BAB I
PENDAHULUAN

1.1 Latar Belakang

Kebanyakan aplikasi yang digunakan setiap orang di Internet pasti memiliki aspek keamanan yang melindungi hak akses setiap orang agar tidak disalahgunakan oleh mereka yang tidak berhak menggunakannya. Metode perlindungan yang paling umum digunakan adalah metode login berbasis teks, yaitu *username* dan *password,* yang bersifat *knowledge-based*. Tetapi seraya zaman berkembang, *text-based password* memiliki berbagai kelemahan dan ancaman, seperti ancaman pencurian *password* oleh *hacker*[1].

Text-based password terkadang sulit diingat oleh pengguna, terutama jika *password* yang digunakan relatif panjang, dan mengingat banyak *password* untuk berbagai macam akun bukanlah hal yang menyenangkan [1][2]. Berberapa pengguna sistem memutuskan untuk menggunakan kata yang mudah diingat sebagai *password* tanpa menyadari bahwa *password* pilihannya dapat dengan mudah di-*brute force* dengan waktu yang singkat[2].

Beberapa metode untuk memudahkan login pada sistem tanpa menggunakan *text password* telah disarankan, seperti dirinci di makalah *Single Sign On with Bluetooth Device* [3], dimana penulis menggunakan *bluetooth device* sebagai token autentikasi *single factor*, tetapi jika *bluetooth device* dicuri, maka pencuri dapat langsung *login* menggunakan *device tersebut*.

Metode autentikasi lain yang diriset adalah menggunakan *recognition-based graphical password*, sebagai contoh aplikasi *ImagePass*, dimana *password* berupa gambar *single object* yang dipilih oleh pengguna [4][5]. *ImagePass* masih memiliki kelemahan terhadap *shoulder surfing*, yaitu teknik pencurian *password* dengan mengamati pengguna melakukan *login*, dan *username enumeration*, yaitu upaya untuk mencari tahu jika suatu *username* ada di dalam sistem.

Tim peneliti lain juga melakukan riset mengenai autentikasi menggunakan metode *graphical password* dengan mengimplementasikan gerakan bidak catur,

tetapi metode ini masih lemah terhadap *password guessing* menggunakan metode *shoulder surfing*[6].

Masalah lain terhadap autentikasi adalah menyeimbangkan *usability* dan *security*. Pengguna pada umumnya mau melakukan login dengan waktu yang relatif singkat tetapi juga ingin memastikan bahwa login dilakukan dengan aman. Suatu perancangan autentikasi bernama "Q-A" menunjukkan bahwa skema autentikasi yang aman bisa jadi memiliki waktu penggunaan yang relatif tinggi [7].

Berdasarkan riset yang disebutkan sebelumnya, penulis menggabungkan implementasi autentikasi berbasis *bluetooth* dan *recognition based graphical password*, yang bertujuan untuk menciptakan skema autentikasi yang mudah dan nyaman digunakan oleh pengguna sebagai alternatif terhadap *text-based password*, dan juga untuk mencegah *username enumeration* dan mempersulit *shoulder surfing*.

1.2 Rumusan Masalah

Berikut adalah rumusan masalah yang dibahas:

- Berapa waktu rata-rata yang dibutuhkan bagi pengguna untuk melakukan fase registrasi dan login menggunakan sistem ini?
- Seberapa kuat sistem ini terhadap upaya pencurian *password* dengan serangan *shoulder surfing*?
- Apakah pengguna dapat mengingat gambar yang dipilih sebagai password setelah satu minggu berlalu?

1.3 Batasan Penelitian

Batasan penelitian adalah antara lain:

1. Aplikasi *website* yang dirancang hanya dapat dijalankan di Google Chrome versi 70 untuk Windows 10 karena sudah mendukung Bluetooth Smart.

2. *Bluetooth device* yang digunakan adalah *smartphone* yang menjalankan Android versi 5.0 (API level 21) dan seterusnya karena sudah memiliki *class* dan *support* yang dibutuhkan untuk proyek ini.
3. Gambar yang digunakan dalam *graphical authentication* bersifat *single object images*.
4. Website dibuat menggunakan bahasa HTML, PHP dan JavaScript, disertai dengan MySQL sebagai database.

1.4 Tujuan Penelitian

Tujuan penelitian ini adalah untuk merancang sistem login berbasis *two factor authentication* yang lebih mudah digunakan pengguna tanpa menggunakan *text-based password* dengan menggabungkan *recognition based graphical password* dan *bluetooth web API*.

1.5 Manfaat Penelitian

Manfaat penelitian ini adalah supaya pengguna dapat melakukan login dengan mudah dan nyaman dengan risiko *shoulder surfing* dan *username enumeration* sekecil mungkin, sehingga pengguna tidak perlu khawatir jika ada yang melihat pengguna memasukkan informasi *username* dan *password* ke dalam sistem.