https://journaledutech.com/index.php/great
Global Research and Innovation Journal (GREAT)
Volume 2, Nomor 1, 2026, Hal. 999-1008
ISSN : 3090-3289

AKSES MASUK GERBANG MENGGUNAKAN *FACE RECOGNITION* DENGAN METODE MULTI-TASK CASCADED CONVOLUTIONAL NETWORK (MTCNN) BERBASIS IOT

Jayanti Logita Sari
Teknik Elektro, Universitas Widya Gama, Malang
E-mail: gita1989sweet@gmail.com

ABSTRAK

Keamanan akses masuk sekolah menjadi hal yang sangat penting untuk melindungi siswa, guru, dan seluruh aktivitas di dalam lingkungan sekolah. Penelitian ini bertujuan merancang sistem akses pintu gerbang otomatis yang dapat mengenali wajah pengguna dan dengan bantuan teknologi Internet of Things (IoT) dapat mengontrol akses pintu gerbang sekolah dari jarak jauh. Pada sistem ini digunakan dua modul ESP32-CAM, di mana kamera pertama berfungsi sebagai pengenalan wajah dan monitoring, sementara kamera kedua bertugas sebagai kontrol jarak jauh. Pada ESP32-CAM memiliki library bawaan untuk *face recognition* yang menggunakan metode MTCNN. Setelah wajah dikenali, data dikirimkan melalui jaringan WiFi dan dipantau melalui web. Aplikasi Blynk digunakan untuk mengambil gambar keadaan secara langsung dan mengontrol buka tutup kunci pintu gerbang dari jarak jauh. Proses pengenalan wajah dilakukan di dalam perangkat ESP32-CAM, sehingga sistem tidak bergantung pada server luar dan mampu bekerja lebih cepat. Hasil pengujian menunjukkan bahwa sistem dapat mengenali wajah dengan baik pada kondisi cahaya normal, dengan akurasi 95%, pada jarak maksimal 80 cm dan sistem dapat dikontrol melalui aplikasi Blynk dengan akurasi 85%, memberikan respon pembukaan kunci gerbang dalam waktu rata-rata kurang dari 3 detik.

Kata kunci **Face Recognition, MTCNN, IoT, ESP32-CAM**

ABSTRACT

School access security is very important to protect students, teachers, and all activities within the school environment. This study aims to design an automatic gate access system that can recognize users' faces and, with the help of Internet of Things (IoT) technology, can control school gate access remotely. This system uses two ESP32-CAM modules, where the first camera functions as face recognition and monitoring, while the second camera is used for remote control. The ESP32-CAM has a built-in library for face recognition that uses the MTCNN method. Once a face is recognized, the data is sent via a WiFi network and monitored via the web. The Blynk application is used to take live images and remotely control the opening and closing of the gate lock. Test results show that the system can recognize faces well under normal lighting conditions, with 95% accuracy, at a maximum distance of 80 cm. The system can be controlled via the Blynk application with 85% accuracy, providing a gate lock opening response in an average time of less than 3 seconds.

Keywords ***Face Recognition, MTCNN, IoT, ESP32-CAM***

1. PENDAHULUAN

Di era modern, tantangan terhadap keamanan di lingkungan pendidikan semakin kompleks. Tidak hanya ancaman fisik seperti kekerasan, pencurian, atau perundungan (bullying), tetapi juga ancaman non-fisik seperti cyberbullying, pelecehan daring, dan penyalahgunaan teknologi informasi. Manajemen sekuriti di lingkungan pendidikan

