BAB III
ANALISIS DAN DESAIN SISTEM

III.1. Analisis Masalah

Analisa masalah sistem pada perbandingan *latency* pada transmisi data terenkripsi di protocol *websocket* ini memerlukan antarmuka untuk mengkoneksikan dan mengendalikan server sebagai uji latency pada transmisi dengan komputer server, menggunakan bahasa pemprograman *Javascript* sebagai antarmuka antara protocol websocket dan komputer server, untuk pembuatan latency yang akan diakses oleh user. Berdasarkan penjelasan mengenai algoritma RC4 dan RC6 di atas, dapat diketahui beberapa perbedaan mendasar antara RC6 dengan RC4.

RC6 menggunakan 4 register berukuran b/4-bit, sedangkan RC4 menggunakan 2 register berukuran b/2-bit, dengan b menyatakan panjang blok. RC6 menggunakan 4 register karena dirancang untuk memenuhi spesifikasi AES, yaitu kemampuan beroperasi dalam mode 128 bit. Dengan 4 register kerja, maka besar masing-masing register kerja yang diperlukan hanya 32 bit ($4 \times 32 = 128$ bit).

III.2. Penerapan Metode

Studi kasus RC4 proses pertama dalam algoritma RC-4 adalah Key Scheduling Algorithm. KSA ini merupakan inisialisasi untuk pentabelan S-BOX dan kunci. RC4 mempunyai sebuah S-Box, S0,S1,...,S255, yang berisi permutasi dari bilangan 0 sampai 255. Terdapat dua indeks yaitu i dan j yang diinisialisasi

dengan bilangan nol. Untuk menghasilkan random byte langkahnya adalah sebagai berikut :

For i ← 0 to 255

S[i] ← i

Dalam operasi selanjutnya, RC-4 akan mengubah isi kotak-S tergantung kunci K dengan operasi sebagai berikut :

j=0

for i ← 0 to 255

j ← (j +S[i] +K[i]) mod 256

pertukarkan isi S[i] dan isi S[j]

Dengan demikian berakhirlah proses KSA. Untuk selanjutnya untuk membangkitkan kunci enkripsi, dilakukan proses PRGA atau Pseudo Random Generation Algorithm.

Algoritma PRGA adalah sebagai berikut :

i ← 0

j← 0 i ←(i + 1) mod 256

j ←(j + S[i]) mod 256

pertukarkan isi S[i] dan S[j]

k = S [S[i] + S [j]] mod 256

perhatikan bahwa k kecil merupakan kunci yang langsung beroperasi terhadap plaintext, sedangkan K besar adalah kunci utama induk.

Bila terdapat plaintext P, maka operasi enkripsi berupa :

C = P XOR k

III.3. Desain Sistem

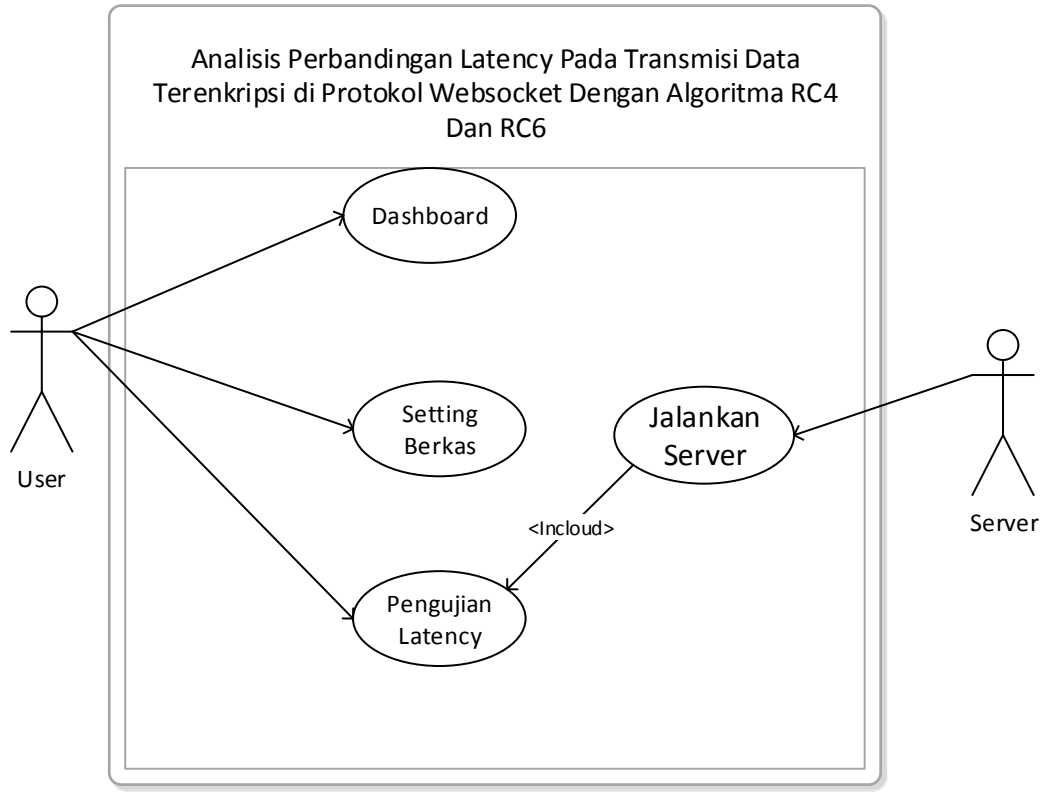
Desain sistem pada penelitian ini dibagi menjadi dua desain, yaitu desain sistem secara global untuk penggambaran model sistem secara garis besar dan desain sistem secara detail untuk membantu dalam pembuatan sistem.

