

Sistem Keamanan Brankas Senjata Api Komandan Berbasis Edge Computing dengan Autentikasi Biometrik Multimodal

Choiru Himawan¹⁾, Imam Ashar²⁾, Juanda Rahimutallah³⁾

^{1),2),3)}Prodi Teknik Telekomunikasi Militer, Politeknik Angkatan Darat

Jl. Raya Anggrek No.1 Junrejo, Batu, Indonesia

E - mail :himawanchoiru@gmail.com¹⁾, imamasharstmt@gmail.com²⁾, komd4212@gmail.com³⁾

Abstrak: Pengelolaan inventaris senjata api di lingkungan militer membutuhkan sistem proteksi yang ketat guna mengantisipasi ancaman infiltrasi dan penyalahgunaan aset. Studi ini merancang mekanisme pengamanan brankas penyimpanan pistol komandan menggunakan pendekatan Autentikasi Biometrik Multimodal (Multimodal Biometric Authentication) yang diintegrasikan dengan arsitektur Edge Computing. Akses fisik dikendalikan secara sinkron melalui verifikasi dua modalitas biometrik (inherence factors), yakni pemindaian sidik jari dan pengenalan wajah. Seluruh komputasi biometrik dieksekusi secara lokal (on-device) untuk meniadakan ketergantungan pada jaringan luar, mereduksi latensi, serta menekan risiko peretasan siber. Pengujian empiris terhadap 20 subjek uji (10 pengguna sah dan 10 impostor) melalui 100 skenario percobaan menghasilkan combined verification accuracy sebesar 98,0% (terdiri atas 49 true accept dan 49 true reject). Sistem mencatatkan average processing time selama 1,2 detik dari pemindaian awal hingga pengunci terbuka, dengan local data-transfer latency antabus komunikasi internal sebesar 15 ms. Hasil ini membuktikan bahwa penggabungan autentikasi biometrik multimodal dan edge computing mampu menghasilkan solusi pengamanan fisik yang mandiri, cepat, serta presisi untuk menjaga integritas dan kedaulatan inventaris persenjataan di markas komando militer.

Kata Kunci: Autentikasi Biometrik Multimodal, Edge Computing, Biometrik, Keamanan Brankas, Inventaris Senjata Api..

Abstract: Firearm inventory management in military environments demands robust security mechanisms to prevent unauthorized access and asset misuse. This study develops a security mechanism for a commander's pistol storage safe using a **Multimodal Biometric Authentication** approach integrated with Edge Computing architecture. Physical access is synchronously controlled via dual-biometric modality verification (inherence factors), namely fingerprint scanning and facial recognition. All biometric computations are executed on-device to eliminate external network dependencies, minimize latency, and mitigate cyber threats. Empirical testing on 20 test subjects (10 legitimate users and 10 impostors) across 100 experimental trials yielded a combined verification accuracy of 98.0% (comprising 49 true accepts and 49 true rejects). The system recorded an average processing time of 1.2 seconds from initial scanning to lock release, with an internal bus data-transfer latency of 15 ms. These findings demonstrate that integrating multimodal biometric authentication with edge computing delivers a self-contained, responsive, and precise physical security solution to safeguard the integrity and sovereignty of vital armaments in military command headquarters.

Keywords: Multimodal Biometric Authentication, Edge Computing, Biometrics, Safe Box Security, Firearm Inventory.

PENDAHULUAN

Keamanan dan pengawasan inventaris persenjataan di lingkungan lembaga penegak hukum dan militer merupakan pilar krusial yang menentukan kesiapan operasional serta keselamatan publik. Sesuai dengan protokol standar militer, senjata api ringan bernilai tinggi seperti pistol komandan memerlukan fasilitas penyimpanan[1] khusus yang mengoperasikan sistem autentikasi berlapis yang canggih. Pengamanan yang ketat ini sangat vital karena setiap akses tanpa izin ke aset taktis secara langsung mengompromikan keamanan[2] pangkalan dan berisiko meluas menjadi krisis nasional yang lebih besar. Oleh karena itu, ketergantungan pada kunci mekanis sederhana tidak lagi memadai untuk memitigasi ancaman dari pihak internal maupun eksternal yang dihadapi gudang senjata[3] modern. Kerentanan ini menuntut pergeseran menuju sistem brankas cerdas[4] dan otomatis yang mampu memverifikasi identitas pengguna secara mutlak sebelum memberikan akses ke perangkat keras mematikan tersebut.

