1. Pendahuluan

1.1 Latar Belakang

Perkembangan teknologi yang pesat selama beberapa dekade terakhir telah berkontribusi dalam peningkatan penyimpanan dan akses data pada perangkat digital. Akses tidak sah terhadap data tersebut dapat menyebabkan kerugian finansial, dan kebocoran data sensitif yang mengancam keamanan informasi [1]. Akibatnya, kebutuhan akan sistem perlindungan data yang efisien menjadi semakin mendesak. Di antara berbagai metode perlindungan data, autentikasi merupakan aspek penting dalam menjaga keamanan data. Saat ini, sistem autentikasi sering bergantung pada sesuatu yang kita ketahui dan/atau miliki seperti penggunaan kata sandi, *personal identification number* (PIN), serta kartu identitas [2, 3, 4]. Namun autentikasi jenis ini dapat dengan mudah hilang, di manipulasi, atau dicuri sehingga menimbulkan berbagai risiko keamanan. [2, 4].

Untuk mengatasi kekurangan tersebut teknologi biometrik banyak dikembangkan sebagai alternatif maupun lapisan keamanan tambahan guna melengkapi sistem autentikasi yang sudah ada [1, 4]. Biometrik memanfaatkan karakteristik fisik dan perilaku unik manusia untuk mengidentifikasi individu yang berbeda. Karakteristik biometrik yang sulit untuk dipalsukan atau dicuri menawarkan tingkat keamanan yang lebih tinggi [5]. Biometrik fisik seperti sidik jari, pengenalan wajah, dan iris memiliki keterbatasan dalam situasi tertentu, seperti kondisi pencahayaan buruk atau cedera pada bagian tubuh yang dipindai [6]. Selain itu, sistem autentikasi berbasis biometrik fisik memerlukan perangkat keras tambahan yang tentunya menambah biaya dan kompleksitas proses autentikasi pengguna [3, 6]. Sebagai alternatif, biometrik berbasis perilaku *keystroke dynamics* yang merupakan pola pengetikan individu pada perangkat digital, menjadi solusi yang lebih praktis dan ekonomis karena tidak memerlukan perangkat tambahan [2, 3, 6].

Sejumlah penelitian terkait *keystroke dynamics* untuk mengidentifikasi dan autentikasi pengguna telah dilakukan menggunakan berbagai jenis fitur dan algoritma [7, 8, 9]. Penelitian [7] melakukan autentikasi pengguna yang menerapkan ekstraksi fitur dengan membagi *keyboard* menjadi tiga bagian, yaitu tombol yang ditekan tangan kiri (L), tombol yang ditekan tangan kanan (R), dan tombol spasi (S). Penelitian ini menunjukkan metode yang digunakan dapat meningkatkan akurasi autentikasi pada tiga perangkat berbeda, PC *keyboard*, *soft keyboard,* dan *touch keyboard*. Sementara itu, penelitian [8] membandingkan kinerja berbagai model *machine learning* untuk autentikasi pengguna berbasis *keystroke dynamics*, di mana model XGBoost menunjukkan performa terbaik dengan akurasi mencapai 96,39%. Penelitian [9] memperkenalkan metode ekstraksi fitur *Distance Enhanced Flight-Time* (DEFT) dengan memperhitungkan jarak antara tombol pada *keyboard* ketika mengukur waktu antara tombol yang ditekan. Penelitian tersebut menggabungkan fitur DEFT dengan fitur-fitur yang digunakan dalam penelitian sebelumnya, dan hasilnya menunjukkan peningkatan akurasi autentikasi yang signifikan. Pada perangkat *desktop*, *mobile*, dan *tablet*, penelitian ini berhasil mencapai akurasi di atas 99% dan EER di bawah 10%.

Pada penelitian ini dilakukan eksplorasi lebih lanjut terkait metode ekstraksi fitur DEFT dalam membangun sistem *keystroke dynamics-based authentication* (KDA). Selain itu, model klasifikasi XGBoost digunakan untuk melakukan autentikasi berdasarkan hasil ekstraksi fitur dari metode DEFT tersebut.

1.2 Topik dan Batasannya

Berdasarkan latar belakang yang telah dijelaskan, rumusan masalah dalam penelitian ini berfokus pada dua hal. Pertama, bagaimana cara mengimplementasikan metode DEFT pada sistem autentikasi pengguna berbasis *keystroke*. Kedua, bagaimana performa metode DEFT pada sistem KDA dengan menggunakan *dataset* Biomey. Penelitian ini dilakukan dengan beberapa batasan. Sistem biometrik yang dikembangkan berfokus pada autentikasi atau verifikasi, sehingga hasil autentikasi akan menentukan apakah pengguna adalah pengguna sah (*genuine*) atau tidak sah (*impostor*). Penelitian ini menggunakan pendekatan yang berbeda dari penelitian sebelumnya [9], dengan mempertimbangkan tidak hanya pola pengetikan pada masing-masing tangan tetapi juga pola pengetikan saat pengguna melakukan perpindahan tangan sehingga memberikan cakupan yang lebih luas dan lebih representatif terhadap variasi pola pengetikan. *Dataset* yang digunakan dalam penelitian ini juga berbeda, di mana d*ataset* yang digunakan dalam penelitian ini adalah Biomey *keystroke dataset*, yang melibatkan 40 partisipan dalam 30 sesi pengambilan menggunakan aplikasi pada perangkat *smartphone*. Selain itu, metrik performansi yang digunakan untuk evaluasi adalah *false acceptance rate* (FAR), *false rejected rate* (FRR), *equal error rate* (EER) serta ROC-AUC.

1.3 Tujuan

Tujuan dari penelitian ini adalah untuk mengimplementasikan metode DEFT pada sistem KDA, serta mengevaluasi performansi sistem menggunakan *dataset* Biomey. Penelitian ini diharapkan dapat memberikan wawasan mengenai kinerja metode DEFT dalam sistem autentikasi berbasis *keystroke dynamics.*

1.4 Organisasi Tulisan

Setelah bagian pendahuluan, penelitian ini dilanjutkan dengan tinjauan pustaka yang menguraikan literatur terkait seperti *keystroke dynamics* dan metode DEFT. Selanjutnya, bagian rancangan sistem menjelaskan tahap-tahap pembangunan sistem KDA serta pemilihan *dataset* yang digunakan. Pada bagian Evaluasi, skenario pengujian serta hasil eksperimen dipaparkan beserta analisis dari hasil pengujian tersebut. Bagian kesimpulan merangkum hasil penelitian dan memberikan rekomendasi untuk penelitian lanjutan. Terakhir, Daftar Pustaka mencantumkan referensi yang digunakan, dan lampiran berisi data tambahan yang mendukung penelitian.