III.3.1. Desain Sistem Secara Global

Desain sistem secara global menggunakan bahasa pemodelan UML yang terdiri dari *flowchart, dan Blok Diagram*.

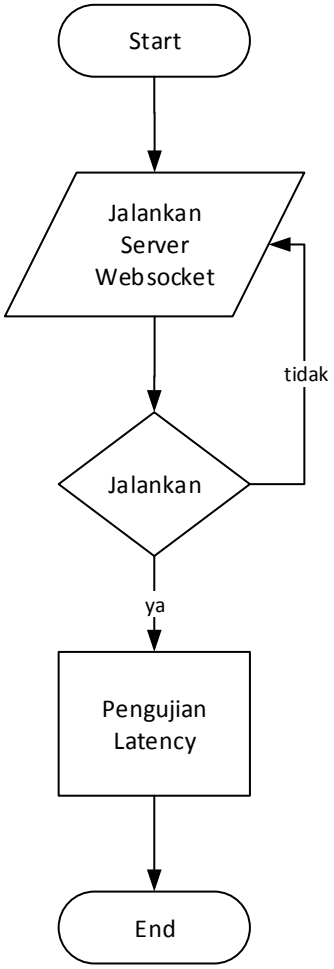
III.3.1.1. *Usecase* Diagram

Rancangan ini disusun dengan tujuan mendesain dan merepresentasikan program. Fungsinya adalah untuk memudahkan pengguna mentransmisi data yang akan dibuat pada gambar III.1 berikut.