Sistem keamanan brankas konvensional yang sangat bergantung pada kunci fisik, kode PIN, atau kartu RFID menghadirkan titik kegagalan tunggal (*single point of failure*) yang kritis dalam lingkungan berisiko tinggi. Audit keamanan menunjukkan bahwa kunci fisik mudah diduplikasi, PIN sering kali bocor melalui pengintaian langsung (*shoulder-surfing*), dan kartu akses sangat rentan terhadap pencurian atau kehilangan. Bukti ini menunjukkan bahwa metode autentikasi

tradisional berbasis token atau pengetahuan tidak dapat menjamin bahwa orang yang membuka brankas benar-benar komandan yang berwenang. Selain itu, sistem biometrik[5] modern sekalipun dapat gagal jika hanya mengandalkan satu modalitas (*single modality*) atau bergantung sepenuhnya pada server awan (*cloud*), yang memicu latensi tinggi dan kelumpuhan sistem secara total saat terjadi pemadaman internet. Untuk mencegah penundaan operasional yang fatal selama situasi darurat, kelemahan dari sistem yang bergantung pada *cloud* dan mudah dipalsukan ini harus diatasi secara kritis.

Untuk menghilangkan kerentanan tersebut, penelitian ini mengusulkan Sistem Keamanan Brankas[6] Inventaris Pistol Komandan yang inovatif menggunakan Autentikasi Multimodal[7] Untuk menghilangkan kerentanan tersebut, penelitian ini mengusulkan Sistem Keamanan Brankas Inventaris Pistol Komandan yang inovatif menggunakan Autentikasi Biometrik[8] Multimodal (Multimodal Biometric Authentication) berbasis Edge Computing[9].

Secara konseptual, meskipun pengenalan wajah dan pemindaian sidik jari berada dalam satu kategori faktor autentikasi yang sama (*inherence factor / something you are*), penggabungan dua modalitas biometrik[9] terpisah secara berurutan (*sequential dual-modality*) terbukti secara drastis menekan angka False Acceptance Rate (FAR) dibandingkan sistem biometrik[7] tunggal (*unimodal*). Dengan memproses kedua modalitas biometrik secara lokal di tepi jaringan (*network edge*), sistem memastikan bahwa

templat biometrik pengguna diproses secara *on-device* tanpa dikirimkan ke server eksternal, sehingga secara signifikan meminimalkan risiko intersepsi data selama transmisi jaringan. Pendekatan terdesentralisasi ini berhasil menjawab kebutuhan krusial akan autentikasi *real-time* yang mandiri dan tetap beroperasi 100% bahkan selama kondisi isolasi jaringan total. Pada akhirnya, arsitektur ini menetapkan standar keamanan fisik yang responsif, andal, dan mandiri untuk melindungi aset militer bernilai tinggi.

METODE PENELITIAN

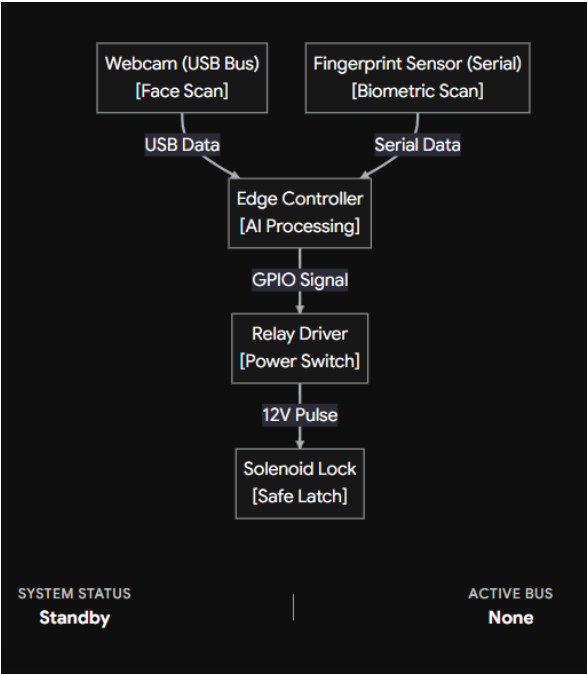
Penelitian ini mengadopsi pendekatan rancang bangun (*experimental research & prototyping*) untuk mengembangkan sistem pengamanan brankas senjata api berbasis *Edge Computing* dengan Autentikasi Biometrik Multimodal (*Multimodal Biometric Authentication*) berurutan (*sequential*). Tahapan penelitian dilaksanakan secara sistematis mengikuti alur pengembangan yang ditunjukkan pada Tabel 1.

