Jurnal Elektronik Ilmu Komputer Udayana
Volume 15, No 1. August 2026

p-ISSN: 2301-5373
e-ISSN: 2654-5101

Implementasi Teknologi *Face Recognition* Menggunakan Metode CNN Dan *Multi-Factor Authentication* Untuk Meningkatkan Keamanan Login Pada *E-Learning*

I Putu Herdy Juniawan[a1], Ida Ayu Gde Suwiprabayanti Putra[a2], Luh Arida Ayu Rahning Putri[a3], I Gusti Ngurah Anom Cahyadi Putra[a4]

[a]Program Studi Informatika, Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Udayana, Jimbaran, Kuta Selatan, Badung, Bali, Indonesia
[1]herdy478@email.com
[2]iagsuwiprabayantiputra@unud.ac.id
[3]rahningputri@unud.ac.id
[4]anom.cp@unud.ac.id

Abstrak

Platform *E-Learning* menjadi salah satu media utama dalam mendukung proses pembelajaran digital. Namun, mekanisme autentikasi yang hanya mengandalkan *username* dan *password* masih rentan terhadap berbagai ancaman keamanan, seperti *Brute Force Attack*. Penelitian ini bertujuan merancang, mengimplementasikan, dan mengevaluasi sistem *Multi-Factor Authentication* (MFA) berbasis *face recognition* menggunakan *Convolutional Neural Network* (CNN) dengan arsitektur VGG16 untuk meningkatkan keamanan autentikasi pada platform *E-Learning*. Tahapan penelitian meliputi pengumpulan dan pengolahan data wajah, pelatihan model, implementasi MFA, evaluasi model menggunakan *confusion matrix* dan *classification report*, serta pengujian keamanan melalui simulasi *Spoofing Attack* dan *Brute Force Attack*. Hasil evaluasi menunjukkan bahwa model memperoleh *accuracy* sebesar 97,95%, dengan nilai rata-rata *precision*, *recall*, dan *F1-score* sebesar 0,98. Sistem berhasil menolak 90% percobaan *Spoofing Attack*. Pada pengujian *Brute Force Attack*, sistem tanpa MFA berhasil menemukan kredensial valid dalam 10 menit 11 detik 852 milidetik, sedangkan setelah penerapan MFA seluruh 1.000 kombinasi *password* diuji dalam 1 jam 8 menit 20 detik 621 milidetik tanpa berhasil memperoleh akses ke sistem. Hasil tersebut menunjukkan bahwa penerapan MFA berbasis *face recognition* mampu meningkatkan keamanan autentikasi pada platform *E-Learning*.

1. Pendahuluan

Seiring dengan perkembangan teknologi informasi dan komunikasi, pendidikan berbasis digital atau *E-Learning* telah menjadi infrastruktur krusial yang menawarkan fleksibilitas akses terhadap sumber belajar. Namun, di balik keunggulan tersebut, terdapat tantangan signifikan berupa peningkatan risiko keamanan siber. Salah satu tantangan utama dalam ekosistem digital adalah memastikan bahwa hanya pengguna yang sah yang dapat mengakses data sensitif dan sumber daya akademik di dalam platform tersebut [1].

Secara konvensional, sistem *E-Learning* mengandalkan mekanisme autentikasi faktor tunggal (*single-factor authentication*) berupa kombinasi nama pengguna (*username*) dan kata sandi (*password*). Meskipun umum digunakan, mekanisme tersebut rentan terhadap berbagai bentuk serangan siber seperti *Brute Force attack*, yaitu serangan yang dilakukan dengan menguji berbagai kemungkinan kombinasi karakter hingga akses berhasil diperoleh [2]. Selain itu, penggunaan kata sandi yang lemah atau penggunaan kembali kata sandi pada berbagai platform dapat meningkatkan risiko *Credential Stuffing*, yaitu penggunaan kredensial yang telah bocor untuk mencoba mengakses sistem lain secara otomatis. Kondisi tersebut dapat berujung pada *Account Takeover* (ATO), yang memungkinkan pihak tidak berwenang mengambil alih akun dan menyalahgunakan identitas pengguna. Oleh karena itu, diperlukan mekanisme autentikasi yang lebih tangguh untuk meningkatkan keamanan akses pada platform *E-Learning* [3].

Salah satu upaya yang dapat diterapkan untuk meningkatkan keamanan autentikasi adalah *Multi-Factor Authentication* (MFA). MFA menambahkan faktor verifikasi tambahan sehingga keberhasilan memperoleh *username* dan *password* tidak secara langsung memberikan akses kepada pihak yang tidak berwenang. Dalam penelitian ini, biometrik wajah (*face recognition*) digunakan sebagai faktor

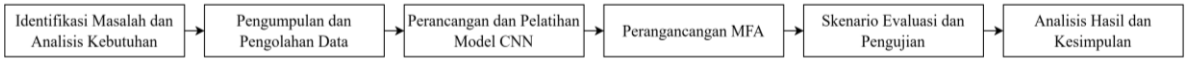
autentikasi kedua karena memanfaatkan karakteristik wajah yang unik pada setiap individu. *Face recognition* merupakan metode biometrik yang menggunakan fitur-fitur unik pada wajah seseorang untuk melakukan verifikasi identitas dan menawarkan mekanisme autentikasi yang lebih kuat dibandingkan penggunaan *username* dan *password* saja [4].

Implementasi *face recognition* dalam penelitian ini menggunakan *Convolutional Neural Network* (CNN) dengan arsitektur VGG16. CNN memiliki kemampuan dalam mengenali pola dan mengekstraksi fitur visual pada citra wajah sehingga dapat digunakan dalam proses pengenalan identitas. Penelitian sebelumnya menunjukkan bahwa CNN mampu memberikan tingkat akurasi yang lebih tinggi dalam pengenalan wajah dibandingkan metode *Principal Component Analysis* (PCA), *Local Binary Patterns Histograms* (LBPH), dan *K-Nearest Neighbour* (KNN) [5].

Berdasarkan permasalahan tersebut, penelitian ini bertujuan untuk merancang, mengimplementasikan, dan mengevaluasi sistem *Multi-Factor Authentication* (MFA) berbasis *face recognition* menggunakan CNN dengan arsitektur VGG16 pada platform *E-Learning*. Model yang dikembangkan digunakan untuk mengekstraksi fitur wajah dan melakukan verifikasi identitas pengguna sebagai faktor autentikasi kedua. Evaluasi dilakukan terhadap performa model dan keamanan sistem melalui simulasi *Spoofing attack* menggunakan media foto serta *Brute Force attack* dengan membandingkan kondisi sistem sebelum dan setelah penerapan MFA. Penelitian ini diharapkan dapat memberikan gambaran mengenai efektivitas penerapan autentikasi biometrik dalam meningkatkan keamanan proses *login* pada platform *E-Learning*.

