmisi data terenkripsi.

Oleh karena itulah, penulis terdorong dan berinisiatif untuk mengambil judul **"Analisis Perbandingan Latency Pada Transmisi Data Terenkripsi di Protokol Websocket Dengan Algoritma RC4 Dan RC6"** dalam penyusunan skripsi ini.

I.2. Ruang lingkup Permasalahan

Adapun beberapa tahap yang dilakukan dalam membuat ruang lingkup permasalahan adalah :

I.2.1. Identifikasi Masalah

Berdasarkan penelitian penulis sehubungan dengan materi yang penulis diangkat dalam skripsi ini, penulis menemukan beberapa masalah antara lain :

1. Rentannya latency pada data terenkripsi di protokol websocket yang bersifat pribadi, sehingga perlu dicari perbandingannya.
2. Pendefenisian dan pengenalan karakteristik algoritma RC4 dan RC6 protokol websocket yang terenkripsi.
3. Server juga tidak dapat langsung melakukan transmisi data ke klien tanpa ada permintaan terlebih dahulu.

I.2.2. Rumusan Masalah

Berikut rumusan masalah yang akan dicari pemecahannya melalui penulisan skripsi ini :

1. Bagaimana merancang aplikasi websocket yang dapat terenkripsi untuk keamanan transmisi data ?

2. Bagaimana pendefenisian dan pengenalan karakteristik data terenkripsi di protokol websocket menggunakan algoritma RC4 dan RC6 ?
3. Bagaimana mempermudah penerapan perbandingan metode yang terlatency pada data terenkripsi ?

I.2.3. Batasan Masalah

Adapun batasan masalah yang penulis berikan dalam pembuatan skripsi ini adalah sebagai berikut :

1. Perancangan aplikasi perbandingan latency pada data terenkripsi yang menggunakan algoritma RC4 dan RC6 pada websocket.
2. Aplikasi dibangun menggunakan pemrograman *Javascript.*
3. Pemodelan perancangan aplikasi menggunakan *Unified Modeling Language* (UML) 2.0.
4. Data yang digunakan hanya berkas *plaintext* (.txt)
5. Parameter pengukuran perbandingan hanya berfokus pada besaran *latency* pada proses transmisi data.
6. Jalur transmisi data yang digunakan adalah jenis *multicast*.

I.3. Tujuan Dan Manfaat

Tujuan dan manfaat yang penulis peroleh dari penelitian skripsi ini adalah sebagai berikut :

I.3.1. Tujuan

Tujuan yang ingin dicapai melalui penulisan skripsi ini adalah sebagai berikut:

1. Merancang aplikasi pada protokol websocket untuk mengetahui data yang terenkripsi.
2. Merancang aplikasi untuk melakukan latency pada data dengan menggunakan algoritma.
3. Merancang aplikasi yang dapat menyampaikan informasi secara *real-time* yang terhubung dengan jaringan menggunakan aplikasi ini.

I.3.2. Manfaat

Manfaat yang diharapkan dari penulisan skripsi ini adalah :

1. *User* dapat langsung mengenkripsi data di protokol websocket ke *user* lainnya.
2. Hasil akhir data dapat disimpan langsung di dalam memori penyimpanan, sehingga tidak perlu penduplikasian secara manual.
3. Memberikan keamanan pada data websocket karena dapat disimpan perangkat *hardware* yang dimiliki, sehingga tidak perlu khawatir kehilangan dan rusak.

I.4. Metodologi Penelitian

Di dalam menyelesaikan penelitian ini penulis menggunakan 2 (dua) metode studi yaitu :

1. Studi Kepustakaan (*Library Research*)

Penulis melakukan studi pustaka untuk memperoleh data-data yang terkaitan dari berbagai sumber bacaan seperti buku panduan pembuatan aplikasi pengolah program dengan *Javasript*, manajemen basis data, dan buku atau jurnal yang membahas tentang konsep pembuatan kartografi pada perpustakaan-perpustakaan umum, perpustakaan Universitas Sumatera Utara, perpustakaan Universitas Potensi Utama.

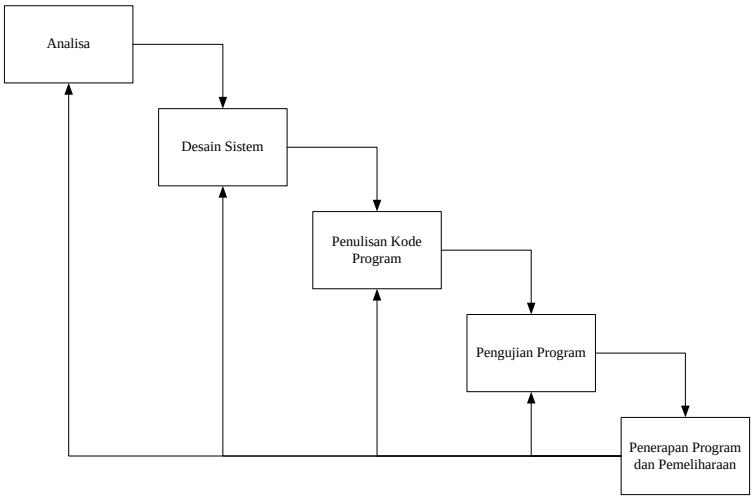
Ada beberapa prosedur yang digunakan dalam penelitian ini adalah sebagai berikut :

1. Prosedur Perancangan

   Merupakan tata cara dan langkah-langkah yang diperlukan untuk mencapai tujuan perancangan yang dilakukan. Langkah-langkahnya adalah :

   a. Menganalisis permasalahan websocket yang terenkripsi.
   b. Merancang sistem yang baru dengan menggunakan model UML (*Unified Modeling Language*).
   c. Membuat aplikasi dengan bahasa pemrograman *Javascript*.

