1. Pendahuluan

1.1 Latar Belakang

Saat ini, perkembangan dunia digital berkembang sangat pesat, khususnya pada pertukaran dan penyimpanan data. Hal ini menyebabkan, perlindungan akses pada data menjadi suatu hal yang sangat penting, karena kemudahan akses pada data-data tersebut. Perlindungan akses secara konvensional itu ada sangat banyak contohnya, seperti PIN, kata sandi, dan kartu identitas[1]. Adapun perlindungan akses tersebut memiliki beberapa kekurangan, contohnya pada PIN dan kata sandi kita harus selalu mengingatnya. Lalu dengan kartu identitas juga harus selalu dibawa, rentan untuk hilang maupun diduplikasi[1]. Oleh karena itu hadir perlindungan baru yang datang sebagai alternatif yaitu Biometrik, biometrik sendiri menawarkan beberapa kelebihan yang tidak dimiliki oleh perlindungan akses konvensional, seperti tidak perlunya mengingat akan sesuatu maupun harus membawa barang fisik kemana-mana karena dengan biometrik melalui ciri fisik maupun tingkah laku dari orang tersebut.

Biometrik merupakan cara mengidentifikasi maupun mengautentikasi seseorang berdasarkan ciri fisik maupun tingkah laku dari orang tersebut. Biometrik sendiri memiliki performa yang lebih rendah dibandingkan dengan perlindungan akses secara konvensional yang ada[1]. Walaupun demikian ada beberapa permasalahan pada Biometrik terkait privasi dan kebersihan atau kehigienisan perangkat[2], [3]. Dimana data fisik seseorang harus disimpan pada beragam sistem biometrik. Sedangkan terkait kebersihan ini sudah dikembangkan Biometrik yang *touchless* seperti *face recognition*, *vein*, dan lain-lain[4]. Untuk menangani persoalan privasi pada Biometrik, dikembangkan penelitian berdasarkan ciri dinamis atau tingkah laku. Dimana ciri ini tidak melekat permanen pada seseorang, karena sifatnya yang dinamis dan bisa berubah pada waktu yang lama[5]. Beberapa biometrik dinamis yang ada seperti *gaze*, *iris*, dan sidik jari, biometrik tersebut mengandalkan perangkat khusus dan memiliki biaya tidak murah. Dikarenakan alasan tersebut, dikembangkanlah sebuah biometrik yang tidak mengandalkan perangkat khusus dan memiliki biaya yang lebih terjangkau, yaitu *Keystroke*. Melalui biometrik *Keystroke* didapatkan ciri seorang pengguna berdasarkan perilaku ketika mengetik teks pada perangkat[5].

Keystroke sendiri merupakan biometrik dinamis yang berdasarkan kepada pola seseorang selama pengetikan teks atau *typing pattern* pada suatu perangkat komputer atau *mobile*. Mengenai penelitian *keystroke* biometrik sendiri sudah banyak dilakukan, contohnya ada yang menggunakan penggabungan dari *Instance-based* mendapatkan hasil dibawah dari 10% *Equal Error Rates* (ERRs) untuk lebih dari 1000 *keystroke* yang ada[6]. Dimana pada penelitian selanjutnya dengan distance metric fusion dari tiga. Mendapatkan EER 34.3% untuk 100 *digraph*, EER 15.3% untuk 200 dan EER 3.6%. untuk 1000 *digraph*[7]. Selanjutnya ada dua penilitian yang menggabungkan *convolutional neural network* (CNN) dan *recursive neural network* (RNN)[8], [9]. Dimana penelitian pertamanya menggunakan satu dataset yaitu dari peniliti di SUNY Buffalo, dengan dataset tersebut mendapatkan hasil FRR = 1.95%, FAR = 4.12% dan EER 3.04%[8]. Penelitian kedua menggunakan dua dataset publik yang ada, yaitu Clarkson II dan Buffalo. Didapatkan hasil untuk dataset Buffalo FRR = 1.89%, FAR = 2.83% dan EER 2.83%. Untuk dataset Clarkson II mendapatkan hasil FRR = 6.61%, FAR = 5.31%, EER = 5.97%[9]. Pada penelitian terbaru dengan menggunakan *instance-based tail area density* (ITAD), ITAD mendapatkan hasil EER dibawah 10% dari 200 digraph. ITAD terbukti mampu mereduksi kebutuhan *keystroke* dalam autentikasi[10]. *Similarity score* dari lima fitur yang ada digabungkan dengan nilai ITAD, dan hasilnya sendiri dua kali lebih cepat dibandingkan dengan *state-of-the-art* yang ada sebelumnya[10]. Oleh karena itu pada penelitian ini mengimplementasi penggunaan ITAD pada biometrik *keystroke*, dengan dataset yang berasal dari Aalto University[11] dan Biomey *Keystroke* Dataset yang dikumpulkan pada penelitian ini.

1.2 Perumusan Masalah

Berdasarkan latar belakang diatas, maka dapat dirumuskan beberapa masalah yaitu pertama bagaimana mengimplementasikan ITAD pada autentikasi pengguna dengan *keystroke* biometrik. Permasalahan kedua yaitu mengenai bagaimana performansi autentikasi pengguna dengan *keystroke* biometrik. Adapun batasan masalah pada penilitian ini dimulai dari sistem yang dibangun adalah autentikasi biometrik, dan dataset yang digunakan adalah dataset dari Aalto University[11] dimana jumlah pengguna yang digunakan dibatasi sebesar 1000 pengguna, dikarenakan dataset ini banyak memiliki atribut yang kosong dan pengecekannya membutuhkan waktu yang lama. Selain itu, dataset lainnya yang digunakan yaitu Biomey *Keystroke* Dataset.

1.3 Tujuan

Berdasarkan dari rumusan masalah yang sudah ditentukan diatas, didapatkan tujuan pada penilitian ini yaitu pertama mengetahui cara mengimplementasikan ITAD pada autentikasi pengguna dengan *keystroke* biometrik.

Dan tujuan selanjutkan untuk mengetahui performansi dari autentikasi pengguna dengan *keystroke* biometrik pada dataset yang digunakan.

1.4 Organisasi Tulisan

Setelah pendahuluan pada bagian pertama, pada bagian kedua berisikan studi terkait mengenai Biometrik hingga perhitungan performansi pada Biometrik. Selanjutnya pada bagian ketiga membahas mengenai sistem yang dibangun, dataset dan performansi. Bagian keempat evaluasi yang didalamnya terdapat skenario pengujian, hasil pengujian dan analisa pengujian. Pada bagian kelima atau terakhir berisi mengenai saran dan kesimpulan dari penelitian ini.