2. Metode Penelitian

2.1. Tahapan Penelitian



Gambar 1 Alur Tahapan Penelitian

Penelitian ini dilakukan melalui enam tahapan yang disusun secara sistematis, yaitu identifikasi masalah dan analisis kebutuhan, pengumpulan dan pengolahan data, perancangan dan pelatihan model *Convolutional Neural Network* (CNN), perancangan *Multi-Factor Authentication* (MFA), penyusunan skenario evaluasi dan pengujian, serta analisis hasil dan penarikan kesimpulan. Tahapan tersebut dirancang sebagai rangkaian proses untuk mengembangkan dan mengevaluasi sistem autentikasi yang menggunakan verifikasi wajah sebagai faktor autentikasi kedua setelah *username* dan *password*.

Tahap awal dilakukan dengan mengidentifikasi permasalahan keamanan pada mekanisme autentikasi serta menganalisis kebutuhan sistem yang akan dikembangkan. Selanjutnya, data citra wajah dikumpulkan dan diolah sebagai dataset untuk proses pelatihan model. Model CNN dengan arsitektur VGG16 kemudian dirancang dan dilatih untuk mengenali identitas wajah, sebelum ditransformasikan menjadi *feature extractor* yang digunakan dalam sistem MFA. Tahap berikutnya dilakukan dengan merancang mekanisme MFA yang mengintegrasikan autentikasi *username* dan *password* dengan verifikasi wajah pada platform *E-Learning*. Selanjutnya, skenario evaluasi dan pengujian disusun untuk mengevaluasi performa model serta keamanan sistem melalui simulasi *Spoofing attack* dan *Brute Force attack*. Hasil evaluasi dan pengujian kemudian dianalisis untuk memperoleh kesimpulan mengenai penerapan MFA berbasis *face recognition* dalam meningkatkan keamanan autentikasi pada platform *E-Learning*. Alur keseluruhan tahapan penelitian ditunjukkan pada Gambar 1.

2.2. Identifikasi Masalah dan Analisis Kebutuhan

Tahap identifikasi masalah dilakukan untuk menentukan permasalahan keamanan yang menjadi dasar pengembangan sistem. Mekanisme autentikasi pada platform *E-Learning* umumnya masih mengandalkan autentikasi faktor tunggal berupa *username* dan *password*. Mekanisme tersebut rentan terhadap serangan *Brute Force*, yaitu serangan yang dilakukan dengan menguji berbagai kemungkinan kombinasi kredensial secara berulang hingga memperoleh akses ke dalam sistem [2]. Selain itu, penggunaan kata sandi yang lemah dan kebocoran kredensial dapat meningkatkan risiko penyalahgunaan akun oleh pihak yang tidak berwenang [3]. Berdasarkan permasalahan tersebut, diperlukan mekanisme autentikasi berlapis untuk meningkatkan keamanan dan memastikan bahwa akses hanya diberikan kepada pengguna yang sah.

Analisis kebutuhan dilakukan untuk menentukan fungsi, mekanisme, dan komponen yang diperlukan dalam pengembangan sistem. Kebutuhan utama sistem adalah penerapan *Multi-Factor Authentication* (MFA) dengan mengintegrasikan *face recognition* sebagai faktor autentikasi kedua setelah verifikasi

p-ISSN: 2301-5373
e-ISSN: 2654-5101

username dan *password*. Mekanisme ini dirancang agar keberhasilan verifikasi kredensial pada faktor pertama tidak secara langsung memberikan akses ke dalam sistem, melainkan pengguna harus melewati proses verifikasi identitas melalui wajah.

Secara fungsional, sistem dirancang untuk mendukung proses registrasi wajah, akuisisi citra melalui kamera, ekstraksi fitur wajah menggunakan model CNN dengan arsitektur VGG16, penyimpanan representasi fitur wajah sebagai data biometrik referensi, serta verifikasi identitas pengguna. Pada proses verifikasi, fitur wajah yang diperoleh dari citra pengguna dibandingkan dengan data referensi yang tersimpan menggunakan *Cosine Similarity*, yaitu metode untuk mengukur tingkat kemiripan antara dua vektor fitur berdasarkan sudut di antara keduanya. Semakin tinggi nilai *Cosine Similarity*, semakin besar tingkat kemiripan antara fitur wajah pengguna dan data wajah referensi yang tersimpan [6]. Akses ke platform *E-Learning* hanya diberikan apabila pengguna berhasil melewati autentikasi *username* dan *password* serta verifikasi wajah. Dari aspek keamanan, sistem dirancang untuk meningkatkan ketahanan proses autentikasi terhadap *Spoofing attack* menggunakan media foto dan *Brute Force attack*. Pengujian terhadap kedua jenis serangan tersebut digunakan untuk mengevaluasi keamanan sistem setelah penerapan MFA berbasis *face recognition*. Implementasi sistem dilakukan pada Moodle sebagai platform *E-Learning*, sedangkan Flask digunakan sebagai *backend* untuk menangani proses registrasi dan verifikasi wajah serta mengintegrasikan proses *face recognition* dengan mekanisme autentikasi pada Moodle. Sistem juga didukung oleh *TensorFlow* dan *Keras* untuk pemrosesan model, *OpenCV* untuk akuisisi dan pengolahan citra, serta *MySQL* untuk penyimpanan data pengguna dan data biometrik.

2.3. Pengumpulan dan Pengolahan Data

Gambar 2 Contoh Hasil Data Wajah

Data yang digunakan dalam penelitian ini berupa citra wajah yang diperoleh dari 13 subjek mahasiswa. Pengumpulan data dilakukan menggunakan kamera (*webcam*) dengan mempertimbangkan variasi ekspresi wajah, sudut pengambilan, dan kondisi pencahayaan. Setiap subjek memiliki 50 citra wajah asli sehingga diperoleh sebanyak 650 citra.

Citra wajah yang telah dikumpulkan kemudian melalui tahap preprocessing berupa pemotongan area wajah (*cropping*) dan perubahan ukuran citra (*resize*) menjadi 224 × 224 piksel sesuai dengan ukuran masukan arsitektur VGG16. Selanjutnya, dilakukan augmentasi data untuk meningkatkan jumlah dan variasi citra pada setiap subjek. Proses augmentasi menghasilkan 100 citra tambahan sehingga setiap subjek memiliki total 150 citra. Dengan demikian, dataset akhir berjumlah 1.950 citra wajah dari 13 subjek. Dataset selanjutnya dibagi menjadi 80% data pelatihan (*training set*) dan 20% data pengujian (*testing set*). Data pelatihan digunakan dalam proses pelatihan model CNN dengan arsitektur VGG16, sedangkan data pengujian digunakan untuk mengevaluasi kemampuan model dalam mengklasifikasikan identitas wajah.

