BAB IV

HASIL DAN PEMBAHASAN

IV.1. Hasil

Hasil yang disajikan oleh sistem berdasarkan Analisis Keamanan Transmisi data teks melalui websocket menggunakan algoritma one-time pad adalah berupa sistem yang menghasilkan informasi-informasi penyampaian data seperti yang telah dirancang, form-form yang berfungsi sebagai media pengolahan data menjadi lebih mudah dan cepat dalam penyebaran informasi dan dilakukan pengujian terhadap sistem untuk mengetahui tingkat koneksi dan keamanan dari sistem yang dirancang. Adapun pembahasan hasil yang disajikan adalah tampilan hasil sistem seperti berikut :

1. Tidak ada sebuah aplikasi yang memiliki sistem keamanan transmisi data yang aman.
2. Belum ada perkembangan algoritma Algoritma one-time pad dalam sistem keamanan berkas atau transmisi data

IV.1.1. Tampilan Hasil

Berikut ini dijelaskan tentang tampilan hasil dari Analisis Keamanan Transmisi data teks melalui websocket menggunakan algoritma one-time pad dapat dilihat sebagai berikut :

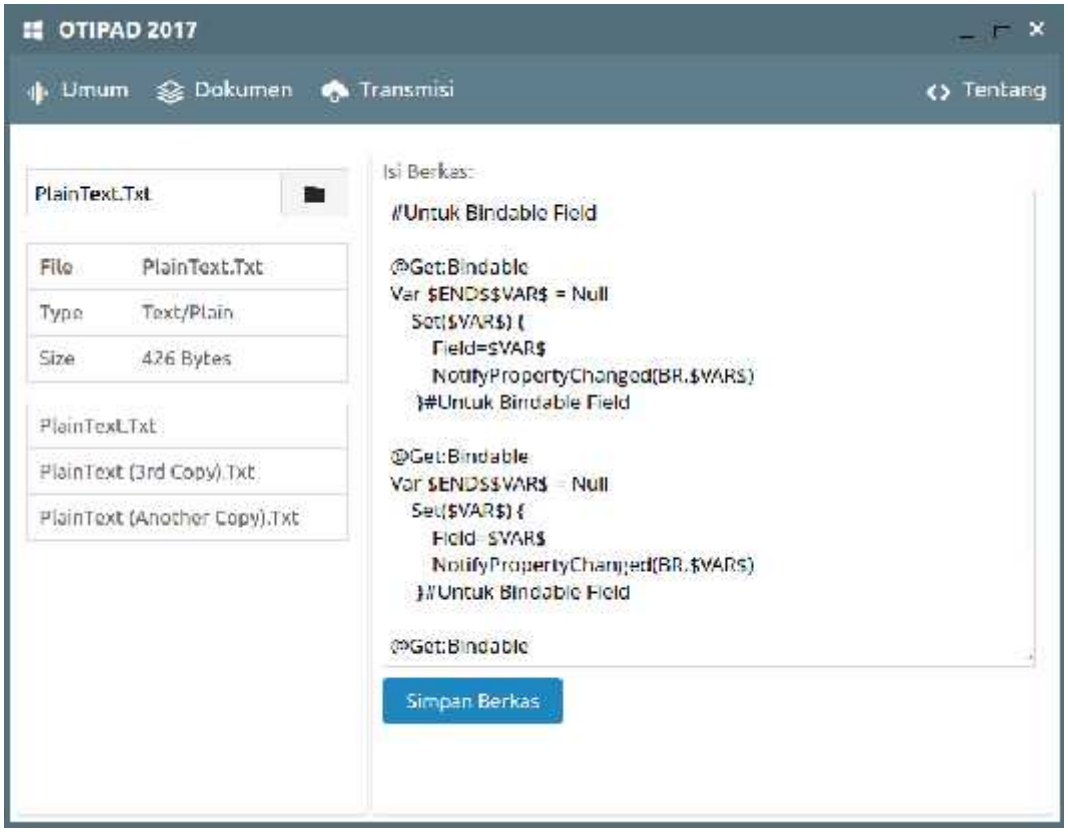
1. Tampilan *Form* Umum

Tampilan pada *form* Umum dapat diterangkan dengan langkah-langkah *state* berikut, yang ditunjukkan pada gambar IV.1 berikut :