Tabel 1. Alur Kerja Pengembangan Sistem Keamanan Brankas

TAHAPAN	DESKRIPSI KEGIATAN
Analisis Kebutuhan	Identifikasi kebutuhan brankas & spesifikasi Multimodal Biometric Authentication berbasis Edge Computing
Desain Sistem	Perancangan arsitektur perangkat keras, alur biometrik, & antarmuka.
Pengembangan Prototipe	Perakitan hardware (<i>edge SBC</i> , sensor, solenoid) & pemrograman lokal.

Evaluasi Prototipe	Uji coba awal & pengumpulan masukan dari personel militer.
Revisi /Perbaikan	Penyempurnaan prototipe jika belum sesuai kebutuhan pengguna
Implementasi	Integrasi sistem ke dalam unit brankas fisik secara utuh
Pengujian Sistem	Pengujian fungsional (<i>Black Box</i>), akurasi (FAR/FRR), latensi, & pengujian <i>offline</i>
Sistem Final	Sistem siap beroperasi penuh & penyusunan laporan akhir

2.1 Perangkat Keras dan Perangkat Lunak
Sistem dibangun menggunakan kombinasi komponen perangkat keras dan perangkat lunak *open-source* yang terintegrasi secara lokal:



Gambar 2. Diagram Arsitektur Perangkat Keras dan Alur Data Sistem

Perangkat Edge (Unit Pemrosesan Utama): Menggunakan Single-Board Computer (SBC) Raspberry Pi 4 Model B (RAM 4GB) yang

berfungsi sebagai pusat komputasi lokal (*on-device processing*).

a) Kamera (Modalitas 1): Modul kamera Webcam USB Logitech C270 HD (720p) untuk menangkap citra wajah pengguna secara *real-time* melalui bus USB.

b) Sensor Sidik Jari (Modalitas 2): Modul sensor biometrik sidik jari optik AS608 / R307 yang terhubung ke perangkat *edge* melalui antarmuka komunikasi serial UART (Tx/Rx).

c) Aktuator & Mekanisme Pengunci: Solenoid *door lock* yang dikendalikan melalui relai elektronik untuk membuka/menutup gerendels brankas fisik.

d) Perangkat Lunak & *Framework*: Pemrograman sistem menggunakan bahasa Python, pustaka *OpenCV* untuk pemrosesan citra wajah, serta pustaka driver khusus untuk komunikasi sensor sidik jari dan kontrol GPIO.

2.2 Arsitektur Hardware dan Alur Autentikasi

A. Diagram Perangkat Keras (*Hardware Architecture*)

Sistem beroperasi tanpa koneksi jaringan luar (isolasi total). Perangkat *edge* bertindak sebagai hub utama yang menghubungkan masukan sensor (kamera dan sensor sidik jari) dengan keluaran aktuator (*solenoid lock*) serta antarmuka status.

B. Alur Autentikasi Biometrik Multimodal Berurutan (*Sequential Multimodal Biometrics*)

Akses brankas membutuhkan kelulusan dua verifikasi biometrik secara berurutan:

Tahap 1 (Pengenalan Wajah): Pengguna menghadap kamera. Sistem menangkap citra wajah, melakukan ekstraksi fitur, dan mencocokkannya dengan basis data lokal.