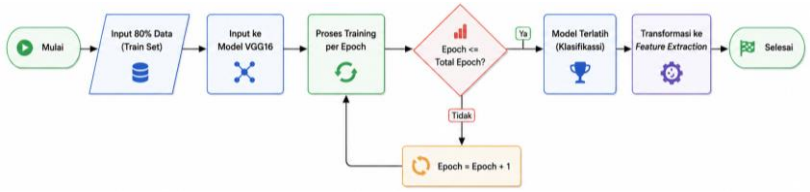
Tabel 1. Distribusi Dataset

Keterangan	Jumlah
Jumlah subjek	13
Citra asli per subjek	50
Citra setelah augmentasi per subjek	150
Total dataset	1.950
Data pelatihan	80%
Data pengujian	20%

2.4. Perancangan dan Pelatihan Model CNN

Model pengenalan wajah dirancang menggunakan *Convolutional Neural Network* (CNN) dengan arsitektur VGG16. CNN merupakan metode *deep learning* yang mampu mengekstraksi fitur visual secara hierarkis melalui lapisan konvolusi, fungsi aktivasi, dan *pooling*, mulai dari fitur sederhana seperti tepi dan tekstur hingga pola visual yang lebih kompleks [7]. Arsitektur VGG16 menggunakan susunan lapisan konvolusi dengan *filter* berukuran 3 × 3 yang memungkinkan proses ekstraksi fitur dilakukan secara bertahap dan mendalam [8].

Dalam penelitian ini, VGG16 diterapkan menggunakan pendekatan *transfer learning* dengan memanfaatkan bobot hasil *pre-training* pada dataset ImageNet. Model digunakan tanpa lapisan klasifikasi bawaan (include_top=False) dengan ukuran masukan citra 224 × 224 × 3. Seluruh lapisan dasar VGG16 dibekukan (*freezing*) agar bobot hasil *pre-training* tetap dipertahankan selama proses pelatihan. Keluaran VGG16 selanjutnya diubah menjadi vektor menggunakan lapisan *Flatten*, kemudian diteruskan ke lapisan *Dense* dengan 128 neuron dan fungsi aktivasi ReLU. Lapisan *Dropout* sebesar 0,5 diterapkan untuk mengurangi risiko *overfitting*, sedangkan lapisan keluaran menggunakan 13 neuron dengan fungsi aktivasi *softmax* sesuai dengan jumlah kelas identitas wajah.

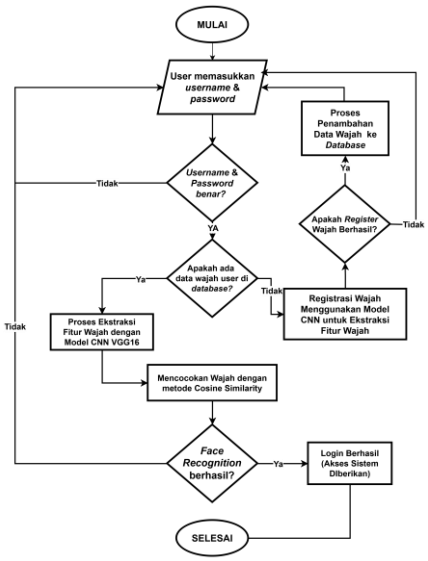


Gambar 3 Flowchart Pelatihan Model

Proses pelatihan dilakukan menggunakan dataset wajah yang telah melalui tahap *preprocessing* dan augmentasi. Model dilatih untuk mempelajari karakteristik visual dari setiap kelas identitas, sedangkan perkembangan proses pembelajaran dipantau berdasarkan nilai *accuracy* dan *loss* pada data *training* dan *validation*. Model klasifikasi yang telah dilatih selanjutnya ditransformasikan menjadi *feature extractor* dengan menggunakan keluaran dari lapisan *Dense* 128 neuron sebagai representasi fitur wajah atau *face embedding*. Representasi numerik tersebut digunakan untuk menggambarkan karakteristik wajah sehingga dapat dimanfaatkan dalam proses pengenalan dan verifikasi identitas [9].

Pada implementasi sistem MFA, proses autentikasi tidak menggunakan hasil klasifikasi kelas secara langsung. *Face embedding* yang dihasilkan dari citra wajah saat autentikasi dibandingkan dengan data biometrik referensi menggunakan *Cosine Similarity*. Nilai kemiripan yang diperoleh selanjutnya digunakan sebagai dasar untuk menentukan kesesuaian identitas pengguna pada tahap verifikasi wajah.

2.5. Perancangan Multi-Factor Authentication



Gambar 4 *Flowchart Multi-Factor Authentication* (MFA)

Multi-Factor Authentication (MFA) merupakan mekanisme autentikasi yang menggabungkan dua atau lebih metode autentikasi untuk mengurangi risiko keamanan yang timbul apabila sistem hanya bergantung pada satu metode autentikasi. Penggunaan lebih dari satu metode autentikasi dapat meningkatkan keamanan karena penyerang harus melewati lebih dari satu tahap verifikasi untuk memperoleh akses ke dalam sistem [10]. Dalam penelitian ini, MFA dirancang dengan mengintegrasikan autentikasi *username* dan *password* sebagai faktor pertama serta *face recognition* sebagai faktor kedua pada platform E-Learning.

Alur autentikasi dimulai ketika pengguna memasukkan *username* dan *password*. Apabila kredensial yang dimasukkan tidak valid, pengguna dikembalikan ke proses *login*. Sebaliknya, apabila kredensial

p-ISSN: 2301-5373
e-ISSN: 2654-5101

valid, sistem memeriksa ketersediaan data wajah pengguna pada *database*. Apabila data wajah belum tersedia, pengguna diarahkan ke proses registrasi wajah. Pada tahap ini, citra wajah pengguna diproses menggunakan model CNN dengan arsitektur VGG16 yang telah ditransformasikan menjadi *feature extractor* untuk menghasilkan *face embedding*. Jika proses registrasi berhasil, *face embedding* disimpan ke dalam *database* sebagai data biometrik referensi pengguna.

Apabila data wajah telah tersedia pada *database*, sistem melanjutkan proses autentikasi ke tahap verifikasi wajah. Citra wajah pengguna diproses menggunakan model CNN dengan arsitektur VGG16 untuk menghasilkan *face embedding*. Representasi fitur tersebut kemudian dibandingkan dengan data biometrik referensi yang tersimpan pada *database* menggunakan metode *Cosine Similarity*. Metode tersebut digunakan untuk mengukur tingkat kemiripan antara *face embedding* hasil ekstraksi citra wajah saat autentikasi dengan *face embedding* referensi yang telah tersimpan. Nilai *Cosine Similarity* berada pada rentang 0 hingga 1, di mana nilai yang semakin mendekati 1 menunjukkan tingkat kemiripan yang semakin tinggi.

Tabel 2 Analisis Penentuan Threshold Verifikasi

Jenis Perbandingan	Nilai Cosine Similarity
Genuine Pair (minimum)	0,932
Genuine Pair (maksimum)	0,963
Impostor Pair (maksimum)	0,901
Threshold Verifikasi	**0,920**

Nilai ambang batas (*threshold*) verifikasi pada penelitian ini ditetapkan sebesar **0,92 (92%)** berdasarkan analisis distribusi nilai *Cosine Similarity* antara pasangan wajah pengguna yang sama (*genuine pair*) dan pasangan wajah pengguna yang berbeda (*impostor pair*). Analisis dilakukan dengan membandingkan *face embedding* hasil ekstraksi citra wajah pada data pengujian terhadap *face embedding* referensi yang tersimpan pada *database*. Hasil analisis menunjukkan bahwa nilai *Cosine Similarity* pada pasangan *genuine* berada pada rentang **0,932 hingga 0,963**, sedangkan nilai *Cosine Similarity* tertinggi pada pasangan *impostor* adalah **0,901**.