Gambar.III.1. *Use Case Webcam*

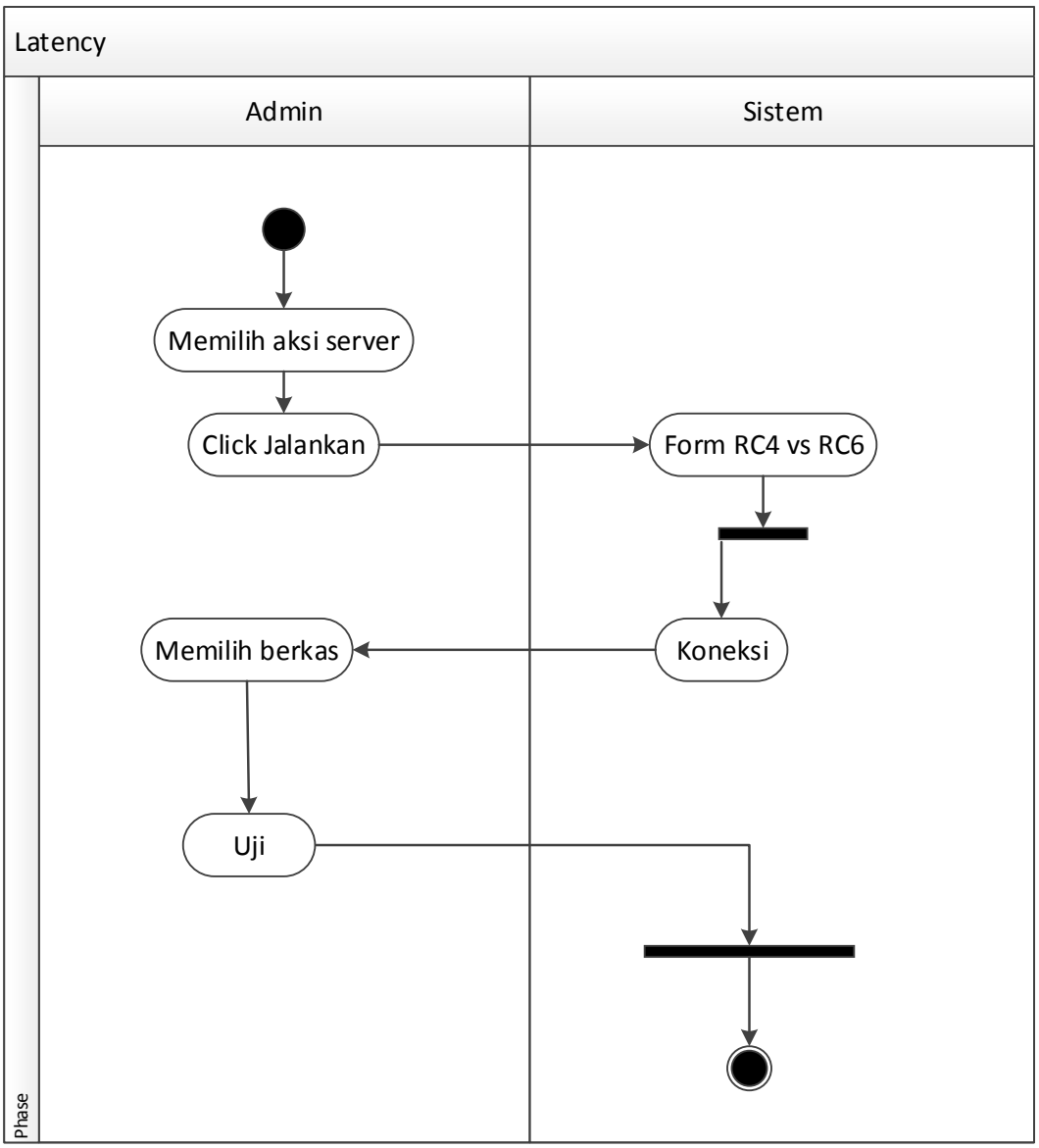
III.3.1.2. *Flow Chart*



Gambar.III.2. *Flow Chart*

III.3.1.3. Blok Diagram

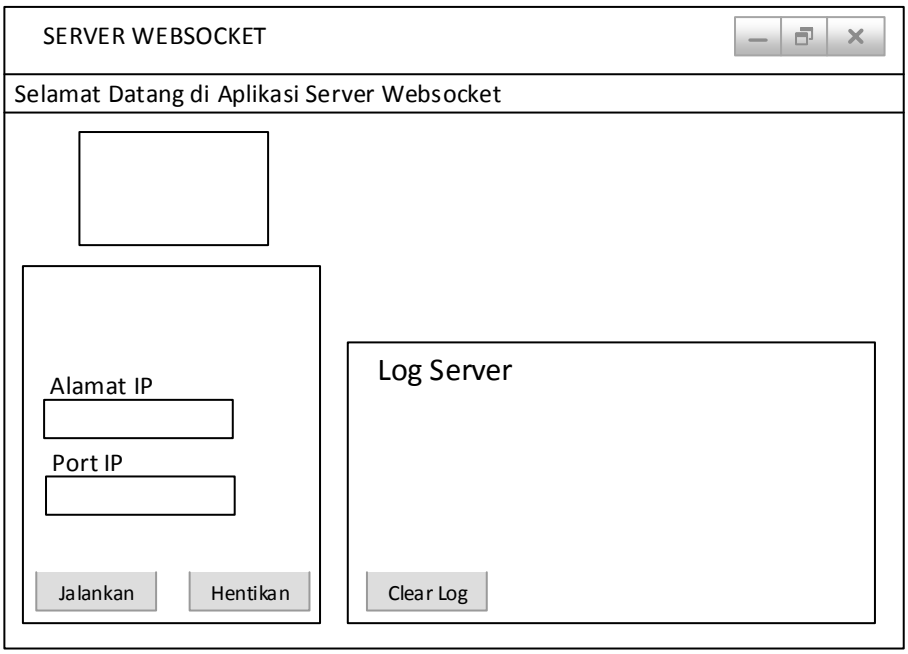
Sistem latency websocket ini memerlukan antarmuka untuk mengkoneksikan dan mengendalikan server sebagai pengujian antara metode dengan sistem latency, menggunakan bahasa pemprograman javascript sebagai antarmuka antara server computer terlihat pada gambar III.3 berikut.



