BAB I

PENDAHULUAN

1.1. Latar Belakang

Sistem keamanan *password* dan *passcode* sudah lazim kita dengar dan sudah sering kita gunakan sekarang. Kedua sistem keamanan tersebut membuat semua yang kita miliki mulai dari laptop, *smartphone* hingga akun media sosial kita terasa aman dan tidak bisa sembarangan diakses oleh orang yang tidak kita kenal. Seperti yang sudah disebutkan, terdapat beberapa sistem keamanan yang paling sering digunakan pada saat ini seperti *password*, *passcode* dan beberapa variasi lainnya seperti *pattern lock*.

Namun terdapat kelemahan dalam sistem keamanan *password* dan *passcode*, yaitu banyaknya variasi *attack* untuk meretas sistem keamanan tersebut, contoh-contoh attack tersebut adalah *Brute-force Attack*, *Dictionary Attack, Table Lookup & Rainbow Table Attack*, penggunaan Markov Model & *Probabilistic Context-Free Grammar, Replay Attack*, penggunaan *keylogger* dan *phishing attack* [1][2]. Serangan-serangan tersebut bisa meretas *password* dan *passcode* dengan mudah dan dalam yang relatif waktu cepat, apalagi jika kedua sistem keamanan yang dibuat mudah ditebak dan tidak menggunakan spesifikasi yang disarankan.

Selain kemudahan password untuk diserang, terdapat juga masalah yang banyak orang, yaitu kesulitan untuk mengingat password karena memiliki banyak password [3] dan menurut penelitian yang dilakukan oleh Zviran [4], hanya 27.2% dari 103 responden yang berhasil mengingat *password* yang dibuat oleh responden dalam rentang waktu tiga bulan. Sulitnya untuk mengingat *password* yang dibuat membuat pengguna melakukan beberapa hal yang berisiko, yaitu menggunakan *password* yang sama untuk beberapa akun, mencatat *password* di sebuah kertas / dokumen dan tidak mengganti *password* secara berkala. Perilaku tersebut membuat gawai dan akun media sosial yang dimiliki oleh pengguna bisa diakses oleh penyerang jika salah satu *password* yang digunakan berulang, dicatat atau tidak diganti diretas.

Melihat kedua masalah yang ditemukan, penulis memiliki sebuah ide untuk membuat sebuah sistem keamanan *graphical password* yang menggunakan gambar doodle sebagai sistem keamanan utamanya dengan nama "Passwle". Selain dari Graphical Password terdapat juga beberapa solusi yang bisa diberikan selain *Graphical Password,* seperti *Pasword Manager*, *Two Factor Authentication, Biometric* dan *One-time Password*. Terdapat beberapa alasan penulis memilih gambar *doodle* sebagai sistem keamanan, karena manusia memiliki ingatan yang lebih baik ketika mengingat gambar dibandingkan dengan tulisan [5] dan menurut penelitian yang dilakukan oleh Calkins partisipan cenderung lebih mudah mengingat objek dalam bentuk gambar dibandingkan dengan menyebutkan objek tersebut dan memperlihatkan tulisan nama dari objek tersebut [6]. Selain itu gambar *doodle* yang dimiliki oleh setiap orang berbeda-beda tergantung dengan tipe kepribadian seseorang [7] dan metode serangan yang dimiliki untuk kategori *graphical password* relatif lebih sedikit dan lebih aman dibandingkan dengan password yang menggunakan teks, dimana metode *attack* rata-rata yang dimiliki oleh *graphical password* adalah *shoulder surfing* dan menebak password hingga benar [8].

Selain dari metode *attack* yang relatif masih sedikit, penggunaan *graphical password* juga merupakan salah satu alternatif yang baik dari segi keamanan, penggunaan dan ingatan pengguna [9]. Algoritma yang digunakan untuk membuat sistem Passwle adalah Siamese Neural Network, dimana Siamese Neural Network dipilih, karena algoritma tersebut tidak memerlukan dataset yang banyak ketika melakukan training, sehingga tidak perlu memakai resource yang banyak jika dibandingkan dengan algoritma lainnya. Selain dari alasan tersebut, Siamese Neural Network dipilih karena keterbaruan teknologi, karena Siamese Neural Network sendiri terbilang masih cukup baru karena dibuat pada tahun 2015 [10], sehingga penulis ingin menguji waktu, tingkat akurasi dan keamanan jika sebuah Graphical Password menggunakan Siamese Neural Network. Sistem yang didesain diharapkan bisa menjadi salah satu alternatif dari sistem keamanan tersebut dan bisa meningkatkan keamanan, daya ingat dan kenyamanan pengguna ketika sistem Passwle dipakai dalam kehidupan nyata.

1.2. Identifikasi Masalah

Terdapat beberapa masalah yang ditemukan berdasarkan latar belakang yang telah ditulis oleh penulis. Masalah-masalah yang ditemukan adalah :

1.2.1 Apakah "*Passwle"* memiliki tingkat akurasi dan kecepatan yang cukup baik ketika diimplementasikan ?

1.2.2 Bagaimana tingkat keamanan dari sistem "*Passwle"* ketika digunakan oleh pengguna ?

1.2.3 Bagaimana daya ingat dan kenyamanan dari pengguna ketika menggunakan sistem "*Passwle"* ?

1.2.4 Apakah "*Passwle"* bisa menjadi alternatif dari sistem keamanan yang sudah ada ?

1.3. Batasan Penelitian

Terdapat beberapa batasan yang penulis temukan dalam penelitian ini, yaitu :

1.3.1. Algoritma Siamese Neural Network yang digunakan diambil dari arsitektur Neural Network orang lain bukan arsitektur Neural Network yang dibangun sendiri.

1.3.2. Diperlukan tombol akun Google dan tombol autorisasi untuk menggunakan sistem "Passwle.

1.4. Tujuan Penelitian

Tujuan dari penelitian yang akan dilakukan oleh penulis adalah untuk memberikan alternatif dari sistem-sistem kemanan yang sudah ada, karena sistem-sistem keamanan yang sudah ada mudah untuk diretas dan untuk meningkatkan daya ingat pengguna dari *password* yang dibuat oleh pengguna.

1.5. Manfaat Penelitian

Manfaat yang bisa diberikan dari penelitian ini adalah :

1.5.1. Memberikan alternatif dari Sistem keamanan yang sudah ada.

1.5.2. Meningkatkan keamanan dari sistem yang menggunakan *framework* "Passwle" dan daya ingat pengguna ketika membuat *password*.