Berdasarkan hasil tersebut, dipilih nilai *threshold* sebesar **0,92** karena berada di antara distribusi nilai *genuine* dan *impostor*. Nilai tersebut dipilih agar seluruh pengguna yang sah masih memiliki nilai *similarity* di atas *threshold*, sedangkan pengguna yang berbeda tetap berada di bawah *threshold*. Dengan demikian, nilai *threshold* mampu memberikan batas keputusan (*decision boundary*) yang memisahkan proses autentikasi pengguna yang valid dan pengguna yang tidak sah. Pemilihan nilai *threshold* tersebut bertujuan untuk meminimalkan kemungkinan terjadinya **False Acceptance**, yaitu kondisi ketika pengguna yang tidak sah diterima oleh sistem, tanpa mengurangi keberhasilan autentikasi pengguna yang sah.

Selanjutnya, hasil perbandingan *Cosine Similarity* digunakan sebagai dasar pengambilan keputusan pada proses verifikasi wajah. Apabila nilai *similarity* yang diperoleh sama dengan atau lebih besar dari **0,92**, maka verifikasi wajah dinyatakan berhasil dan pengguna diberikan akses ke dalam sistem. Sebaliknya, apabila nilai *similarity* berada di bawah nilai *threshold*, proses autentikasi dinyatakan gagal sehingga pengguna tidak memperoleh akses ke dalam sistem. Alur perancangan MFA berbasis *face recognition* ditunjukkan pada Gambar 4.

2.6. Skenario Evaluasi dan Pengujian Sistem

Evaluasi dan pengujian dilakukan untuk mengukur performa model CNN dengan arsitektur VGG16 serta mengevaluasi keamanan sistem *Multi-Factor Authentication* (MFA) berbasis *face recognition*. Tahapan ini terdiri atas evaluasi model dan pengujian keamanan sistem melalui skenario *Spoofing attack* dan *Brute Force attack*.

a. Evaluasi Model

Evaluasi model dilakukan untuk mengukur kemampuan model CNN dengan arsitektur VGG16 dalam mengklasifikasikan citra wajah sebelum digunakan sebagai *feature extractor* pada sistem Multi-Factor Authentication (MFA). Evaluasi dilakukan menggunakan **Confusion Matrix** dengan membandingkan hasil prediksi model terhadap label sebenarnya (*ground truth*). Berdasarkan Confusion Matrix, performa model dianalisis menggunakan metrik **Accuracy, Precision, Recall,** dan **F1-Score** yang disajikan

dalam bentuk *classification report*. Accuracy digunakan untuk mengukur proporsi keseluruhan prediksi yang benar terhadap seluruh data uji. Precision digunakan untuk mengukur ketepatan model dalam mengklasifikasikan setiap kelas, Recall digunakan untuk mengukur kemampuan model dalam mengenali seluruh data yang benar pada setiap kelas, sedangkan F1-Score merupakan rata-rata harmonis antara Precision dan Recall sehingga memberikan gambaran keseimbangan performa model. Penggunaan keempat metrik tersebut memungkinkan evaluasi performa model dilakukan secara lebih komprehensif pada setiap kelas identitas sebelum model digunakan sebagai *feature extractor* dalam proses verifikasi wajah pada sistem MFA [8].

b. Pengujian *Spoofing Attack*

Pengujian *Spoofing attack* dilakukan untuk mengevaluasi ketahanan sistem terhadap upaya autentikasi menggunakan media *non-live* berupa foto wajah pengguna yang telah terdaftar. Foto ditampilkan di depan kamera selama proses verifikasi wajah untuk mensimulasikan serangan *spoofing*. Pada setiap percobaan, proses verifikasi dilakukan hingga batas waktu (*timeout*) yang telah ditentukan. Nilai *Cosine Similarity* tertinggi (*highest similarity score*) yang diperoleh selama satu sesi verifikasi digunakan sebagai acuan evaluasi dan dibandingkan dengan nilai ambang batas (*threshold*). Serangan dinyatakan berhasil apabila nilai kemiripan melebihi *threshold* sehingga foto diterima sebagai wajah yang valid. Sebaliknya, serangan dinyatakan gagal apabila nilai kemiripan tetap berada di bawah *threshold* hingga proses verifikasi berakhir .

c. Pengujian *Brute Force Attack*

Pengujian *Brute Force attack* dilakukan untuk mengevaluasi efektivitas penerapan MFA dalam meningkatkan keamanan terhadap serangan penebakan kata sandi (*password guessing attack*). *Brute Force Attack* merupakan metode serangan yang dilakukan dengan mencoba berbagai kombinasi kredensial secara berulang hingga memperoleh kombinasi yang benar [11] Pengujian membandingkan dua kondisi, yaitu sistem *E-Learning* yang hanya menggunakan autentikasi *username* dan *password* serta sistem yang telah menerapkan MFA berbasis verifikasi wajah. Simulasi serangan dilakukan menggunakan Burp Suite melalui fitur *Intruder* dengan metode *Pitchfork Attack*. Parameter yang diuji meliputi *username*, *password*, dan *login token*, sedangkan fitur *Grep Extract* digunakan untuk memperbarui *login token* yang bersifat dinamis pada setiap permintaan autentikasi.

Pengujian menggunakan *wordlist* yang terdiri atas 1.000 kombinasi *password* terhadap akun dengan *username* **admin** yang diasumsikan telah diketahui oleh penyerang. Keberhasilan serangan pada kedua kondisi dievaluasi berdasarkan nilai *redirect*, *response length*, dan isi respons (*response content*) dari server. Selain itu, waktu serangan diukur sejak proses *Brute Force attack* dimulai hingga ditemukan indikator keberhasilan autentikasi atau seluruh *wordlist* selesai diuji. Fitur *Auto-Pause Attack* dikonfigurasi untuk menghentikan serangan secara otomatis apabila respons mengandung kata **Dashboard** sebagai indikator keberhasilan autentikasi. Apabila seluruh *wordlist* selesai diuji tanpa menemukan indikator tersebut, serangan dinyatakan tidak berhasil.

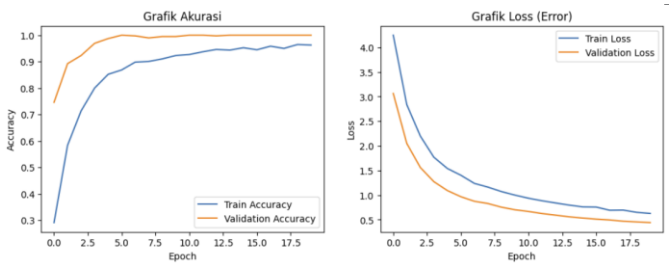
3. Hasil dan Pembahasan

3.1. Hasil Pelatihan dan Evaluasi Model

Proses pelatihan model CNN dengan arsitektur VGG16 dilakukan menggunakan dataset wajah yang telah melalui tahap *preprocessing* dan augmentasi. Model dilatih untuk mempelajari karakteristik visual dari 13 kelas identitas wajah. Perkembangan performa model selama proses pelatihan diamati melalui *learning curves* yang menunjukkan perubahan nilai *accuracy* dan *loss* pada data pelatihan dan validasi.

