BAB I
PENDAHULUAN

1.1. Latar Belakang

Seiring perkembangan teknologi, institusi pendidikan tinggi semakin memanfaatkan sistem berbasis web untuk mendukung aktivitas administratif dan pembelajaran. Teknologi ini menawarkan efisiensi dalam pengelolaan data, termasuk data pribadi mahasiswa. Namun, dengan semakin banyaknya data yang disimpan dan diakses secara *online*, keamanan informasi menjadi perhatian utama. Berbagai ancaman seperti serangan siber dan kebocoran data semakin meningkat, dan salah satu tantangan terbesar adalah menjaga keamanan data pribadi dari akses yang tidak sah. Oleh karena itu, keamanan sistem, terutama dalam autentikasi pengguna, harus ditingkatkan untuk mengurangi risiko ini.

Penggunaan kata sandi sebagai metode autentikasi masih menjadi salah satu titik lemah dalam sistem keamanan. Berdasarkan penelitian yang dilakukan oleh Alqahtani [1], yang meneliti kesadaran keamanan siber di kalangan mahasiswa, sekitar 41% tidak setuju dengan perubahan kata sandi secara periodik, 39% menggunakan kata sandi lama untuk membuat kata sandi baru, dan 30% memilih satu kata sandi untuk semua *website* karena tidak ingin menghafal banyak kata sandi panjang untuk setiap *website*. Kondisi ini meningkatkan risiko kebocoran data, terutama jika salah satu platform yang mereka gunakan diretas. Dampaknya tidak hanya terbatas pada keamanan data individu, tetapi juga dapat memengaruhi reputasi institusi.

Kebocoran atau hilangnya data pribadi mahasiswa dapat menimbulkan risiko serius bagi individu yang terlibat serta dapat merusak reputasi universitas [2]. Selain itu, hilangnya kepercayaan pada keamanan sistem dapat menghambat penerapan teknologi dalam proses pembelajaran dan administrasi kampus. Oleh sebab itu, universitas harus memperhatikan pentingnya keamanan, terutama dalam proses autentikasi pengguna. Penggunaan autentikasi yang lebih aman dan akurat sangat diperlukan untuk mencegah terjadinya insiden kebocoran data yang merugikan.

Sebagai solusi terhadap tantangan tersebut, autentikasi biometrik dapat diterapkan sebagai alternatif dari penggunaan kata sandi. Autentikasi biometrik memanfaatkan karakteristik fisik atau perilaku unik individu, seperti sidik jari, wajah, atau pola suara, untuk verifikasi identitas [3]. Teknologi ini dianggap lebih aman karena setiap individu memiliki ciri khas yang sulit untuk ditiru atau dicuri.

Pengenalan wajah merupakan salah satu bentuk autentikasi biometrik yang diakui paling efektif dan cepat [4]. Selain itu, pengenalan wajah merupakan autentikasi biometrik yang lebih akurat dibanding biometrik lainnya dalam mengidentifikasi seseorang karena wajah memilikir fitur yang unik dan sulit [5]. Fitur dalam wajah tidak dapat di duplikasi, dicuri atau dilupakan [6]. Kecepatan dan keakuratan pengenalan wajah menjadikannya pilihan unggulan dalam sistem autentikasi, terutama dalam lingkungan yang membutuhkan keamanan tinggi dan kemudahan penggunaan.

Terdapat beberapa penelitian yang mendukung penggunaan pengenalan wajah dalam berbagai aplikasi. Pada penelitian yang dilakukan oleh Dewanto, dkk. [7] telah membahas tentang perbandingan efektivitas YOLO (You Only Look Once) dan CNN (*Convolutional Neural* Network) untuk pengenalan wajah bermasker secara *real-time*. Peneliti menggunakan algoritma YOLOv5 bersama ResNet100 dan Haar Cascade bersama CNN. Dari hasil penelitian didapatkan hasil bahwa CNN mencapai akurasi 99,3% untuk pengenalan wajah bermasker, dan 97,3% untuk wajah tidak bermasker. CNN juga memperoleh skor F1 sebesar 0,97 dan frame ratenya 3,57. Sedangkan YOLO mencapai akurasi yang lebih rendah yaitu 79,3% untuk wajah bemasker dan 81,3% untuk wajah tanpa masker. Namun, YOLO memiliki skor F1 yang lebih tinggi yaitu 1,00 dan frame rate yang lebih besar yaitu 3,67 FPS. Peneliti telah menyarankan bahwa peningkatan kualitas data dan kuantitas data dapat menjadi langkah efektif untuk meningkatkan akurasi model. Penelitian ini memberikan peluang untuk pengembangan lebih lanjut, terutama dalam meningkatkan akurasi YOLO tanpa mengorbankan keunggulannya dalam hal kecepatan.