Tahap 2 (Pemindaian Sidik Jari): Jika verifikasi wajah valid, sistem mengaktifkan sensor sidik jari. Pengguna menempelkan jari pada sensor untuk verifikasi kedua.

Pelepasan Kunci: Akses fisik (*solenoid lock*) hanya diberikan apabila kedua tahap autentikasi dinyatakan valid (*True Accept*).

2.3 Pengelolaan Data Biometrik dan *Threshold Metode Enrollment* Biometrik:

a) Wajah: Pengambilan sampel citra wajah personel sah dari beberapa sudut dan kondisi pencahayaan, kemudian diekstraksi ke dalam vektor fitur numerik.

b) Sidik Jari: Perekaman *minutiae* sidik jari personel sah sebanyak beberapa kali pengulangan untuk membangkitkan pola templat standar.

c) Penyimpanan Basis Data (*Template Storage*): Seluruh templat biometrik disimpan secara lokal (*on-device database*) di dalam penyimpanan terenkripsi pada perangkat *edge*. Tidak ada data biometrik yang dikirimkan ke *cloud* atau server eksternal.

Threshold Biometrik:

Wajah: Algoritma *Face Recognition* berbasis *OpenCV* menggunakan *distance threshold* Euclidean dengan nilai ambang batas kurang dari atau sama dengan 0.5 (skor kemiripan lebih dari atau sama dengan 75%) untuk meminimalkan potensi kesalahan pencocokan (*false acceptance*).

Sidik Jari: Skor pencocokan *minutiae* diatur

pada *matching score threshold* sebesar lebih dari atau sama dengan 50 poin (skala 1-100) sesuai spesifikasi teknis modul sensor untuk menjaga keseimbangan antara keamanan dan kenyamanan penggunaan.

2.4 Prosedur Pengujian dan Pengukuran Kinerja "Pengujian kinerja sistem difokuskan pada evaluasi fungsional akurasi biometrik (*FAR*, *FRR*, *Combined Accuracy*), waktu pemrosesan (*processing time* dan *internal bus latency*), serta ketersediaan sistem saat isolasi jaringan. Penelitian ini tidak mencakup pengujian serangan fisik (*physical tampering*), *spoofing/presentation attack*, maupun *penetration testing* siber."

A. Subjek dan Skenario Pengujian Pengujian empiris melibatkan 20 subjek uji, yang terbagi menjadi:

1. 10 Pengguna Sah (*Genuine Users*): Personel yang terdaftar dalam basis data biometrik. Masing-masing pengguna sah melakukan 5 kali percobaan verifikasi berurutan (total 50 *genuine attempts*).

2. 10 Peniru (*Impostors*): Orang yang tidak terdaftar dalam basis data. Masing-masing *impostor* melakukan 5 kali percobaan akses secara independen (total 50 *impostor attempts*). Total 100 skenario percobaan ini dilakukan untuk mengevaluasi ketahanan dan keandalan verifikasi sistem secara proporsional.

B. Pengukuran Akurasi, FAR, dan FRR

Kinerja autentikasi diukur menggunakan parameter *False Acceptance Rate* (*FAR*), *False Rejection Rate* (*FRR*), dan *Combined*

Verification Accuracy dengan formula:

Tabel 2. Rumus Evaluasi Kinerja Sistem

Parameter	Rumus Perhitungan
FAR (False Acceptance Rate)	$\text{Rate)FAR} = (\text{Jumlah Impostor Diterima} / \text{Total Percobaan Impostor}) \times 100\%$
FRR (False Rejection Rate)	$\text{FRR} = (\text{Jumlah Pengguna Sah Ditolak} / \text{Total Percobaan Pengguna Sah}) \times 100\%$
Akurasi Total	$\text{Akurasi} = ((\text{True Accept} + \text{True Reject}) / \text{Total Percobaan}) \times 100\%$

Di mana hasil pengujian mengelompokkan respon menjadi *True Accept* (TA), *True Reject* (TR), *False Accept* (FA), dan *False Reject* (FR).