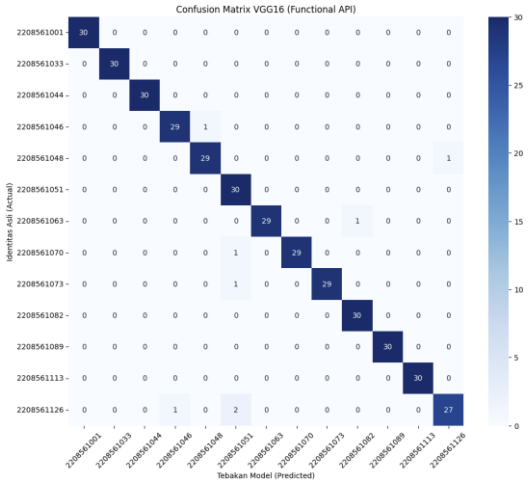
Berdasarkan *learning curves* pada Gambar 5, nilai *accuracy* pada data pelatihan mengalami peningkatan dari sekitar 0,29 pada *epoch* awal hingga mencapai lebih dari 0,95 pada *epoch* akhir. Sementara itu, *accuracy* pada data validasi menunjukkan nilai yang tinggi dan stabil mendekati 1,00. Pada grafik *loss*, nilai *loss* pada data pelatihan dan validasi mengalami penurunan selama proses pelatihan. Pola tersebut menunjukkan bahwa model mampu mempelajari karakteristik data dengan baik dan tidak menunjukkan indikasi *overfitting* yang signifikan karena kurva pelatihan dan validasi menunjukkan pola perkembangan yang sejalan.

p-ISSN: 2301-5373
e-ISSN: 2654-5101



Gambar 5 Hasil Pelatihan Model (*Learning Curves*)

Setelah proses pelatihan selesai, model dievaluasi menggunakan data *testing* untuk mengetahui kemampuannya dalam mengklasifikasikan identitas wajah sebelum ditransformasikan menjadi *feature extractor*. Evaluasi dilakukan terhadap 390 citra wajah yang terdiri atas 13 kelas, dengan masing-masing kelas memiliki 30 data uji. Hasil klasifikasi dianalisis menggunakan **Confusion Matrix** serta metrik **Accuracy, Precision, Recall,** dan **F1-Score** yang disajikan dalam bentuk *classification report*..



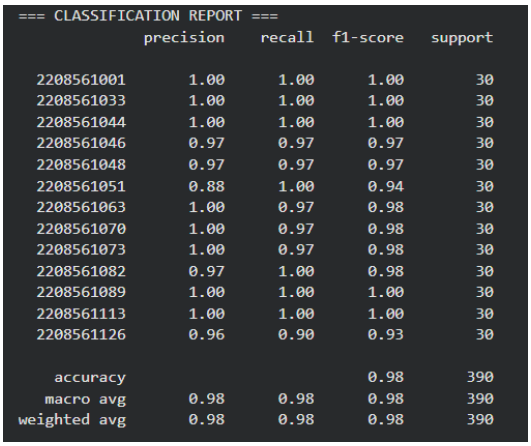
Gambar 6 Hasil Evaluasi Model (*Confusion Matrix*)

Hasil evaluasi pada *Confusion Matrix* menunjukkan bahwa sebagian besar citra berhasil diklasifikasikan ke dalam kelas yang sesuai, yang ditunjukkan oleh dominasi nilai pada diagonal utama matriks. Beberapa kelas berhasil mengklasifikasikan seluruh 30 data uji dengan benar, sedangkan sebagian besar kelas lainnya hanya mengalami satu kesalahan klasifikasi. Secara keseluruhan, model berhasil mengklasifikasikan 382 dari 390 citra wajah dengan benar dan menghasilkan 8 kesalahan klasifikasi.

Nilai *Accuracy* dihitung sebagai berikut:

$$Accuracy = \frac{382}{390} \times 100\% = 97{,}95\% \quad (1)$$

Selain menggunakan *Accuracy*, performa model juga dianalisis menggunakan *classification report* yang mencakup nilai **Precision, Recall,** dan **F1-Score** untuk setiap kelas identitas. Hasil *classification report* ditunjukkan pada Gambar 7



=== CLASSIFICATION REPORT ===

	precision	recall	f1-score	support
2208561001	1.00	1.00	1.00	30
2208561033	1.00	1.00	1.00	30
2208561044	1.00	1.00	1.00	30
2208561046	0.97	0.97	0.97	30
2208561048	0.97	0.97	0.97	30
2208561051	0.88	1.00	0.94	30
2208561063	1.00	0.97	0.98	30
2208561070	1.00	0.97	0.98	30
2208561073	1.00	0.97	0.98	30
2208561082	0.97	1.00	0.98	30
2208561089	1.00	1.00	1.00	30
2208561113	1.00	1.00	1.00	30
2208561126	0.96	0.90	0.93	30
accuracy			0.98	390
macro avg	0.98	0.98	0.98	390
weighted avg	0.98	0.98	0.98	390

Gambar 7 Hasil Evaluasi Model (*Classification Report*)

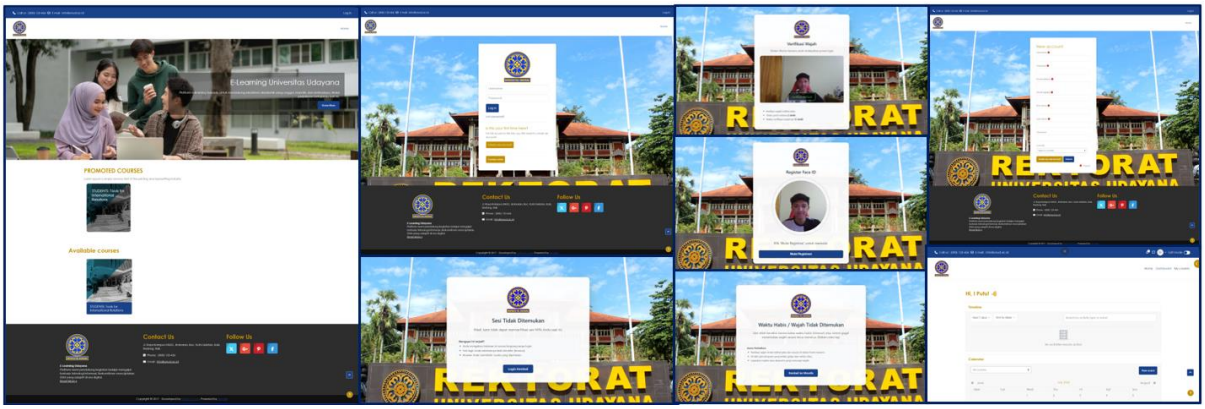
Berdasarkan hasil pengujian pada Tabel 3, sebanyak **9 dari 10** percobaan menghasilkan nilai *Cosine Similarity* di bawah *threshold* sebesar **92%**, sehingga sistem berhasil menolak autentikasi menggunakan media foto. Hanya **1 percobaan** yang menghasilkan nilai *similarity* sebesar **92,8%**, sehingga melebihi *threshold* dan menyebabkan proses autentikasi berhasil. Secara keseluruhan, sistem berhasil menolak **90%** percobaan *Spoofing Attack*.