Selain itu, pada penelitian yang dilakukan oleh Sanchez-Moreno, dkk. [8] telah membahas tentang pengenalan wajah menggunakan berbagai model dan algoritma. Peneliti menggunakan berbagai algoritma untuk melakukan deteksi

wajah seperti VJ, MTCNN, dan YOLO-Face (berdasar YOLOv3). Peneliti juga menggunakan berbagai model untuk pengenalan wajah seperti FaceNet+SVM, FaceNet+KNN, dan FaceNet+RF. Hasil penelitian menunjukkan bahwa YOLO-Face memiliki nilai *precision, recall,* dan *accuracy* yang paling konsisten dalam deteksi wajah. Sementara itu, FaceNet+SVM mencapai hasil rekognisi terbaik dengan akurasi sebesar 99,7%. Penelitian ini menunjukkan bahwa algoritma YOLO dan FaceNet dapat menjadi kombinasi yang baik dalam pengenalan wajah. Namun, algoritma YOLO yang digunakan sudah tergolong lama, sehingga ada peluang untuk meningkatkan akurasi dengan teknologi terbaru seperti YOLOv8.

YOLOv8 telah menunjukkan kemampuan luar biasa dalam mendeteksi objek, termasuk dalam aplikasi deteksi masker wajah. Dalam penelitian yang dilakukan oleh Dewi, dkk. [9] didapatkan hasil bahwa YOLOv8 mampu mendeteksi masker secara baik, ditunjukkan dengan akurasi sebesar 99,1%. Kemampuan ini menunjukkan potensi YOLOv8 untuk diterapkan dalam deteksi wajah, terutama jika digabungkan dengan teknologi seperti InceptionResNet untuk pengenalan wajah yang lebih akurat.

Selain itu juga terdapat penelitian oleh Warot Moungsouy, dkk. [10] yang membahas tentang pengenalan wajah dalam skenario penggunaan masker menggunakan algoritma MTCNN dan InceptionResNetV1. Dari hasil penelitian didapatkan akurasi model sebesar 99,2% dalam pengenalan wajah menggunakan masker. Dari penelitian ini didapatkan bahwa InceptionResNetV1 merupakan model yang baik dalam pengenalan wajah menggunakan masker. Sehingga model ini memiliki peluang yang baik untuk melakukan tugas pengenalan wajah tanpa masker.

Selanjutnya, terdapat penelitian oleh Sikarwar, dkk. [11] yang membahas sistem verifikasi biometrik berbasis pengenalan wajah untuk meningkatkan keamanan dan efisiensi organisasi. Sistem ini menggunakan pipeline Zero-DCE untuk peningkatan kualitas gambar, MTCNN untuk deteksi wajah, dan InceptionResNetV1 untuk menghasilkan *embeddings* wajah. Dataset yang digunakan adalah Faces94 dan Grimace dari University of Essex. Aplikasi ini dikembangkan menggunakan framework Kivy. Hasil pengujian menunjukkan akurasi sebesar 96,76%, dengan keunggulan utama berupa kecepatan dan

skalabilitas karena sistem tidak memerlukan pelatihan ulang saat pengguna baru ditambahkan. Penelitian ini menjadi relevan sebagai pembanding karena menggunakan pipeline lengkap dari deteksi hingga verifikasi wajah, meskipun model deteksi dan antarmuka yang digunakan masih dapat ditingkatkan dengan pendekatan terbaru seperti YOLOv8 dan *web-based interface*.

Sebagai solusi inovatif, integrasi YOLOv8 dan InceptionResNetV1 menawarkan peningkatan signifikan dalam sistem pengenalan wajah. YOLOv8 dapat digunakan untuk mendeteksi wajah dengan cepat dan akurat dalam berbagai kondisi, sedangkan InceptionResNetV1 berperan dalam mengenali identitas individu melalui ekstraksi fitur wajah yang unik. Dengan gabungan kedua teknologi ini, sistem pengenalan wajah tidak hanya akan lebih akurat, tetapi juga lebih efisien dalam memproses data gambar berukuran besar, sehingga cocok untuk diterapkan dalam sistem autentikasi mahasiswa berbasis web. Inovasi ini diharapkan mampu mengatasi kelemahan-kelemahan penelitian sebelumnya, khususnya dalam hal kecepatan, akurasi, dan skalabilitas.

1.2. Rumusan Masalah

Berdasarkan penjelasan latar belakang yang telah disampaikan, rumusan masalah dalam penelitian ini dapat dirumuskan sebagai berikut:

1) Bagaimana mengimplementasikan deteksi wajah untuk autentikasi *login* mahasiswa menggunakan YOLOv8?
2) Bagaimana mengimplementasikan pengenalan wajah untuk autentikasi *login* mahasiswa menggunakan InceptionResNetV1?
3) Bagaimana performa pengenalan wajah antara menggunakan *pretrained* dataset VGGFace2 dan CASIA-WebFace?