Gambar.III.3. *Blok Diagram*

III.4. Desain User Interface

Berikut ini adalah rancangan atau desain *input* sebagai antarmuka server terdapat pada gambar III.4 :



Gambar.III.4. Desain Tampilan Server

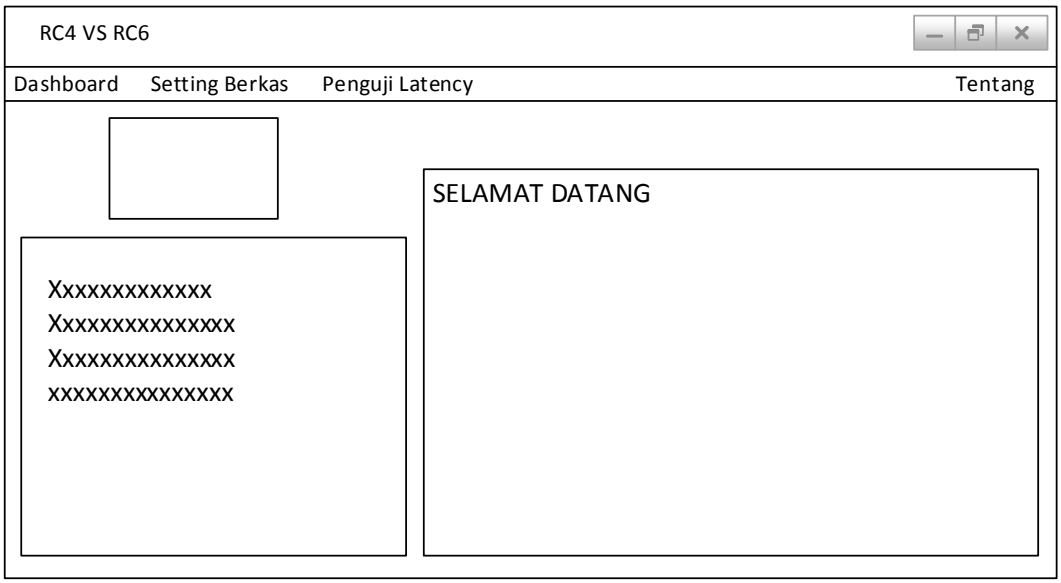
Keterangan :

Dari desain tampilan server websocket terdapat untuk menjalakan alamat ip dan port ip pada aplikasi ini mesti melakukan klik jalankan untuk menjalakan alamat ip dan port ip pada server.

Tombol hentikan untuk mengentikan jalannya server ke klient pada alamat ip tersebt

1. Desain Tampilan Dashboard

Desain yang dirancang untuk melihat tampilan depan aplikasi dari aplikasi sistem klient terlihat seperti pada gambar III.5 berikut :



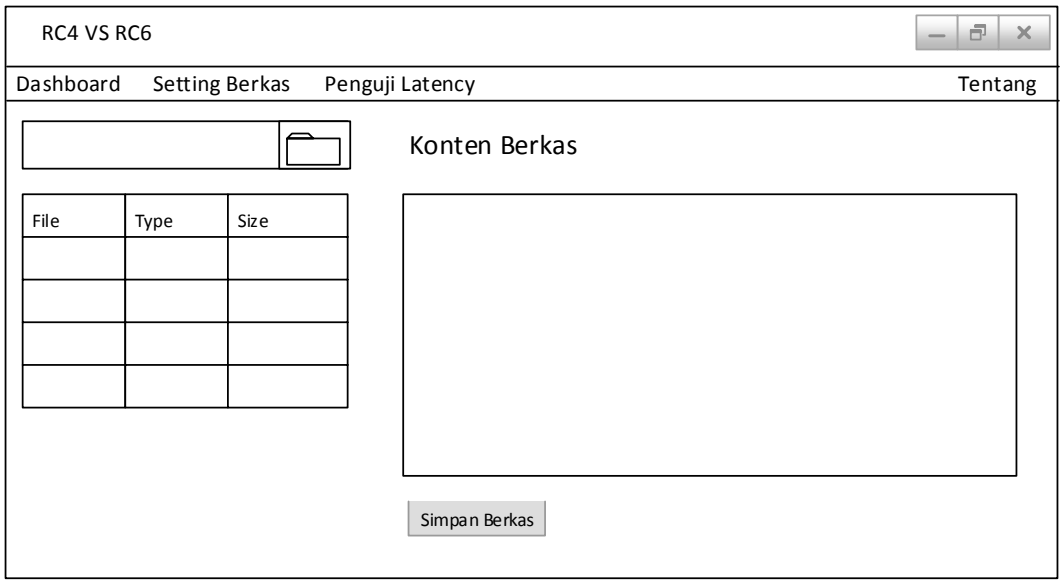
Gambar.III.5. Desain Dashboard

Keterangan :

Dari desain ini terdapat halaman dashboard, klient siap melakukan perbandingan latency yang sesuai kebutuhan dengan menekan tombol-tombol yang telah disediakan.

