BAB I

PENDAHULUAN

1.1 Latar Belakang

Kata sandi merupakan mekanisme penting yang sering digunakan untuk mengautentikasi pada sistem komputer yang bertujuan untuk verifikasi bahwa pengguna tersebut adalah asli, dalam penggunaan kata sandi pengguna harus mengingat banyak kata(Carnut & Hora, dkk., 2021), (Mukherjee dkk., 2023). Kata sandi merupakan alfanumerik dari sekumpulan *string* yang digunakan untuk memvalidasi seorang pengguna yang memiliki hak akses pada suatu sistem komputer dan *platform social media*. Kata sandi sangat diperlukan dalam proses komunikasi dan memberikan keamanan data pengguna (Sandanasamy & Muthulakshmi, dkk., 2014).

Situasi saat ini penggunaan kata sandi sangat penting dalam mengamankan sistem komputer dan *platform social media,* hal ini berfungsi untuk menjaga keamanan informasi pribadi agar terhindar dari pembobolan oleh orang yang tidak bertanggung jawab. Kebanyakan pengguna membuat kata sandi dengan kata yang pendek dan mudah diingat tanpa menyadari kuat lemahnya sehingga keamanan dari akses masih sangat diragukan. Masalah bagi pengguna adalah tidak mengetahui bahwa kata sandi yang telah dibuat memiliki tingkat keamanan yang lemah. Umumnya pengguna dalam pembuatan kata sandi cenderung menggunakan kalimat kata yang pendek dan mengaitkan informasi dirinya seperti nama kesayangan untuk pacarnya, peliharaannya, tempat lahir, tanggal lahir, bahkan dari makanan kesukaannya agar mudah di ingat (Lee dkk., 2006). Penggunaan kata sandi yang

mudah tersebut dapat ditebak oleh orang yang tidak bertanggung jawab karena informasi tersebut tercantum di *platform social media* (Bhana & Flowerday, 2020). Agar dapat terhindar dari penyerang, kata sandi yang lebih baik dibuat dengan menggunakan kalimat kata yang lebih panjang dan lebih sulit ditebak (Mukherjee dkk., 2023). Salah satu metode yang disarankan saat ini untuk meningkatkan keamanan kata sandi yang cukup rumit namun mudah untuk diingat adalah algoritma pembuatan kata sandi acak *Diceware* (Antonov & Georgieva, 2020) (Buchyk dkk., 2021). Hasil penelitian yang dilakukan oleh (Leonhard & Venkatakrishnan, dkk., 2007) menunjukkan bahwa algoritma ini memiliki kekuatan kata sandi yang kuat sehingga layak untuk digunakan.

Diceware merupakan metode acak kata yang dikembangkan oleh Aronld Reinhold, pada penggunaan sebuah kamus yang berfungsi untuk menerjemahkan kode acak kedalam kata-kata umum sehingga menghasilkan frasa kata sandi dan *variable kriptografi* menggunakan dadu sebagai perangkat untuk menghasilkan angka acak. Angka acak yang dihasilkan akan diubah menjadi kode yang kemudian digunakan untuk mencari sebuah kata yang sudah tersedia dalam *wordlist* sehingga menghasilkan kata-kata yang sudah tersedia secara akurat (Buchyk dkk., 2021)(Carnut & Hora, dkk., 2021).

Jaro Winkler Distance merupakan metrik *string* yang digunakan dalam ilmu komputer untuk metode pengukuran kemiripan antara dua urutan, algoritma ini sering digunakan untuk perbandingan *string*, dokumen dan pendeteksian plagiarisme seperti karya tulis ilmiah (Cahyono, 2019),(Aritomatika dkk., 2021). Peneliti terdahulu yang dilakukan oleh tangga dkk., telah melakukan analisis

perbandingan algoritma *Jaro Winkler* dan *Levenshtein Distance* untuk mendeteksi plagiarisme pada dokumen teks, hasil analisis menunjukkan bahwa algoritma *jaro winkler* lebih akurat dalam pengujian nilai *similarity* dan rata-rata waktu pemrosesan (Tannga dkk., 2017).

Alat untuk mengukur kekuatan kata sandi dapat memberikan hasil numerik kepada pengguna seperti '*weak*', '*medium*', '*strong*', dan '*excellent*' (Yıldırım & Mackie, 2019). Ada beberapa hal yang harus diperhatikan agar kata sandi menjadi lebih kuat dan sulit ditebak oleh orang yang tidak bertanggung jawab. Beberapa kriteria yang dapat membantu meningkatkan kekuatan kata sandi adalah kombinasi huruf besar dan kecil, penggunaan angka dan simbol tertentu, dan minimal 8 karakter perkata. Karena keamanan kata sandi yang lebih tinggi, kata sandi yang lebih panjang juga akan lebih aman.

Penelitian sebelumnya yang berjudul "*Diceware Password Generation Algorithm Modification based on Pseudo-Random Sequences*" telah melakukan pembuatan kata sandi menggunakan algoritma *Diceware* yang dimodifikasi menggunakan *based on pseudo-random sequence*, hasilnya menunjukkan bahwa modifikasi algoritma tahan terhadap serangan, tetapi terdapat kekurangan dalam meningkatkan daya ingat terhadap kata sandi yang telah di hasilkan (Buchyk dkk., 2021).

Berdasarkan uraian tersebut, masih memiliki peluang pengembangan penelitian tentang pembuatan kata sandi menggunakan algoritma *Diceware* dengan pengukuran *similarity* menggunakan algoritma *Jaro Winkler* yang berfungsi untuk

pengukur kemiripan hasil kata sandi serta pengukuran *password strength* yang dapat membantu penilaian tingkat kekuatan kata sandi.

1.2 Rumusan Masalah

Berdasarkan latar belakang di atas, maka dapat dirumuskan masalah dalam penelitian ini adalah :

1. Bagaimana mengimplementasikan algrotima *Jaro Winkler Distance* untuk mengukur *Memorability* pada *passphrase* yang dihasilkan Algoritma *Diceware*.?
2. Bagaimana mengimplementasikan Algoritma *Password strength* untuk mengukur tingkat kekuatan pada *passphrase* yang dihasilkan Algoritma *Diceware*.?

1.3 Batasan Masalah

1. Jumlah dadu yang digunakan hanya 3 buah.
2. *Wordlist* yang dibangun terdiri dari 3 *file txt*, masing-masing menyimpan *maximal* 216 kata.
3. Frasa kata sandi yang dihasilkan terdiri dari 3 kata yang diambil dari *wordlist*
4. Pengukuran *memorability* hanya mengacu pada kemiripan (*similarity*) kata dalam frasa yang dihasilkan dengan menggunakan algoritma *diceware*.

1.4 Tujuan Penelitian

1. Melakukan pengukuran *memorability* pada *passphrase* yang dihasilkan Algoritma *Diceware* dengan pendekatan perhitungan *similarity* menggunakan Algortima *Jaro Winkler Distance*
2. Melakukan pengukuran tingkat kekuatan pada *passphrase* yang dihasilkan Algoritma *Diceware*.

1.5 Manfaat Penelitian

Penelitian ini diharapkan dapat bermanfaat bagi pengguna yang terkait diantaranya adalah :

1. Memberi kontribusi terhadap pembuatan *generator* kata sandi
2. Mempermudah pengguna untuk mendapatkan kata sandi dengan kalimat yang baik dan mudah diingat dengan kekuatan kata sandi yang kuat