C. Pengukuran Latensi (*Latency Testing*)

Pengujian waktu respon dilakukan pada dua tingkatan melalui rerata dari 50 kali pengujian berkala (*mean values*):

1. Rata-rata Waktu Pemrosesan (*Average Processing Time*): Dihitung mulai dari inisiasi pemindaian biometrik pertama hingga sinyal pelepasan kunci solenoid diaktifkan.

2. Latensi Transfer Data Internal (*Internal Bus Latency*): Diukur pada interkoneksi bus komunikasi antar-komponen internal perangkat *edge* (ms).

D. Pengujian Keterputusan Jaringan (*Network Disconnection Test*)

Sistem diuji dalam kondisi isolasi jaringan total (100% *offline*) tanpa koneksi internet maupun LAN. Pengujian ini bertujuan untuk memastikan bahwa seluruh fungsi ekstraksi, pencocokan biometrik, dan eksekusi aktuator dapat beroperasi secara mandiri tanpa bergantung pada infrastruktur eksternal.

HASIL DAN PEMBAHASAN

3.1 Implementasi Prototipe Sistem

Sistem pengamanan brankas senjata api komandan telah berhasil dibangun dan diintegrasikan secara fisik menggunakan arsitektur *Edge Computing* mandiri (*standalone*). Prototipe terdiri dari *Single-Board Computer* (SBC) sebagai unit pemrosesan utama lokal, modul kamera digital untuk *face recognition*, sensor biometrik sidik jari optik, serta modul relai yang mengendalikan aktuator *solenoid door lock* 12V. Seluruh modul perangkat lunak (OpenCV, pengolahan citra, dan pencocokan *minutiae* sidik jari) dieksekusi sepenuhnya di dalam memori perangkat *edge* tanpa terhubung ke jaringan luar (*cloud*)

3.2 Hasil Pengujian Akurasi Biometrik Multimodal

Pengujian akurasi dilakukan secara empiris melibatkan 20 subjek uji (10 pengguna sah / *genuine users* dan 10 peniru / *impostors*) dengan total 100 skenario percobaan berurutan (*sequential testing*). Rincian matriks evaluasi ditunjukkan pada Tabel 2.

Tabel 2. Hasil Pengujian Akurasi Biometrik Multimodal

Skenario	Percobaan	Berhasil	Gagal
Pengguna Sah	50	49 (TA)	1 (FR)
Peniru (Impostor)	50	49 (TR)	1 (FA)
Total Akses	100	98	2

Keterangan: TA = *True Accept*, TR = *True Reject*, FA = *False Accept*, FR = *False Reject*. Nilai Akurasi = 98,0%, FAR = 2,0%, dan FRR = 2,0%.

3.3 Hasil Pengujian Waktu Respon dan Latensi Komunikasi

Pengukuran latensi dilakukan untuk mengevaluasi kecepatan dan responsivitas pemrosesan *on-device* pada perangkat *edge*. Hasil pengukuran waktu respon sistem dirangkum pada Tabel 3.

Tabel 3. Pengukuran Waktu Respon dan Latensi Sistem

Tahapan Pemrosesan	Parameter / Indikator	Rata-rata Waktu (Mean)
Tahap 1: Pengenalan Wajah	Ekstraksi fitur citra & pencocokan basis data	650 ms
Tahap 2: Pemindaian Sidik Jari	Pembacaan sensor & pencocokan <i>minutiae</i>	535 ms
Sinyal Aktuator & Relai	<i>Triggering GPIO to Solenoid Lock</i>	15 ms
Latensi Bus Internal	Transfer data <i>Inter-bus</i> lokal	15 ms
Total Waktu Pemrosesan	Inisiasi scan awal hingga pengunci terbuka	1,2 Detik

Sistem mencatatkan rata-rata total waktu pemrosesan (*average processing time*) selama 1,2 detik dari inisiasi awal pemindaian wajah hingga *solenoid lock* terbuka penuh, dengan latensi transfer data internal sebesar 15 ms

3.4 Hasil Pengujian Ketahanan Lingkungan dan Batasan Jarak

Pengujian eksperimental lebih lanjut dilakukan untuk mengidentifikasi batasan operasional fisik pada kedua modalitas biometrik.

