

1. Pendahuluan

1.1 Latar Belakang

Autentikasi sangatlah penting bagi sistem informasi, seiring dengan transformasi digital data, baik itu data sensitif maupun pribadi, membuat perlindungan data pengguna menjadi suatu hal yang sangatlah penting. Saat ini, masih banyak sekali sistem yang menggunakan keamanan dengan mekanisme tradisional yang berbasis pengetahuan, seperti PIN, Kata Sandi maupun berbasis Token [1][2]. Kekurangan dalam metode tersebut adalah pengguna cenderung memilih kata sandi yang pendek dan mudah diingat yang menjadikan kata sandi mudah ditebak, selain itu kecenderungan penggunaan kata sandi yang sama untuk beberapa akun, serangan bruteforce, serangan Keylogger, dan lain sebagainya [3][4][5]. Pendekatan alternatif yang bisa digunakan yaitu Biometrik, Media autentikasi yang menggunakan ciri fisik dan tingkah laku dari pengguna, sehingga pengguna tidak perlu mengingat ataupun membawa media autentikasi [1]. Ciri fisik memiliki kelemahan terhadap serangan spoofing atau kebutuhan perangkat yang mahal [6]. Ciri tingkah laku yang memiliki kekurangan karena sifat dinamis yakni adanya adaptasi dan menunjukkan ketidakstabilan atau berfluktuasi karena beberapa faktor temporer sesuai dengan kondisi emosional pengguna, sehingga berdampak pada rendahnya hasil autentikasi [7]. Sifat dinamis dari Biometrik ini berpotensi menjadi suatu kelebihan atau kekuatan bahwa ciri biometrik ini susah untuk ditiru karena karena sifatnya yang dinamis. Hal ini akan tercapai apabila hasil ciri yang diekstraksi merupakan ciri yang dinamis, bukan tentang apa yang pengguna ketik, melainkan bagaimana pengguna mengetik [8]. *Keystroke dynamic* (KD) merupakan salah satu metode autentikasi pengguna berbasis perilaku seseorang pada saat pengetikan suatu teks tertentu [7]. Secara umum ciri perilaku diperoleh dari ritme jari ketika menekan dan melepas tombol pada perangkat mobile atau komputer. KD menawarkan biaya yang lebih hemat, nyaman digunakan, dan tidak memerlukan perangkat tambahan karena sudah terdapat pada perangkat mobile atau komputer [7][9]. Penelitian terkait KD terdapat pada [10], metode User-Adaptive diperkenalkan sebagai metode ekstraksi fitur dalam sistem KD yang memanfaatkan kecepatan dan ciri perilaku mengetik pengguna (digraf). Penelitian tersebut menunjukkan bahwa metode User-Adaptive dapat meningkatkan akurasi sebesar 44% lebih baik dari penelitian sebelumnya.

Autentikasi dilakukan dengan membandingkan antara fitur hasil ciri ekstraksi yang diperoleh dengan fitur ciri ekstraksi yang terdaftar dalam sistem. Perbandingan tersebut akan diperoleh nilai jarak yang mana penghitungan jarak menggunakan *distance-based*, penerapan tersebut telah dilakukan pada sejumlah penelitian sebelumnya. Salah satu *distance-based* yang digunakan terdapat pada penelitian [11], Mahalanobis Distance digunakan untuk *generate threshold* yang nantinya diolah untuk penerapan empat klasifikasi yang berbeda diantaranya Random Forest, Isolation Forest, Gradient Boosting, dan SVM. Akurasi terbaik yang didapat adalah 90% dari model klasifikasi Isolated Forest. Penerapan autentikasi dengan enam metode *distance-based* yang berbeda telah dilakukan pada penelitian [12], beberapa diantaranya ITAD, KDE, Manhattan Distance, Scaled Manhattan Distance, Mahalanobis Distance dan Transformed Mahalanobis Distance dengan menggunakan Clarskson II Dataset. Penelitian tersebut menerapkan teknik *fusion* pada fitur waktu dan diperoleh Equal Error Rate (EER) terbaik sebesar 12,3% pada metode ITAD, dan Mahalanobis Distance memperoleh Equal Error Rate (EER) sebesar 22%.

Tujuan Penelitian ini adalah mengeksplorasi lebih lanjut mengenai Mahalanobis Distance, tidak hanya untuk mendapatkan *threshold* tetapi juga untuk autentikasi, selain itu dengan menggunakan metode User-Adaptive sebagai *feature extraction* dapat membuka potensi bagi Mahalanobis Distance sebagai *feature matching* untuk mendapatkan hasil yang lebih baik dengan menggunakan Biomey Biometrics Dataset.

1.2 Topik dan Batasannya

Berdasarkan topik penelitian yang sudah di teliti oleh penulis, maka dapat dirumuskan beberapa masalah sebagai berikut, yaitu menerapkan User-Adaptive pada *keystroke biometric* dengan Mahalanobis Distance dan mengetahui performansi Multimodal dari User-Adaptive pada *keystroke biometrics* dengan Mahalanobis Distance. Batasan masalah pada penelitian ini digunakan autentikasi biometrik berupa penekanan tombol keyboard pada perangkat *smartphone*, dengan *dataset* yang digunakan adalah Biomey Biometric Dataset yang melibatkan pengguna sebanyak 40 Responden yang melakukan pengetikan pada aplikasi khusus [17].

1.3 Tujuan

Tujuan penelitian ini untuk menerapkan User-Adaptive pada *keystroke biometrics* dengan Mahalanobis Distance dan mengetahui performansi multimodal dari User-Adaptive pada *keystroke biometrics* dengan Mahalanobis Distance.

1.4 Organisasi Tulisan

Pada bab selanjutnya, studi terkait menjelaskan beberapa studi terdahulu dan definisi metode terkait dengan penelitian ini. Bab 3 mencakup penjelasan sistem yang dibangun dan langkah-langkahnya, dilanjutkan dengan bab evaluasi yang menjelaskan beberapa skenario yang dilakukan dan menampilkan hasil yang didapat. Bab terakhir merupakan kesimpulan dari penelitian ini dan harapan untuk penelitian kedepan.