bertujuan untuk menciptakan lingkungan yang aman dan kondusif bagi seluruh aktivitas belajar-mengajar, serta melindungi siswa, staf, dan fasilitas yang ada. Dalam perlindungan siswa, penerapan sistem keamanan seperti pengawasan ketat melalui CCTV, keberadaan petugas keamanan, dan pembatasan akses masuk hanya bagi pihak yang berkepentingan menjadi langkah utama (Sayyidah Khalillah T. et al., 2025). Namun banyak sekolah mengeluhkan sistem penguncian gerbang yang kurang efisien seperti jam di luar sekolah, hari libur, atau ketika waktu tertentu yang mengharuskan penjaga sekolah membuka kunci gerbang karena alasan penting. Kondisi ini menyulitkan petugas untuk memantau seluruh aktivitas keluar-masuk ketika sekolah sepi dan kurang penjagaan, terutama ketika terdapat orang tua, tamu, maupun pihak luar yang tidak memiliki kepentingan langsung. Akibatnya, risiko akses tidak sah ke lingkungan sekolah menjadi lebih tinggi, sementara pencatatan siapa saja yang masuk dan keluar belum dapat dilakukan secara akurat dan real-time.

Karena alasan tersebut penelitian ini dibuat, untuk mempermudah pengawasan di pintu gerbang sekolah dengan membatasi akses kunci, hanya beberapa orang saja yang dapat membuka kunci pintu gerbang sekolah dengan mengidentifikasi wajah beberapa orang. Selain itu, alat ini dapat juga digunakan sebagai media untuk mendisiplinkan siswa dan karyawan ketika datang terlambat di pagi hari.

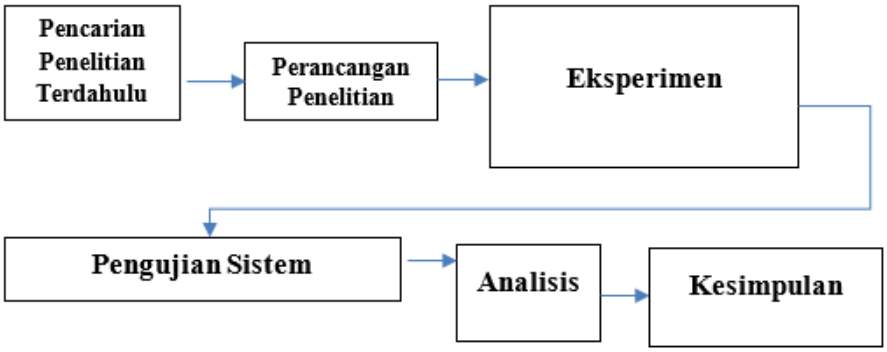
Adapun penelitian yang berjudul Rancang Bangun Keamanan Pintu Otomatis Menggunakan Face Recognition Berbasis Internet Of Things (IoT) (Zulfikar *et al.*, 2023), memang telah berhasil menghadirkan pintu otomatis berbasis IoT dengan teknologi face recognition. Namun, penelitian tersebut belum menjawab kebutuhan nyata di lingkungan sekolah, di mana keamanan bukan hanya soal membuka atau menutup pintu, tetapi juga memastikan siapa yang masuk, bagaimana proses pengawasannya, dan bagaimana petugas dapat memantau situasi secara langsung. Selain itu, penelitian terdahulu belum memanfaatkan lebih dari satu kamera untuk membedakan fungsi pengenalan wajah dan pemantauan kondisi gerbang. Karena itulah penelitian ini mencoba mengisi kekosongan tersebut dengan menghadirkan akses pintu gerbang sekolah berbasis ESP32-CAM yang tidak hanya mengenali wajah untuk akses pintu gerbang, tetapi juga menyediakan pemantauan real-time melalui platform Blynk yang dapat dikontrol sewaktu-waktu melalui *smartphone*, sehingga keamanan sekolah dapat terjaga lebih menyeluruh dan mudah diawasi.

Penelitian ini menjadi penting karena menawarkan solusi yang sederhana namun kuat, memanfaatkan ESP32-CAM untuk pengenalan wajah dan monitoring real-time. Jika diterapkan, alat ini berpotensi membantu sekolah mengurangi risiko penyusupan, meningkatkan keamanan akses, serta menciptakan lingkungan belajar yang lebih nyaman dan terlindungi bagi semua warga sekolah.