Hasil tersebut menunjukkan bahwa nilai *threshold* sebesar **92%** yang digunakan pada sistem mampu membedakan sebagian besar media foto dengan wajah asli. Hal ini sejalan dengan hasil analisis pada tahap perancangan, di mana nilai *Cosine Similarity* tertinggi antar pengguna yang berbeda (*impostor pair*) hanya mencapai **0,901**, sedangkan nilai *similarity* pengguna yang sah (*genuine pair*) berada pada rentang **0,932–0,963**. Dengan demikian, *threshold* sebesar **0,92** mampu memisahkan mayoritas pasangan *genuine* dan *impostor* pada data evaluasi.

Meskipun demikian, masih terdapat satu percobaan yang berhasil melewati proses verifikasi dengan nilai *similarity* sebesar **92,8%**. Hal ini menunjukkan bahwa media foto dengan kualitas tertentu masih dapat menghasilkan representasi fitur (*face embedding*) yang sangat menyerupai wajah asli sehingga nilai *Cosine Similarity* yang dihasilkan melebihi *threshold* verifikasi. Kondisi tersebut mengindikasikan bahwa sistem masih memiliki potensi mengalami **False Acceptance** terhadap *presentation attack* yang menggunakan media foto berkualitas tinggi.

Secara keseluruhan, hasil pengujian menunjukkan bahwa penerapan *face recognition* sebagai faktor kedua pada mekanisme MFA mampu meningkatkan keamanan autentikasi dengan menolak sebagian besar upaya *Spoofing Attack*. Namun, pengujian ini juga menunjukkan bahwa penggunaan *face recognition* tanpa mekanisme pendeteksian keaslian wajah (*liveness detection*) belum sepenuhnya mampu mencegah serangan berbasis media foto. Oleh karena itu, penelitian selanjutnya dapat mengintegrasikan metode *liveness detection*, seperti deteksi kedipan mata, analisis gerakan kepala, atau pendekatan *deep learning*-based *presentation attack detection*, untuk meningkatkan ketahanan sistem terhadap serangan *spoofing*.

3.2. Hasil Implementasi MFA Berbasis *Face Recognition*



Gambar 8 Hasil Implementasi Antarmuka

Hasil implementasi menunjukkan bahwa mekanisme *Multi-Factor Authentication* (MFA) berbasis *face recognition* telah berhasil diintegrasikan pada platform *E-Learning*. Sistem menerapkan dua faktor autentikasi, yaitu verifikasi *username* dan *password* sebagai faktor pertama serta verifikasi wajah sebagai faktor kedua. Moodle digunakan sebagai platform utama *E-Learning*, sedangkan Flask berperan sebagai *backend* yang menangani proses registrasi dan verifikasi wajah.

Proses autentikasi dimulai ketika pengguna melakukan *login* dengan memasukkan *username* dan *password*. Setelah kredensial berhasil diverifikasi, sistem memeriksa ketersediaan data wajah pengguna di dalam *database*. Apabila data wajah belum tersedia, pengguna diarahkan ke halaman registrasi wajah. Citra wajah yang diperoleh kemudian diproses menggunakan model CNN dengan arsitektur VGG16 yang telah ditransformasikan menjadi *feature extractor*. Hasil ekstraksi fitur selanjutnya disimpan ke dalam *database* sebagai data biometrik referensi untuk proses verifikasi wajah.

Apabila data wajah telah tersedia, pengguna diarahkan ke tahap verifikasi wajah sebagai faktor autentikasi kedua. Citra wajah yang diperoleh melalui kamera diproses menggunakan *feature extractor* untuk menghasilkan representasi fitur wajah, kemudian dibandingkan dengan data biometrik referensi menggunakan metode *Cosine Similarity*. Apabila nilai kemiripan memenuhi *threshold* yang telah ditetapkan, verifikasi dinyatakan berhasil dan pengguna diberikan akses ke halaman *Dashboard*.

p-ISSN: 2301-5373
e-ISSN: 2654-5101

Sebaliknya, apabila verifikasi wajah gagal, akses ke dalam sistem tidak diberikan. Sistem juga menerapkan pengelolaan sesi untuk menangani kondisi sesi yang tidak valid maupun proses autentikasi yang melebihi batas waktu (*timeout*).

Keseluruhan hasil implementasi antarmuka, yang meliputi halaman *Home*, *Login*, *Register*, registrasi wajah, verifikasi MFA, *Session Error*, *Timeout*, dan *Dashboard*, ditunjukkan pada Gambar 8. Hasil implementasi tersebut menunjukkan bahwa autentikasi berbasis *username* dan *password* telah berhasil diintegrasikan dengan verifikasi wajah dalam satu alur MFA, sehingga akses ke dalam platform *E-Learning* hanya diberikan setelah pengguna berhasil melewati tahapan autentikasi yang ditetapkan.

3.3. Hasil Pengujian Sistem

Pengujian sistem dilakukan untuk mengevaluasi keamanan sistem *Multi-Factor Authentication* (MFA) berbasis *face recognition* terhadap upaya serangan pada proses autentikasi. Pengujian dilakukan melalui dua skenario, yaitu *Spoofing attack* menggunakan media foto wajah dan *Brute Force attack* dengan membandingkan sistem sebelum dan setelah penerapan MFA.

a. Hasil Pengujian *Spoofing Attack*

Pengujian *Spoofing attack* dilakukan terhadap 10 pengguna menggunakan media foto wajah yang ditampilkan di depan kamera pada saat proses verifikasi. Setiap proses verifikasi dijalankan hingga batas waktu (*timeout*), dan nilai *Cosine Similarity* tertinggi yang diperoleh selama satu sesi digunakan sebagai acuan evaluasi. Nilai tersebut dibandingkan dengan *threshold* sebesar 92% untuk menentukan keberhasilan autentikasi.

Tabel 3. Hasil Pengujian Spoofing Attack

ID	Username	Media Pengujian	Nilai Similarity	Hasil
01	2208561001	Foto wajah	73,2%	Ditolak
02	2208561126	Foto wajah	92.8%	Berhasil Login
03	2208561070	Foto wajah	84,3%	Ditolak
04	2208561033	Foto wajah	78,6%	Ditolak
05	2208561051	Foto wajah	86,1%	Ditolak
06	2208561063	Foto wajah	71,3%	Ditolak
07	2208561073	Foto wajah	72,6%	Ditolak
08	2208561082	Foto wajah	68,4%	Ditolak
09	2208561089	Foto wajah	70,7%	Ditolak
10	2208561113	Foto wajah	65,1%	Ditolak

Hasil pengujian menunjukkan bahwa 9 dari 10 percobaan menghasilkan nilai *similarity* tertinggi di bawah *threshold*, sehingga sistem berhasil menolak autentikasi menggunakan media foto. Namun, satu percobaan menghasilkan nilai *similarity* sebesar 92,8%, sehingga melebihi *threshold* dan menyebabkan proses autentikasi berhasil. Secara keseluruhan, sistem berhasil menolak 90% percobaan *Spoofing attack*. Hasil ini menunjukkan bahwa sistem mampu menolak sebagian besar upaya autentikasi menggunakan foto, meskipun masih terdapat kemungkinan media foto diterima sebagai wajah valid apabila menghasilkan nilai kemiripan yang melebihi *threshold*.

