BAB I
PENDAHULUAN

1.1 Latar Belakang

User authentication merupakan komponen utama dalam infrastruktur keamanan akhir – akhir ini. *User authentication* juga merupakan masalah untuk setiap sistem akses layanan keamanan menjadi berharga, informasi aman, dan layanan *personality*. Ada 3 cara untuk menentukan *user authentication* : *knowledge-based system, token-based system,* dan *system based on biometrics*.

Pada saat ini skema *token-based* sangat umum digunakan seperti *key card*, *bank card*, dan *smart card*. Sebagai contoh digunakan untuk ATM (Anjungan Tunai Mandiri). *Biometrics system* memang lebih aman dibandingkan dengan kedua authentikasi lainnya tapi ada beberapa permasalahan pada sistem biometrics salah satunya harus menggunakan alat khusus yang dianjurkan, mahal dan mungkin penggunaanya lebih rumit.

Textual password pada umumnya menggunakan karakter alfanumerik (atau printable ASCII characters) untuk mengindentifikasi pengguna yang bersangkutan. *Password* yang sederhana memudahkan pengguna untuk mengingatnya tetapi mudah juga untuk dipecahkan. Sedangkan *password* yang rumit, penggunaannya tidak nyaman tapi sulit untuk dipecahkan. Bagaimanapun juga penggunaan *textual password* dapat dipecahkan cepat atau lambat, karena *user* berulang – ulang memilih *password* yang mudah dikenali. Hal ini disebabkan karena ingatan manusia yang terbatas. Kasus ini biasanya disebut ”*small dictionary*”.

Penyerangan terhadap ”small dictionary” menurut Dr. Klein [Klein 1990] ini ternyata dapat berhasil dilakukan, sekitar 25% dari 14000 *password* dapat di pecahkan oleh sebuah ”dictionary” hanya dengan 3 juta masukan (ukuran dictionary 21.5 bits).

Disisi lain, penggunaan alat – alat yang besifat *personal* dan mobilitas yang tinggi cenderung meningkat akhir – akhir ini. Ada beberapa masalah dalam hal *personality*: jika *user authentication* tidak diaktifkan, memungkinkan pengguna umum dapat memakainya. Sehingga ini bukan bersifat *personal* lagi.

Bahkan apabila *user authentication* ini diaktifkan, mungkin saja mekanismenya lemah. Sekali mengaktifkan authentikasi ini, harus berulang – ulang diperbaharui.

Dalam tugas akhir ini, saya akan membuat aplikasi menggunakan skema graphical *password* dengan menggunakan gambar sebagai node – node yang nantinya dapat dikombinasikan layaknya *password* pada umumnya. Dan diharapkan keamanan berbading lurus dengan kenyamanan.

I.2. Perumusan Masalah

1. Metode *textual password* bisa dipecahkan (kekuatan *textual password*).
2. Gambar lebih mudah dikenali dibandingkan teks.
3. Tingkat keamanan dan kenyamanan penggunaan atuhentication.
4. Kesulitan mencari dan mengingat *password* yang ingin digunakan.
5. Parameter – parameter yang dianalisa :
   - Efektifitas, meliputi daya ingat seseorang tentang *picture/image* yang digunakan sebagai *password.*
   - Kecepatan Waktu Entry, waktu yang dibutuhkan seseorang saat meng*entry picture/image* sebagai *password*.
   - Kekuatan *password* secara umum.
   - User satisfaction (Kepuasan Pengguna), meliputi *Mean Opinion Square*.
6. Parameter – parameter yang disimpulkan :
   - Apakah Picture *Password* dapat dijadikan alternatif authentication yang cukup dapat diandalkan dibandingkan metode authenticatin pada umumnya.
   - Apakah Picture *Password* yang digunakan cukup dapat memenuhi kenyamanan yang diinginkan (MOS).

I.3. Tujuan Pembahasan

Tujuan yang ingin dicapai dari penyusunan tugas akhir ini adalah:

1. Merancang Graphical *Password* menggunakan image selection (picture *password*).

2. Menganalisa performansi dari skema *password* tersebut meliputi parameter diatas.

I.4. Batasan Masalah

Dalam pembangunan aplikasi ini dibatasi beberapa hal yaitu :

1. Panjang *password* maksimum yang digunakan 7 digit.
2. Menggunakan pengamanan kriptografi hash MD5.
3. Gambar sudah ada (ditentukan dari awal) jadi pengguna hanya memilih.
4. Setiap gambar berbentuk persegi dengan ukuran 80x80 piksel.
5. Digunakan untuk pengguna tunggal (*single user*) dan *single password*.
6. Gambar sebagai interface inputan.
7. Sistem tidak melakukan proses pengkodean gambar.
8. File penyimpanan berekstensi Reg (.reg).
9. Sistem diterapkan dan hanya berjalan pada Sistem Operasi Windows.

I.5. Metodologi Penyelesaian Masalah

Dalam penelitian nantinya, penulis akan melakukan metode sebagai berikut :

1. Studi literatur.
   - Mengambil referensi – referensi yang menunjang penelitian tugas akhir ini.
   - Pengumpulan data dari penelitian sebelumnya tentang skema *Graphical password*.
2. Perancangan.
   - Merancang aplikasi *picture password* yang akan digunakan.
3. Percobaan.
4. Validasi
5. Analisa.
   - Menganalisa parameter – parameter tersebut di atas dengan analisa teknis dan penilaian berdasarkan MOS.
6. Kesimpulan dan Saran.

I.6. Sistematika Penulisan

BAB I PENDAHULUAN

Berisi latar belakang, perumusan masalah, batasan masalah, tujuan pembahasan, metodologi penyelesaian masalah dan sistematika penulisan.

BAB II LANDASAN TEORI

Berisi penjelasan umum tentang landasan teori yang berkaitan dengan penyusunan tugas akhir.

BAB III PERANCANGAN DAN DESAIN SISTEM

Berisi analisis sistem yang akan dikembangkan mencakup analisa kebutuhan sistem, perancangan dan desain sistem, sehingga dapat dipahami dengan mudah.

BAB IV IMPLEMENTASI DAN ANALISIS PROGRAM

Membahas analisa hasil percobaan berdsarkan parameter yang telah disebutkan di atas.

BAB V KESIMPULAN DAN SARAN

Diuraikan kesimpulan dan saran yang didapat dari hasil pengembangan sistem.