2. METODE PENELITIAN

Penelitian ini menggunakan gabungan dua metode yaitu, metode penelitian RnD (Research and Development) dan eksperimental. Metode RnD digunakan untuk mencari landasan teori dan kerangka berpikir, membantu memahami penelitian terdahulu, dan mengembangkan hasil produk yang sudah ada.

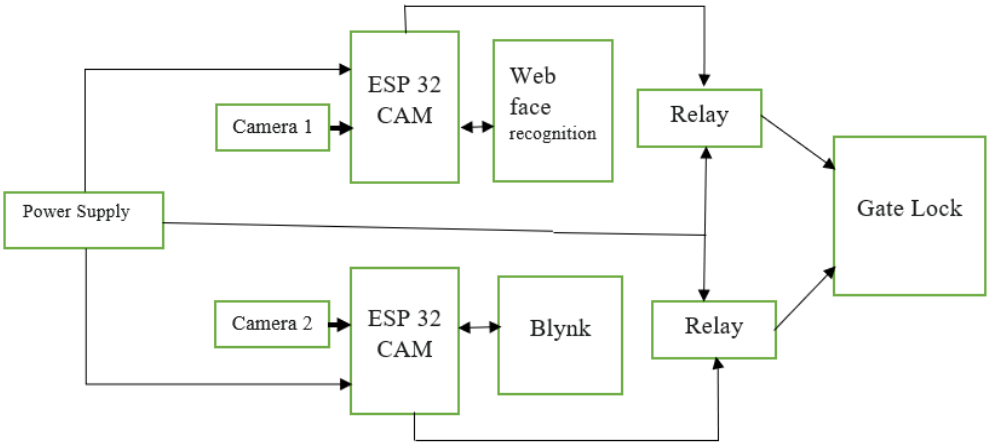
Penelitian ini bukan penelitian dengan topik baru, maka membutuhkan banyak literatur untuk menyusunnya dan sebagai dasar untuk pengembangan penelitian.