1.3. Batasan Masalah

Batasan masalah menjadi aspek penting dalam penelitian untuk menghindari ruang lingkup yang terlalu luas. Berikut adalah beberapa pembatasan masalah yang diterapkan dalam penelitian ini:

1) Pengambilan data wajah dilakukan hanya pada 67 mahasiswa Program Studi Sains Data UPN "Veteran" Jawa Timur sebagai sampel penelitian
2) Proses pengenalan wajah hanya dilakukan di lingkungan dengan pencahayaan normal atau cukup, tidak mencakup kondisi minim atau ekstrem cahaya
3) Deteksi wajah dilakukan menggunakan model yolov8n-face.pt secara langsung tanpa pelatihan ulang (*retraining*)
4) Penelitian membandingkan dua model *embedding* wajah yang masing-masing menggunakan *pretrained* dataset VGGFace2 dan CASIA-WebFace
5) Data wajah yang digunakan dalam penelitian ini terbatas pada citra dua dimensi (2D), tanpa mempertimbangkan data tiga dimensi (3D)
6) Penelitian tidak mencakup pengujian terhadap *spoofing attack*, seperti membedakan antara wajah asli dan gambar atau rekaman wajah
7) Data wajah yang digunakan tidak mencakup kondisi dengan aksesoris seperti kacamata, masker, atau pencahayaan ekstrem
8) Implementasi *website* dalam penelitian ini hanya berjalan secara lokal (*localhost*) dan tidak diunggah ke server publik atau internet

1.4. Tujuan Penelitian

Tujuan dari penelitian ini adalah untuk menjawab rumusan masalah serta memberikan arahan yang lebih jelas bagi penelitian ini. Dengan menggabungkan model YOLOv8 dan InceptionResNetV1, penelitian ini bertujuan menghasilkan sistem autentikasi wajah yang mampu menjadi solusi atas kelemahan autentikasi konvensional berbasis password yang rawan disalahgunakan. Adapun tujuan penelitian ini adalah sebagai berikut:

1) Mengimplementasikan deteksi wajah untuk autentikasi *login* mahasiswa menggunakan YOLOv8.
2) Mengimplementasikan pengenalan wajah untuk autentikasi *login* mahasiswa menggunakan InceptionResNetV1.
3) Membandingkan performa pengenalan wajah antara model yang dilatih dengan *pretrained dataset* VGGFace2 dan Casia-WebFace, serta mengevaluasi perbedaannya dalam konteks autentikasi *login* mahasiswa.

1.5. Manfaat Penelitian

Penelitian ini diharapkan mampu memberikan kontribusi baik secara praktis maupun akademis. Berikut adalah manfaat yang diharapkan dari penelitian ini:

1) Proses *Login* yang Cepat

Dengan teknologi deteksi wajah cepat dari YOLOv8 dan ekstraksi fitur yang akurat dari InceptionResNetV1, sistem memungkinkan *login* dilakukan dalam hitungan detik, tanpa perlu mengetikkan *username* atau *password.* Ini meningkatkan efisiensi waktu dan pengalaman pengguna.

2) Validasi *Login* yang Lebih Akurat

Kombinasi metode *deep learning* ini mampu memberikan validasi yang akurat, terbukti dari hasil evaluasi sistem dengan tingkat akurasi mencapai 98.75% dan *recall* 100%. Ini menjamin bahwa hanya pengguna yang terdaftar yang dapat mengakses sistem.

3) Penerapan yang Luas dan Fleksibel

Sistem yang dikembangkan dapat diimplementasikan di berbagai *platform* berbasis *web*, baik untuk *login* mahasiswa ke portal akademik, sistem presensi, akses ke lab komputer, sistem peminjaman fasilitas kampus, maupun kontrol akses ke ruang tertentu (misalnya ruang dosen, perpustakaan, dan ruang ujian).

4) Dasar Penelitian dan Inovasi Selanjutnya

Penelitian ini membuka peluang untuk pengembangan sistem autentikasi berbasis wajah yang lebih kompleks di masa depan. Hasil penelitian ini dapat digunakan sebagai dasar untuk mengembangkan sistem multi-user login, pengawasan ujian berbasis wajah, dan verifikasi identitas dalam pemungutan suara digital. Selain itu, sistem ini juga dapat diadaptasi untuk aplikasi mobile dan dikembangkan untuk mengenali perubahan wajah pengguna, seperti penuaan atau penggunaan aksesori. Inovasi-inovasi ini akan mendukung penerapan autentikasi wajah yang lebih fleksibel dan efisien di lingkungan kampus dan di luar itu.

5) Keamanan Autentikasi yang Lebih Baik

Metode yang digunakan dalam penelitian ini menawarkan keamanan yang lebih tinggi dibandingkan autentikasi berbasis kata sandi. YOLOv8 berperan sebagai pendeteksi wajah yang cepat dan ringan, sementara InceptionResNetV1 menghasilkan representasi fitur wajah secara presisi. Kombinasi ini memungkinkan sistem hanya mengenali wajah yang sah, mengurangi risiko penyalahgunaan akses akibat pencurian atau kebocoran informasi *login*.

\

Halaman ini sengaja dikosongkan