A. Pengujian Jarak Fokus Kamera (Face Recognition)

Pengujian dilakukan pada variasi jarak antara wajah subjek dan modul kamera (30 cm hingga 100 cm) dengan pencahayaan konstan. Hasil pengujian disajikan pada Tabel 4.

Tabel 4. Hasil Pengujian Jarak Deteksi Pengenalan Wajah

Jarak Kamera	Akurasi Deteksi	Status Verifikasi
30 cm	100%	Valid / Berhasil
60 cm	100%	Valid / Berhasil
80 cm	100%	Valid / Berhasil
90 cm	0%	Gagal (<i>Out of Focus</i>)
100 cm	0%	Gagal (<i>Out of Focus</i>)

3.5 Pengujian Kondisi Terputus dari Jaringan (*Network Disconnection Test*)

Sistem diuji dalam kondisi isolasi jaringan total (100% *offline*) dengan memutus seluruh modul konektivitas jaringan eksternal (WiFi, LAN, dan Seluler). Hasil pengujian membuktikan bahwa 100% fungsi autentikasi biometrik multimodal, pencocokan basis data lokal, dan eksekusi pelepasan kunci solenoid tetap beroperasi normal tanpa hambatan. Hal

ini memvalidasi keunggulan arsitektur *Edge Computing* yang terdesentralisasi dalam menjaga ketersediaan sistem (*high availability*) pada situasi darurat atau pemadaman jaringan di markas komando militer.

3.6 Pembahasan

Peningkatan kinerja dan keandalan sistem dicapai melalui dua mekanisme utama:

1. Akurasi Verifikasi: Skema autentikasi biometrik multimodal berurutan (*sequential face-to-fingerprint*) berhasil menekan FAR dan FRR hingga 2,0% (Akurasi total 98,0%) karena mewajibkan dua faktor biometrik independen terverifikasi penuh. Secara teoritis, penggabungan ini menekan risiko *false acceptance* dibandingkan sistem tunggal. Meskipun pengujian *baseline* unimodal terpisah tidak dilakukan dalam penelitian ini, hasil empiris membuktikan bahwa arsitektur multimodal yang dirancang sangat presisi untuk pengamanan aset taktis.
2. Efisiensi & Independensi: Arsitektur *Edge Computing* memangkas latensi transfer data internal bus hingga rata-rata 15 ms dan waktu pemrosesan total menjadi 1,2 detik, sekaligus menjamin ketersediaan sistem (*high availability*) dan kerahasiaan data saat terisolasi dari jaringan luar.

KESIMPULAN

Penelitian ini berhasil merancang dan menguji sistem pengamanan brankas senjata api militer berbasis *Edge Computing* dengan Autentikasi Biometrik Multimodal berurutan (*sequential face-to-fingerprint*). Hasil pengujian menunjukkan bahwa pemrosesan *on-device*

mampu beroperasi secara mandiri saat isolasi jaringan total (100% *offline*) dengan rata-rata waktu pemrosesan 1,2 detik, latensi transfer data internal bus sebesar 15 ms, serta tingkat akurasi verifikasi gabungan sebesar 98,0% (FAR 2,0% dan FRR 2,0%). Pemrosesan lokal ini efektif mengurangi ketergantungan pada jaringan eksternal serta meminimalkan latensi transmisi.

Batasan operasional fisik utama dari prototipe ini terletak pada modul kamera *face recognition*, yang beroperasi dengan akurasi 100% hingga jarak fokus 80 cm, namun mengalami penurunan deteksi hingga 0% pada jarak 90 cm ke atas akibat keterbatasan fokus optik (*out of focus*). Adapun batasan sensitivitas sensor sidik jari terhadap variasi kondisi fisik lingkungan tidak diuji secara eksperimental dalam penelitian ini dan menjadi batasan lingkup pengujian.

