1. Pendahuluan

1.1. Latar Belakang

Jumlah pengguna *smartphone* secara global mengalami kenaikan yang signifikan, selama satu dekade terakhir. Pada tahun 2023 diperkirakan jumlah pengguna *smartphone* menembus angka 5,25 miliar pengguna dan akan terus bertambah[1]. Pertumbuhan pengguna *smartphone* yang signifikan ini diikuti juga dengan pesatnya perkembangan teknologi dalam hal penyimpanan dan pertukaran data. Hal tersebut menjadi perhatian khusus tentang bagaimana data-data pengguna *smartphone* mendapatkan perlindungan akses sehingga keamanan datanya terjamin.

Umumnya, perlindungan akses pengguna pada *smartphone* menggunakan sistem *authentication* yang masih konvensional seperti *personal identification numbers* (PINs) atau *password*[2]. Sistem *authentication* yang konvensional atau *password-based authentication* memang mudah sekali untuk diimplementasikan dan dikembangkan[3]. Di sisi lain, sistem *authentication* tersebut memiliki kelemahan, di mana sistem melakukan *authentication* pengguna melalui sebuah teks atau beberapa karakter. Hal tersebut berarti pengguna tidak dikenali secara *authentic* sebagai siapa, tetapi pengguna dikenali atas apa yang diketik dan dicocokkan dengan *password* yang sebelumnya sudah disimpan di sistem[2], [4]. Hal ini membuat *password* dapat dengan mudah dicuri, karena berbentuk *fixed-text* atau teks yang tetap. Kelemahan tersebut bisa menjadi celah keamanan, karena seharusnya hanya pengguna yang *legitimate* saja yang memiliki akses untuk masuk ke dalam sistem[2], [3].

Untuk mengatasi masalah kelemahan tersebut, ditambahkan kombinasi sistem *authentication* lain, salah satunya adalah *biometric*. *Biometric* dibagi menjadi dua karakteristik, *biological* dan *behavioral*[4], [5]. Umumnya karakteristik *biological* seperti, sidik jari, gambar wajah, dan iris. Berbeda dengan karakteristik *biological*, karakteristik *behavioral* berbasiskan pola perilaku seperti, tanda tangan, pola dalam mengetik (*keystroke*), dan pergerakan bibir ketika berbicara[5].

Penelitian mengenai *keystroke biometric* sudah banyak dilakukan. Salah satunya menggunakan metode *Siamese Network*s yang berbasiskan *convolutional neural network* (CNN) untuk menghasilkan dua buah vektor yang akan digunakan untuk menghitung *Manhattan distance* dan *Mahalanobis distance*. Hasilnya didapatkan performansi *equal error rate* (EER) sebesar 31% dengan menggunakan 200 data *keystroke*[6]. Penelitian lainnya juga membahas tentang peningkatan efisiensi algoritma *keystroke biometric* dengan melakukan modifikasi pada rumus perhitungan *Manhattan distance*. Modifikasi rumus tersebut bertujuan untuk mengurangi nilai EER. Sebelum rumus *Manhattan distance* dimodifikasi, nilai EER yang diperoleh sebesar 5,32%, sementara setelah modifikasi, nilai EER turun menjadi 3,27%. Artinya, nilai EER mengalami *enhancement* sebesar 38.53%[7]. *Distance similarity* sangat umum digunakan dalam penelitian *keystroke biometric* karena dapat mengukur perbedaan antara pola ketikan pengguna[8]. Pada penelitian-penelitian *keystroke biometric* yang menggunakan *distance similarity*, ditemukan beberapa masalah. Salah satunya, penelitian yang menggunakan metode *Euclidean distance* mendapatkan nilai akurasi yang lebih rendah dibandingkan dengan metode *distance similarity* lainnya[11]. Oleh karena itu, penelitian lebih lanjut diperlukan untuk mengeksplorasi metode pengukuran alternatif yang dapat meningkatkan akurasi sistem *keystroke biometric* dan menjaga keamanan data dengan lebih efektif.

1.2. Topik dan Batasannya

Berdasarkan latar belakang permasalahan di atas, dapat dirumuskan masalah sebagai berikut:

1. Bagaimana implementasi dan efektivitas beragam metode *distance similarity* dalam sistem *keystroke biometric* dengan *user-adaptive* fitur?
2. Bagaimana performansi sistem *keystroke biometric* dengan *user-adaptive* fitur yang menggunakan beragam metode *distance similarity* dalam mengurangi tingkat kesalahan (EER, FAR, dan FRR)?

Agar penelitian tidak melebar, batasan masalah pada penelitian ini adalah:

1. *Dataset* yang digunakan adalah *dataset* dari Aalto University.
2. Rentang nilai *distance similarity* yang digunakan adalah 0-1. Nilainya menyesuaikan sebaran data yang digunakan.
3. Sistem *keystroke biometric* yang dibangun menggunakan data *free-text* dan tidak mencakup data *fixed-text*.

1.3. Tujuan

Berdasarkan latar belakang dan perumusan masalah di atas, maka tujuan dari penelitian ini adalah:

1. Mengevaluasi efektivitas beragam metode *distance similarity* dalam sistem *keystroke biometric* dengan *user-adaptive* fitur.

2. Menganalisis performansi sistem *keystroke biometric* dengan *user-adaptive* fitur yang menggunakan beragam metode *distance similarity*, dalam hal *equal error rate* (EER), *false acceptance rate* (FAR), dan *false rejection rate* (FRR).

1.4. Organisasi Tulisan

Setelah memaparkan pendahuluan pada bagian pertama, bagian kedua akan membahas kajian terkait *keystroke biometric*, termasuk perhitungan performansinya. Pada bagian ketiga, fokus akan beralih ke sistem yang dikembangkan, termasuk deskripsi *dataset* dan analisis performansi. Bagian keempat akan menyajikan evaluasi, meliputi skenario pengujian, hasil pengujian, dan analisis dari hasil pengujian tersebut. Terakhir, bagian kelima akan menyajikan kesimpulan dan saran dari penelitian ini.