Gambar IV.1. Tampilan *Form* Umum

2. Tampilan *Form* Dokumen

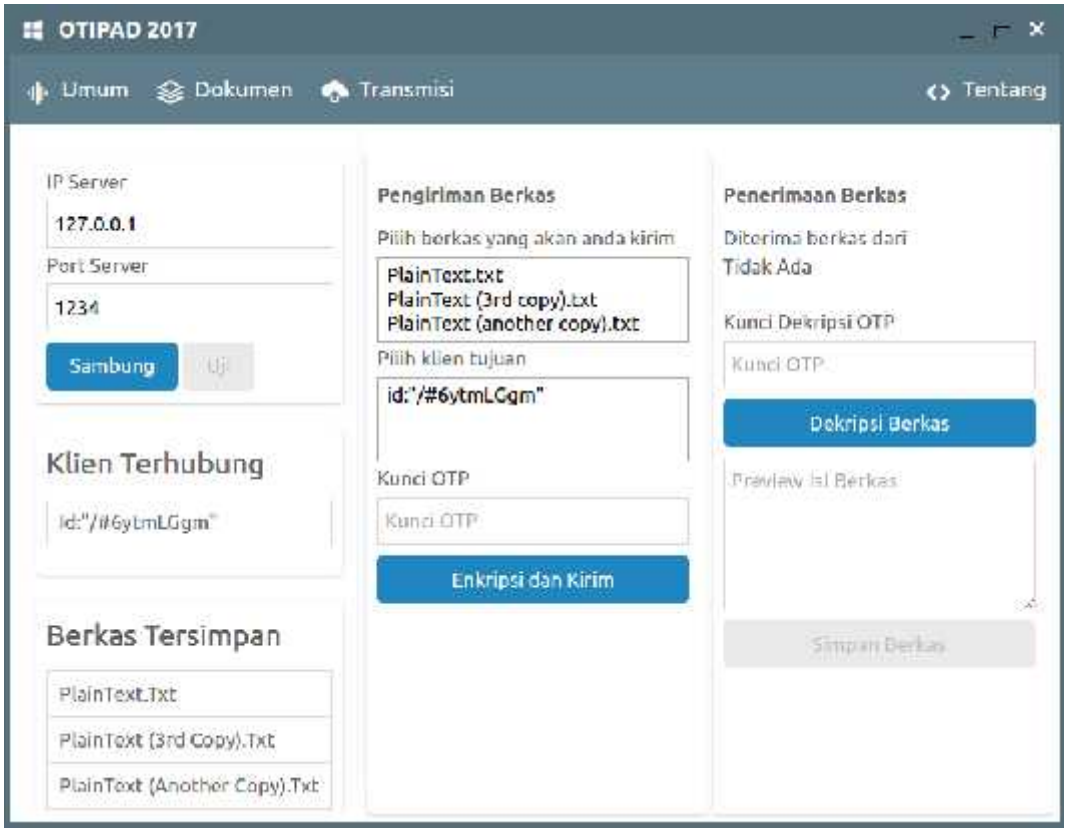
Tampilan pada *form* Dokumen dapat diterangkan dengan langkah-langkah *state* berikut, yang ditunjukkan pada gambar IV.2 berikut :