Didalam melakukan pengembangan sistem penulis menggunakan paradigma *waterfall*. Adapun metode *waterfall* mempunyai tahapan-tahapan sebagai berikut :



Gambar I.1. *Waterfall*

Adapun tahapan dalam menyelesaikan permasalahan diatas seperti terlihat pada alur prosedur perancangan diatas yaitu :

1. Analisa Kebutuhan

   Adapun tahap yang dilakukan pada analisa kebutuhan yaitu mengumpulkan data data yang akan menjadi *outputan* dan juga *inputan* dalam sistem. Pada tahapan ini untuk mengetahui perbandingan latency pada data terenkripsi.

2. Desain Sistem

   Desain sistem ini dirancang dengan permodelan *UML* menggunakan *Microsoft Visio* 2010 yang digunakan untuk membuat desain sistem aplikasi.

3. Penulisan Kode Program

   Penulisan kode program menggunakan *Javasript*. Hal ini sangat memudahkan proses pasca perancangan kode program. Setelah pengkodean selesai maka akan dilakukan *testing* terhadap sistem yang telah dibuat tadi. Tujuan *testing*

adalah menemukan kesalahan kesalahan terhadap sistem tersebut dan kemudian bisa diperbaiki.

4. Pengujian Program

Berisi langkah-langkah yang dilakukan dalam pembuatan alat serta tahapan-tahapan pengujian yang dilakukan untuk masing masing blok peralatan yang dirancang.

   a. Menganalisis beberapa kesalahan yang ada pada sistem yang lama.
   b. Melakukan pengujian aplikasi yang baru utuk meminimalisir kesalahan yang ada.
   c. Melakukan perawatan sistem yang baru apabila terjadi kesalahan.

5. Penerapan Program dan Pemeliharaan

   Perangkat lunak yang merupakan suatu kegiatan untuk memelihara perangkat lunak yang sudah dibuat, pemeliharaan tersebut dilakukan agar keutuhan program dapat terjaga seperti validasi data, update data, dan integrasi data.

I.5. Keaslian Penelitian

Perancangan Dan Pembuatan Analisis Perbandingan Latency Pada Transmisi Data Terenkripsi di Protokol Websocket Dengan Algoritma RC4 Dan RC6” perbandinganya dapat dilihat pada tabel I.1 dibawah ini :

Tabel I.1. Keaslian Penelitian

No	Materi Perbandingan	Instrumen
Penelitian pertama : Perbandingan Algoritma Block Cipher RC5 Dan RC6 Hasil : Dapat dilihat berdasarkan kebutuhan plaintext, bahwa RC6 jauh lebih kuat daripada RC5. Jumlah ronde yang dianjurkan untuk menggunakan RC6 adalah 20 ronde, karena pada ronde tersebut jumlah kebutuhan plaintext sudah melebihi 2128 untuk kedua jenis serangan		
1.	Algoritma yang digunakan	RC5 dan RC6
2.	Penelitian	*Block chipper*
3.	Basis Aplikasi	Desktop
4.	Perangkat Lunak	Tidak diketahui
Penelitian kedua : Penerapan Algoritma RC6 Untuk Ekripsi SMS Telepon Seluler Hasil : Penerapan algoritma kunci privat untuk enkripsi SMS pada telepon selular dapat meningkatkan keamanan. Pesan yang terenkripsi tidak akan dapat dibaca jika tidak didekripsi dengan menggunakan kunci yang benar, sehingga orang yang tidak mengetahui kunci yang sebenarnya tidak dapat membaca pesan yang dikirimkan. Algoritma RC6 dapat diterapkan dengan baik untuk melakukan enkripsi SMS yang bekerja pada jaringan GSM dengan mengirimkan pesan yang berbentuk *binary*. Kekurangan dari implementasi algoritma RC6 untuk enkripsi SMS adalah pesan yang dikirimkan menjadi lebih besar karena harus bekerja pada 8 bit dan dibutuhkan *padding* untuk memenuhi panjang blok .		
1.	Algoritma yang digunakan	RC6
2.	Penelitian	Enkripsi SMS
3.	Basis Aplikasi	*Openwrt*
4.	Perangkat Lunak	Tidak digunakan
Penelitian yang akan dibuat : Analisis Perbandingan Latency Pada Transmisi Data Terenkripsi di Protokol Websocket Dengan Algoritma RC4 Dan RC6		

1.	Algoritma/Metode yang digunakan	RC4 dan RC6.
2.	Penelitian	Latency Pada Transmisi Data Terenkripsi
3.	Basis Aplikasi	Dekstop.
4.	Perangkat Lunak	Node js, Java script

I.6. Sistematika Penulisan

Adapun sistematika penulisan yang diajukan dalam Skripsi ini adalahsebagai berikut :

BAB I : PENDAHULUAN

Pada bab ini menerangkan tentang latar belakang, ruang lingkup permasalahan, tujuan dan manfaat, metode penelitian dan sistematika penulisan.

BAB II : TINJAUAN PUSTAKA

Pada bab ini menerangkan tentang teori-teori dan metode yang berhubungan dengan topik yang dibahas atau permasalahan yang sedang dihadapi.

BAB III : ANALISA DAN DESAIN SISTEM

Pada bab ini mengemukakan tentang analisa sistem yang sedang berjalan, evaluasi sistem yang berjalan dan desain sistem secara detail.

BAB IV : HASIL DAN UJI COBA

Pada bab ini menerangkan hasil dan pembahasan program yang dirancang serta kelebihan dan kekurangan sistem yang dirancang.

BAB V : KESIMPULAN DAN SARAN

Pada bab ini berisi kesimpulan penulisan dan saran dari penulis sebagai perbaikan di masa yang akan datang untuk sistem.