2. Desain Tampilan Setting Berkas

Desain tampilan setting berkas yang dirancang untuk mengetahui kapasitas berkas yang akan dibandingkan terlihat seperti pada gambar III.6 berikut :



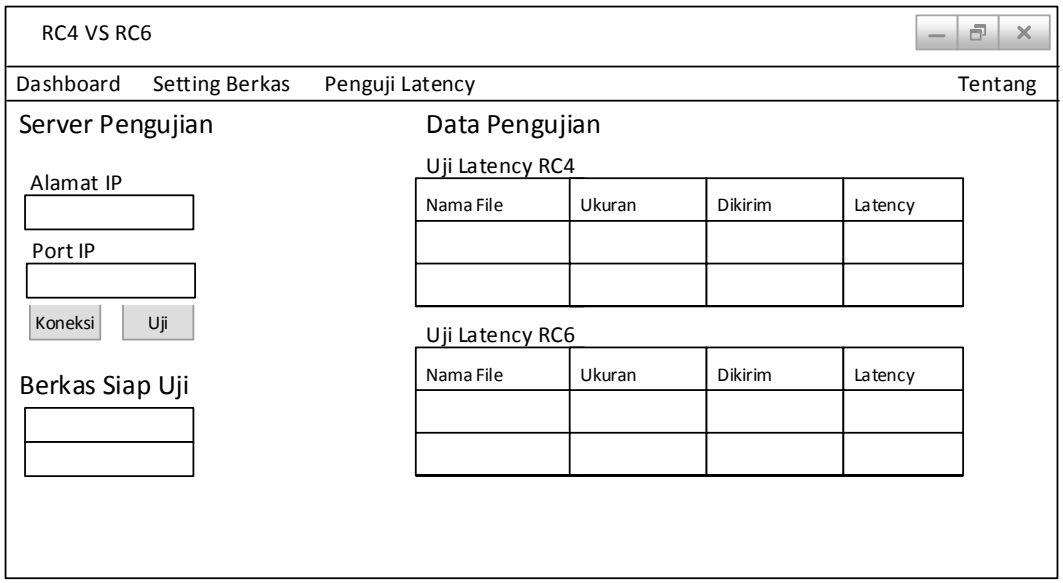
Gambar.III.6. Desain Tampilan Setting Berkas

Keterangan :

Dari desain setting berkas terdapat nama berkas yang akan di latency untuk mengetahui konten berkas yang aka disimpan.

3. Desain Tampilan Pengujian Latency

Desain tampilan pengujian latency dari server yang harus dikoneksi dari data pengujian terlihat seperti pada gambar III.7 berikut :



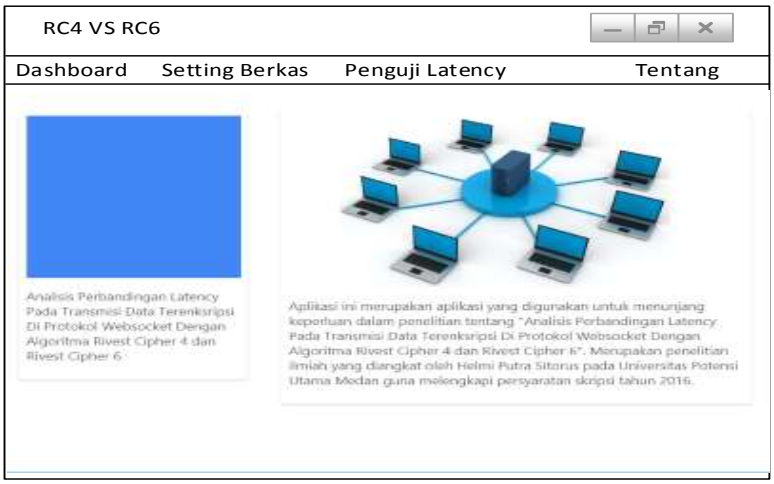
Gambar.III.7. Desain Tampilan Pengujian Latency

Keterangan :

Dari desain pengaturan program ini untuk mengatur aplikasi webcam sesuai yang kita butuhkan.

4. Desain Tampilan Tentang

Desain tampilan tentang untuk mengetahui aplikasi terlihat seperti pada gambar III.8 berikut :



Gambar.III.8. Desain Tampilan Tentang

Keterangan :

Dari desain tampilan tentang untuk mengetahui versi program yang telah dibuat