Gambar IV.2. Tampilan *Form* Dokumen

3. Tampilan *Form* Transmisi

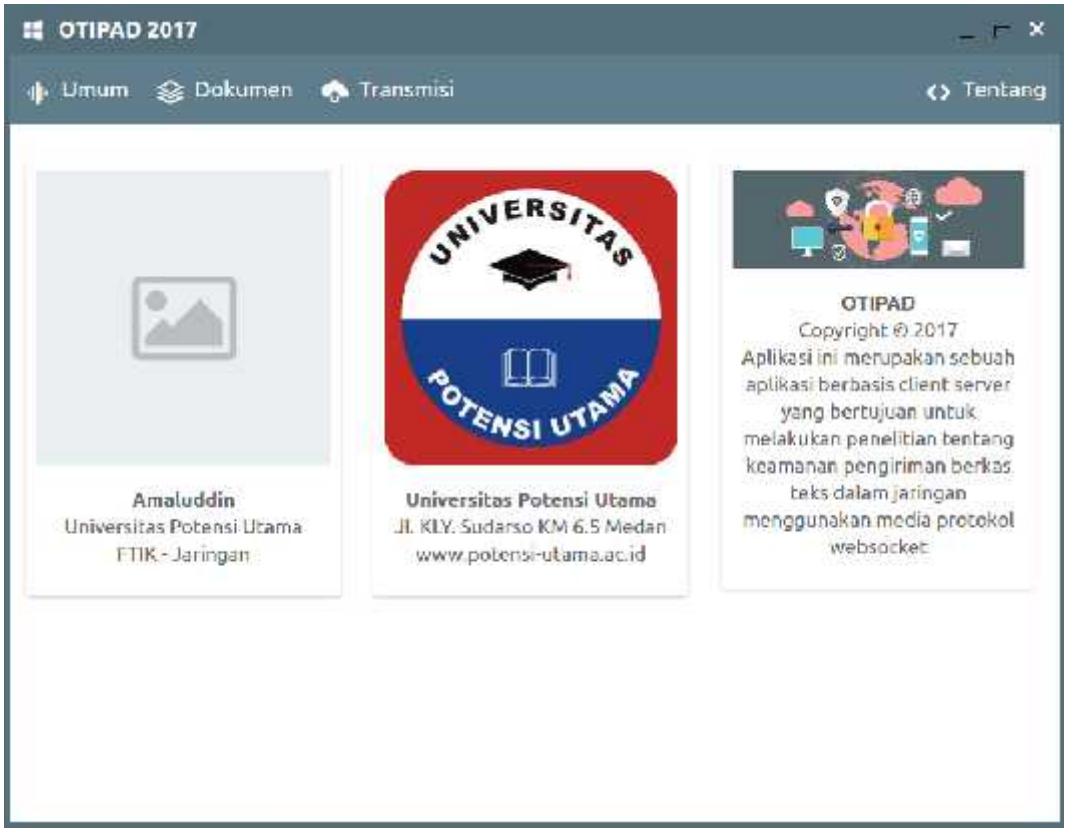
Tampilan pada *form* Transmisi dapat diterangkan dengan langkah-langkah *state* berikut, yang ditunjukkan pada gambar IV.3 berikut :



Gambar IV.3. Tampilan *Form* Transmisi

4. Tampilan Form Tentang

Tampilan pada form tentang dapat diterangkan dengan langkah-langkah *state* berikut, yang ditunjukkan pada gambar IV.4 berikut :



Gambar IV.4. Tampilan Form Form Tentang

IV.2 Pembahasan

Instrumen yang digunakan untuk melakukan pengujian ini yaitu dengan menggunakan:

1. Satu unit laptop dengan spesifikasi sebagai berikut:
    a. Processor Intel Core Duo
    b. Memory 2 Gb
    c. Hardisk 500 Gb
2. Perangkat Lunak dengan spesifikasi sebagai berikut:
    a. Javascript

IV.2.1. Penerapan Algoritma One-Time Pad

Dalam kriptografi dikenal beberapa algoritma, diantaranya adalah algoritma One Time Pad (OTP).One Time Pad adalah salah satu metode kriptografi dengan algoritma jenis simetri. Ditemukan pada tahun 1917 oleh Major Yoseph Mouborgne dan Gilbert Vernam pada perang dunia ke dua. Metode ini telah diklaim sebagai satu-satunya algoritma kriptografi sempurna yang tidak dapat dipecahkan. Suatu algoritma dikatakan aman, apabila tidak ada cara untuk menemukan plaintext-nya. Sampai saat ini, hanya algoritma One Time Pad (OTP) yang dinyatakan tidak dapat dipecahkan meskipun diberikan sumber daya yang tidak terbatas. Dalam proses enkripsi One Time Pad, cipherteks diperoleh dengan melakukan penjumlahan modulo 26 dari satu bit plainteks dengan satu bit kunci, seperti terlihat pada Rumus :