Gambar 1: Diagram Metode Penelitian

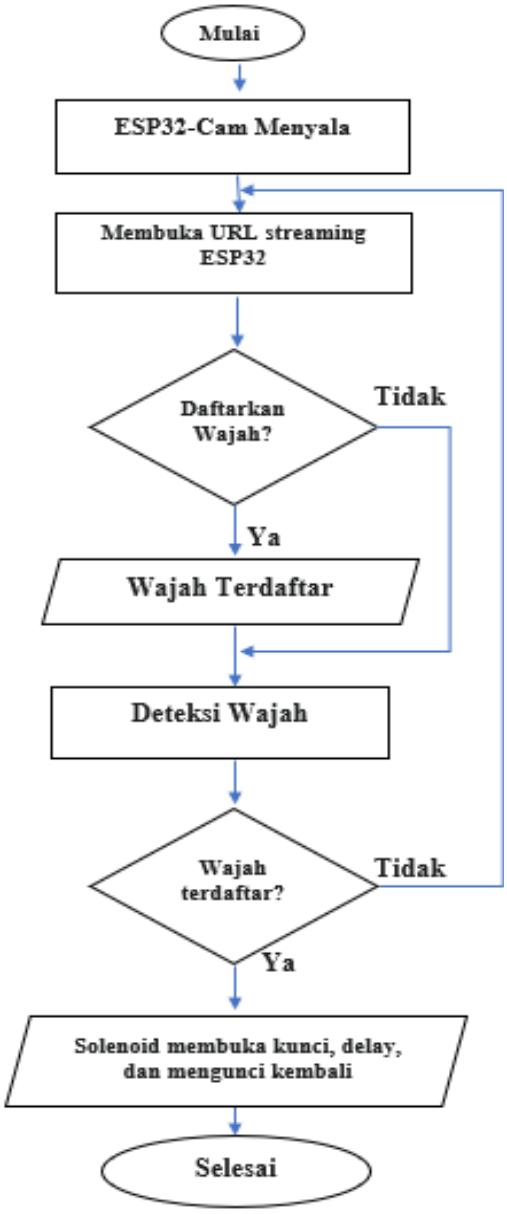
2.1 Perancangan Alat

Perangkat keras yang digunakan pada penelitian ini adalah: ESP32-CAM, kamera, power supply, modul relay, solenoid gatelock, jaringan internet, dan *smartphone*. Sedangkan untuk software penelitian ini menggunakan Arduino IDE, Blynk, dan database wajah. Pada tahap ini membuat rancangan dengan blok diagram sistem akses gerbang sekolah berbasis IoT seperti berikut.

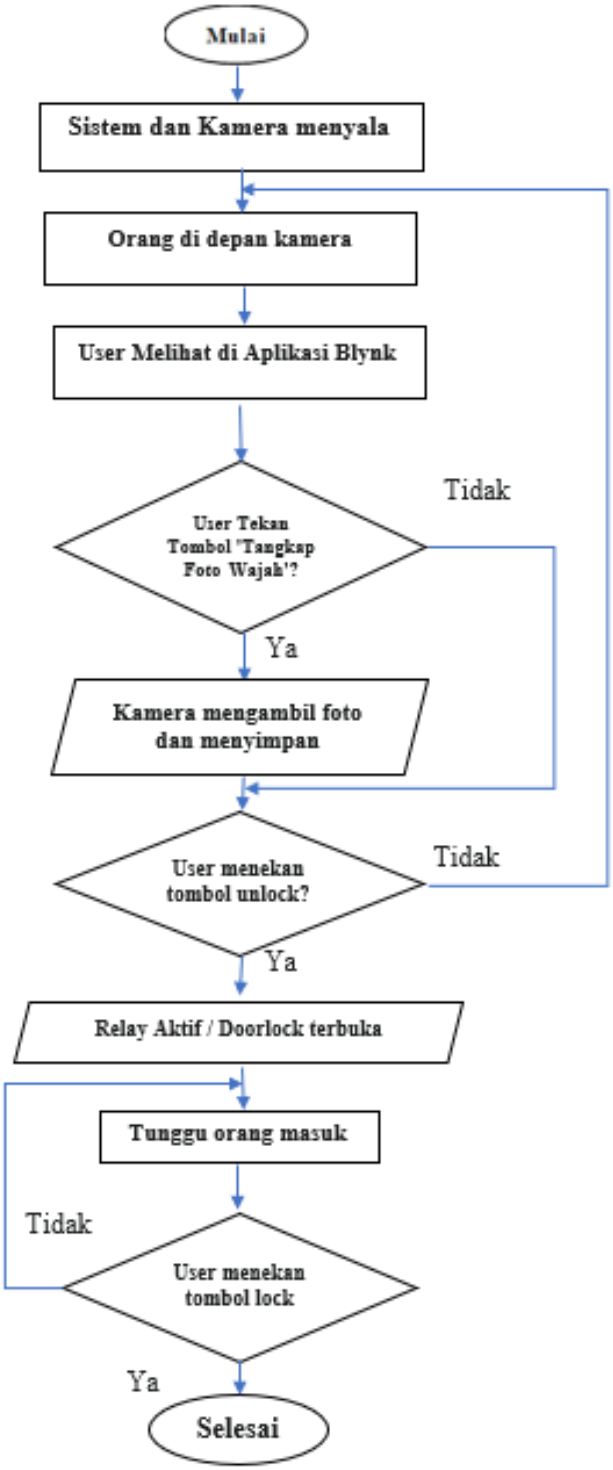


Gambar 2: Blok Diagram Perencanaan Alat

Kamera 1 terhubung dengan ESP32-CAM dan web, yang berfungsi sebagai kamera utama untuk proses *face recognition* (pengenalan wajah) dan monitoring. Sedangkan Kamera 2 terhubung dengan ESP32-CAM kedua, yang diintegrasikan dengan aplikasi Blynk sebagai sistem kontrol jarak jauh dan pengambil gambar.