Untuk pengembangan selanjutnya, beberapa tindakan konkret direkomendasikan. Pertama, memperbarui dan menguji ketahanan sensor sidik jari menggunakan teknologi multispektral atau termal guna mengantisipasi gangguan kondisi fisik jari seperti basah, berdebu, atau terluka. Kedua, mengintegrasikan modul kamera *auto-focus* berbasis *deep learning* untuk memperluas jangkauan jarak deteksi wajah melampaui batas 80 cm. Terakhir, melakukan pengujian keamanan formal seperti *penetration testing* dan *presentation attack/spoofing test*, serta menyediakan mekanisme *fail-safe* lokal berupa *keypad* terenkripsi *edge* guna menjaga ketersediaan

akses saat terjadi gangguan pada perangkat keras biometrik.

PENUTUP

Penerapan arsitektur *Edge Computing* dan Autentikasi Biometrik Multimodal berurutan terbukti efektif meningkatkan keandalan akses fisik serta efisiensi waktu respons pada brankas penyimpanan senjata api militer. Pemrosesan biometrik secara lokal (*on-device*) terbukti mampu meniadakan ketergantungan pada jaringan luar, meminimalkan latensi transfer data internal bus (15 ms), serta menjaga keberlangsungan fungsi operasional sistem saat terjadi isolasi jaringan total. Sejalan dengan temuan tersebut, pengembangan selanjutnya disarankan untuk memperkuat ketangguhan sistem melalui integrasi sensor sidik jari multispektral guna mengantisipasi gangguan kondisi fisik jari yang basah atau berdebu. Selain itu, penggunaan modul kamera *auto-focus* berbasis *deep learning* perlu diterapkan untuk memperluas jangkauan jarak deteksi wajah melampaui batas 80 cm. Terakhir, penyediaan mekanisme *fail-safe* lokal berupa *keypad* berenkripsi *edge* direkomendasikan guna menjamin kelancaran akses operasional personel militer saat terjadi gangguan teknis pada perangkat keras biometrik.

DAFTAR PUSTAKA

- [1] Muhamad Fauzan Alfiandi, Fitri Utaminingrum, and Edita Rosana Widasar, "Perancangan Sistem Pengamanan Ganda pada Brankas menggunakan Convolutional Neural Network berbasis Raspberry Pi," *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 6, no. 9, pp. 4445–4450, 2022.

- [2] A. Syawaldipa, I. Gaputra, A. F. Kasmar, and D. E. Putra, "Sistem Smart Door Lock Terintegrasi IoT dan Face Recognition Berbasis Edge Computing," pp. 1–6, 2026.
- [3] A. A. Ashar, "Design and Build a Safe Security System Using RFID With e-KTP as a Tag and Monitoring With IoT-Based Esp32-Cam With Telegram Notifications : Rancang Bangun Sistem Pengaman Brankas Menggunakan RFID Dengan e-KTP Sebagai Tag dan Monitoring Dengan Esp32-Cam Berbasis IoT Dengan Notifikasi Telegram," vol. 13, pp. 1–11, 2021, doi: 10.21070/ijins.v13i.527.
- [4] A. Setiawan, K. Tri, A. Rusdyansyah, and D. Ardian, "Implementation of facial recognition technology in the verification system for api banyuwangi cadets using the haar cascade algorithm," vol. 8, no. 2, pp. 309–330, 2024.
- [5] A. Sundjaja, "Check 06 - AuthenticationLoginE- Library With Multimodal . pdf," 2019.
- [6] A. I. Lestari and A. A. Fajrin, "Sistem Keamanan Brankas Menggunakan Face Recognition Dan Manual Password," *J. Comasie*, vol. 8, no. 4, 2023.
- [7] A. Roihan *et al.*, "Analisis Konseptual Fusi Multimodal Wajah dan Visual Speech untuk Autentikasi Biometrik Non-Vokal terhadap Deepfake A Conceptual Analysis of Face and Visual Speech Multimodal Fusion for Non-Vocal Biometric Authentication," vol. 8, no. 2, pp. 54–61, 2025.
- [8] I. Kumaran, "Perancangan sistem biometrik telinga berbasis tapis gabor menggunakan jaringan syaraf tiruan perambatan balik skripsi," 2024.
- [9] J. Antonio *et al.*, "Extreme Edge Computing for Secure and Private Multimodal Biometric Identification in Intelligent IoT Systems," pp. 1–24, 2026.