$C_i = (P_i + K_i) \text{ mod} 26$

Dimana :

C_i = cipher teks

P_i = plainteks

K_i = kunci

Sedangkan dalam proses dekripsi, untuk mendapatkan kembali plainteks, diperoleh dengan melakukan penjumlahan modulo 26 dari satu bit cipherteks dengan satu bit kunci (Febryan Christy Winaryo ; 2014 : 4):

$$P_i = (C_i - K_i) \text{ mod } 26$$

Rumus melakukan One Time Pad ini yaitu :
Enkripsi : E(x) = (P(x) + K(x)) Mod 26
Dekripsi : D(x) = (C(x) – K(x)) Mod 26

Nilai modulo disesuaikan dengan kebutuhan enkripsi, penyandian abjad latin maka digunakan angka 26 yaitu jumlah abjad yang ada, sementara untuk karakter penuh menggunakan angka 256 sejumlah banyaknya kode ASCII.

Pemakaian One Time Pad digunakan pada sederetan abjad A..Z dengan memberikan nilai urutan abjad yaitu A=0, B=1, C=2, D=3, E=4…..sampai Z.

Contoh Enkripsi Pesan :

Pesan : ZENSHIFU
Kunci : OTIMEPAD
maka perhatikan langkahnya seperti di bawah ini :

Plaintext 25(Z) 4(E) 13(N) 18(S) 7(H) 8(I) 5(F) 20(U)
Kunci 14(O) 19(T) 8(I) 12(M) 4(E) 15(P) 0(A) 3(D)
——————————————— +
Hasil mod 26 13 23 21 4 11 23 5 23
Chipertext N X V E L X F X
Jadi Chipertext yang di hasilkan yaitu : NXVELXFX

Dekripsi pesan, perhatikan langkah di bawah ini

Chipertext 13(N) 23(X) 21(V) 4(E) 11(L) 23(X) 5(F) 23(X)
Kunci 14(O) 19(T) 8(I) 12(M) 4(E) 15(P) 0(A) 3(D)
——————————————— –
Hasil mod 26 25 4 13 18 7 8 5 20
Plaintext Z E N S H I F U
Jadi Plaintext yaitu : ZENSHIFU

IV.3. Kelebihan dan Kekurangan Sistem

Setiap sistem memiliki kelebihan dan kekurangan, berikut ini adalah kelebihan dan kekurangan sistem yang telah dibuat.

IV.3.1. Kelebihan Sistem

Kelebihan sistem ini diantaranya yaitu:

1. Aplikasi keamanan transmisi data dengan memanfaatkan sistem keamanan transmisi data dapat menjaga kerahasiaan dan keamanan pengiriman transmisi data pada aplikasi keamanan transmisi data sehingga pengirim pesan dapat merasa nyaman dan aman dalam melakukan transfer transmisi data atau pesan
2. Implementasi Algoritma one-time pad terhadap aplikasi keamanan transmisi data dirancang untuk penggunaan memori yang seminimal mungkin dengan kecepatan proses yang maksimal.

IV.3.2. Kekurangan Sistem

Adapun kekurangan sistem yang telah dibuat diantaranya yaitu:

1. Pengiriman data menggunakan socket tidak dapat dilakukan untuk berkas berukuran besar.
2. Berkas yang dikirim tidak dapat berupa multipart body.
3. Aplikasi tidak dapat melakukan preview untuk berkas dengan format kompleks.
4. Koneksi ke server tidak dapat dilakukan dengan persisten, saat koneksi terputus dan terhubung kembali, klien akan dikenali dengan ID baru.