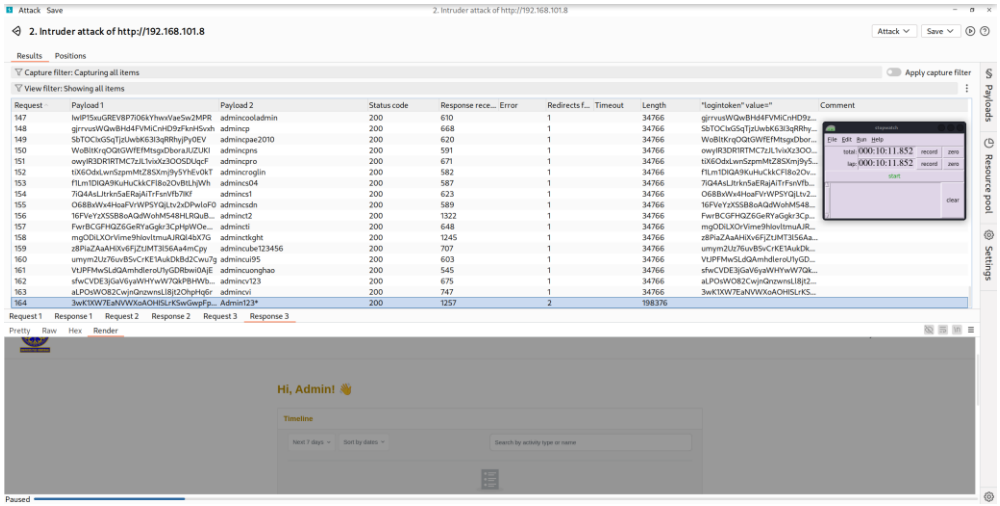
b. Hasil Pengujian *Brute Force Attack*

Pengujian *Brute Force Attack* dilakukan dengan membandingkan sistem *E-Learning* sebelum dan setelah penerapan Multi-Factor Authentication (MFA) menggunakan konfigurasi pengujian yang sama. Serangan dilakukan menggunakan Burp Suite dengan *wordlist* yang terdiri atas **1.000** kombinasi *password*. Keberhasilan serangan dianalisis berdasarkan perubahan karakteristik respons server, meliputi nilai *redirect*, *response length*, dan isi respons (*response content*), serta waktu yang diperlukan untuk memperoleh indikator keberhasilan autentikasi.

Pada sistem yang belum menerapkan MFA, serangan berhasil mengidentifikasi kombinasi *username* dan *password* yang valid pada *wordlist* ke-164. Keberhasilan tersebut ditandai dengan aktifnya fitur **Auto-Pause Attack** pada Burp Suite ketika respons server mengandung kata **Dashboard**, sehingga proses serangan dihentikan secara otomatis tanpa harus menguji seluruh *wordlist*. Waktu yang dibutuhkan sejak serangan dimulai hingga ditemukan kredensial yang valid adalah **10 menit 11 detik 852 milidetik**.

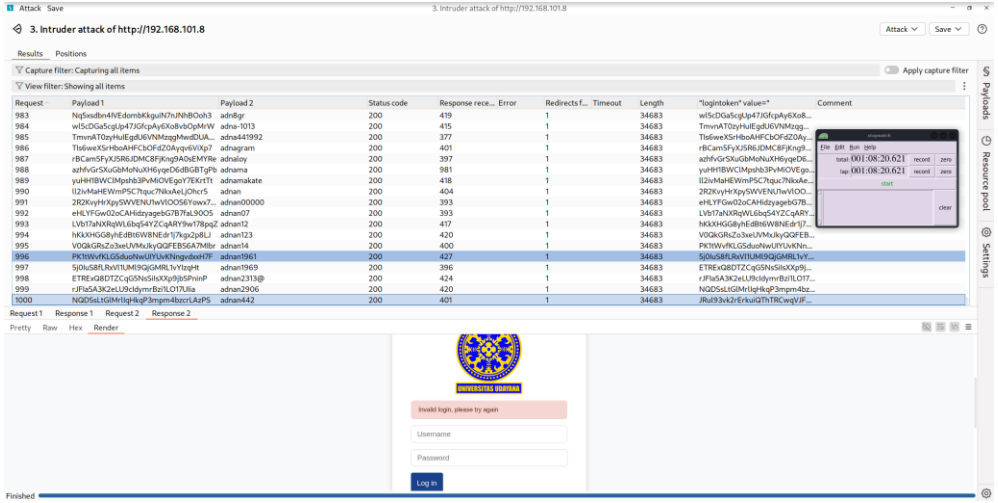
Keberhasilan serangan juga dapat diidentifikasi melalui perubahan karakteristik respons server. Pada sebagian besar percobaan, nilai **redirect** bernilai **1**, sedangkan ketika kombinasi *username* dan *password* yang benar ditemukan, nilai tersebut berubah menjadi **2**, yang menunjukkan bahwa sistem telah melakukan pengalihan menuju halaman setelah proses autentikasi berhasil. Selain itu, **response**

length mengalami peningkatan dari sekitar **34.766 byte** menjadi **197.380 byte**, yang menunjukkan bahwa server mengirimkan halaman yang berbeda dibandingkan respons sebelumnya. Berdasarkan analisis isi respons, ditemukan bahwa server telah mengembalikan halaman **Dashboard**, sehingga kombinasi *username* dan *password* pada *payload* tersebut dapat dinyatakan valid. Hasil *Brute Force Attack* pada sistem yang belum menerapkan MFA ditunjukkan pada Gambar 9.



Gambar 9 Waktu Pengujian Brute Force pada Sistem yang Belum Menerapkan MFA

Sebaliknya, pada sistem yang telah menerapkan MFA berbasis *face recognition*, seluruh **1.000** kombinasi *password* berhasil diuji hingga selesai dalam waktu **1 jam 8 menit 20 detik 621 milidetik** tanpa ditemukan indikator keberhasilan autentikasi.



Gambar 10 Waktu Pengujian Brute Force pada Sistem yang Telah Menerapkan MFA

Berbeda dengan sistem tanpa MFA, fitur **Auto-Pause Attack** tidak pernah aktif selama proses pengujian karena tidak ditemukan satu pun respons yang mengandung kata **Dashboard**. Seluruh respons server memiliki karakteristik yang relatif seragam, di mana nilai **redirect** tetap bernilai **1** dan **response length** berada pada kisaran **34.683 byte**. Tidak ditemukan perubahan karakteristik respons meskipun kombinasi *username* dan *password* yang benar terdapat dalam *wordlist*. Hasil *Brute Force Attack* pada sistem yang telah menerapkan MFA ditunjukkan pada Gambar 9.

Berdasarkan analisis isi respons, server tidak pernah mengembalikan halaman **Dashboard** maupun indikator lain yang menunjukkan bahwa proses autentikasi telah berhasil diselesaikan. Hal ini menunjukkan bahwa setelah kredensial yang benar diterima oleh sistem, pengguna masih diwajibkan melewati tahap verifikasi wajah sebagai faktor autentikasi kedua. Dengan demikian, informasi mengenai keberhasilan autentikasi tahap pertama tidak pernah ditampilkan kepada penyerang sehingga proses *Brute Force Attack* tidak dapat memperoleh akses ke dalam sistem hanya dengan menebak *password*.

Secara keseluruhan, hasil pengujian menunjukkan bahwa penerapan MFA berbasis *face recognition* mampu meningkatkan keamanan proses autentikasi terhadap *Brute Force Attack*. Keberhasilan

autentikasi tidak lagi hanya ditentukan oleh kecocokan *username* dan *password*, tetapi juga bergantung pada keberhasilan verifikasi biometrik wajah. Akibatnya, meskipun penyerang berhasil menemukan kombinasi kredensial yang valid, akses ke dalam sistem tetap tidak dapat diperoleh tanpa melewati faktor autentikasi kedua. Hasil ini menunjukkan bahwa mekanisme MFA secara efektif mengurangi risiko akses tidak sah akibat serangan *Brute Force* yang hanya menargetkan kredensial berbasis kata sandi.

4. Kesimpulan

Penelitian ini berhasil mengimplementasikan Multi-Factor Authentication (MFA) berbasis *face recognition* pada platform *E-Learning* dengan mengintegrasikan autentikasi *username* dan *password* sebagai faktor pertama serta verifikasi wajah sebagai faktor kedua. Model CNN dengan arsitektur VGG16 yang digunakan sebagai *feature extractor* menunjukkan performa yang baik dalam mengenali identitas wajah, dengan memperoleh accuracy sebesar 97,95%, serta nilai rata-rata precision, recall, dan F1-score sebesar 0,98 berdasarkan hasil *classification report*. Selain itu, penentuan nilai *threshold* verifikasi sebesar 0,92 didasarkan pada analisis distribusi nilai *Cosine Similarity* antara pasangan *genuine* dan *impostor*, sehingga mampu memberikan batas keputusan yang efektif dalam membedakan pengguna yang sah dan pengguna yang tidak sah.

Hasil pengujian keamanan menunjukkan bahwa sistem mampu menolak 9 dari 10 percobaan *Spoofing Attack* menggunakan media foto atau sebesar 90%, meskipun masih terdapat satu percobaan yang berhasil melewati verifikasi karena menghasilkan nilai *Cosine Similarity* di atas *threshold*. Sementara itu, pada pengujian *Brute Force Attack*, sistem tanpa MFA berhasil menemukan kombinasi kredensial yang valid dalam waktu 10 menit 11 detik 852 milidetik, sedangkan setelah penerapan MFA seluruh 1.000 kombinasi *password* selesai diuji dalam waktu 1 jam 8 menit 20 detik 621 milidetik tanpa berhasil memperoleh akses ke dalam sistem. Hasil tersebut menunjukkan bahwa penerapan MFA berbasis *face recognition* secara efektif meningkatkan keamanan autentikasi pada platform *E-Learning* dengan mencegah akses tidak sah meskipun kredensial yang benar berhasil diperoleh. Meskipun demikian, hasil pengujian *Spoofing Attack* menunjukkan bahwa sistem masih berpotensi mengalami *False Acceptance* terhadap media foto tertentu, sehingga penerapan mekanisme *liveness detection* dapat dipertimbangkan sebagai pengembangan pada penelitian selanjutnya.

Referensi

[1] A. S. Puspaningrum, E. R. Susanto, and N. Neneng, “Penerapan Dan Pelatihan e-Learning Pada SMA Tunas Mekar Indonesia,” *Jurnal Pengabdian Kepada Masyarakat (JPKM) TABIKPUN*, vol. 2, no. 2, pp. 91–100, Jul. 2021, doi: 10.23960/jpkmt.v2i2.34.

[2] A. M. Sari *et al.*, “PENGUKURAN EFEKTIVITAS SQL INJECTION PADA WEBSITE DENGAN MENGGUNAKAN TOOLS JSQL, HAVIJ, dan THE MOLE,” 2023.

[3] K. G. J. W. Buana, L. Widyawati, and O. Asroni, “Analisis Dan Implementasi Keamanan Authentication Menggunakan Multi Factor Authentication (MFA) pada Aplikasi Web,” Sep. 2025. doi: https://doi.org/10.30812/corisindo.v1.5549.

[4] N. R. Andri and F. Fadly, “Penerapan Face Recognition Pada Sistem Presensi,” *Journal of Applied Computer Science and Technology*, vol. 2, no. 1, pp. 12–17, Jun. 2021, doi: 10.52158/jacost.v2i1.121.

[5] P. Kamencay, M. Benco, T. Mizdos, and R. Radil, “A new method for face recognition using convolutional neural network,” *Advances in Electrical and Electronic Engineering*, vol. 15, no. 4 Special Issue, pp. 663–672, 2021, doi: 10.15598/aeee.v15i4.2389.

[6] R. R. Rafi, R. A. Ramadhani, and A. Sanjaya, “PEMANFAATAN ALGORITMA COSINE SIMILARITY UNTUK MENGKOREKSI UJIAN ESAI,” *JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)*, vol. 10, no. 3, pp. 2242–2254, Aug. 2025, doi: 10.29100/jipi.v10i3.8058.

[7] F. A. Febriyanti, “IMAGE PROCESSING DENGAN METODE CONVOLUTIONAL NEURAL NETWORK (CNN) UNTUK DETEKSI PENYAKIT KULIT PADA MANUSIA,” 2024, [Online]. Available: https://ejournal.warunayama.org/kohesi

[8] A. L. Seandrio, A. H. Pratomo, and Y. M. Florestiyanto, “Implementasi Convolutional Neural Network (CNN) Pada Pengenalan Ekspresi Wajah,” *Jurnal Informatika dan Teknologi Informasi*, vol. 18, no. 2, pp. 211–221, 2021, doi: 10.31515/telematika.v18i2.4823.

[9] Q. Cao, L. Shen, W. Xie, O. M. Parkhi, and A. Zisserman, “VGGFace2: A Dataset for Recognising Faces across Pose and Age,” in *2018 13th IEEE International Conference on*

Automatic Face & Gesture Recognition (FG 2018), 2022, pp. 67–74. doi: 10.1109/FG.2018.00020.

[10] H. D. Lie and M. M. Engel, “LIBRARY SELF SERVICE SYSTEM USING NFC AND 2FA GOOGLE AUTHENTICATOR,” *Jurnal Teknik Informatika (JUTIF)*, vol. 3, no. 3, 2022, doi: 10.20884/1.jutif.2022.3.3.345.

[11] S. A. Rahmah, “Efektifitas Penerapan Algoritma Brute Force dan Penyalahgunaannya Dalam Sistem Berbasis Web,” vol. 2, no. 3, pp. 112–119, 2023, doi: 10.56427/jcbd.v2n3.235.