Gambar 3: Flowchart Kamera 1



Gambar 4: Flowchart Kamera 2

2.2 Skenario Pengujian

Pengujian melibatkan 10 orang subjek uji yang dibagi menjadi dua kategori, yaitu subjek "dikenal" (wajah telah direkam dan disimpan dalam basis data sistem) dan subjek "tidak dikenal" (wajah tidak terdaftar). Setiap subjek melakukan beberapa kali percobaan autentikasi pada jarak 50 cm hingga 100 cm dari kamera dengan pencahayaan normal. Kamera 1 digunakan sebagai sensor utama untuk proses pengenalan wajah dan pembukaan kunci, sedangkan kamera 2 digunakan untuk kontrol kunci jarak jauh dengan memonitor wajah siapa yang akan masuk gerbang selama proses pengujian berlangsung. Setiap percobaan dicatat apakah sistem berhasil mengenali wajah dan membuka kunci atau menolak akses.

Tabel 1: Deskripsi Data Awal

Atribut	Deskripsi	Tipe Data
Nama Orang	Terdiri dari nama personal yang akan diuji	Karakter
Jarak (cm)	Jarak antara kamera dan wajah dengan range 50, 75, 85, dan 100	Integer
Objek Dikenali/Tidak	wajah dikenali =1 tidak dikenali = 0	Binary digit
Latency (detik)	Waktu yang digunakan dimulai dari perintah sampai actuator melakukan aksi	Integer
Akurasi	Menampilkan TP, TN, FP, FN	Binary digit

2.3 Confusion Matrix sebagai Dasar Evaluasi *Face Recognition*

Confusion matrix digunakan untuk menggambarkan hubungan antara hasil prediksi sistem dengan kondisi sebenarnya (Helmud *et al.*, 2024). Confusion matrix terdiri dari empat komponen utama, yaitu :

True Positive (TP): wajah dikenal dan sistem membuka kunci.
True Negative (TN): wajah tidak dikenal dan sistem menolak akses.
False Positive (FP): wajah tidak dikenal tetapi sistem membuka kunci.
False Negative (FN): wajah dikenal tetapi sistem menolak akses

a. Recall (Sensitivity)

Recall adalah ukuran yang menunjukkan kemampuan sistem dalam mendeteksi seluruh data positif yang sebenarnya. Recall mengukur seberapa besar proporsi data positif yang berhasil dikenali dengan benar oleh sistem.

$$\text{Recall} = \frac{TP}{TP + FN} \times 100\%$$

b. Presisi (Precision)

Presisi mengukur tingkat ketepatan sistem dalam memberikan prediksi positif. Presisi menunjukkan seberapa besar proporsi prediksi positif yang benar-benar sesuai dengan kondisi sebenarnya.

$$\text{Presisi} = \frac{TP}{TP + FP} \times 100\%$$

c. F1-Score

F1-Score merupakan ukuran gabungan yang menyeimbangkan nilai recall dan presisi menggunakan rata-rata harmonik. Metrik ini digunakan ketika diperlukan keseimbangan antara kemampuan mendeteksi data positif dan ketepatan prediksi sistem.

$$\text{F1-Score} = \frac{2 \times (\text{Presisi} \times \text{Recall})}{\text{Presisi} + \text{Recall}} \text{ x } 100\%$$

d. Akurasi Pengenalan Wajah

Akurasi dihitung berdasarkan hasil klasifikasi sistem terhadap wajah subjek uji. Nilai akurasi dihitung menggunakan persamaan:

$$\text{Akurasi} = \frac{TP + TN}{TP + TN + FP + FN} \times 100\%$$

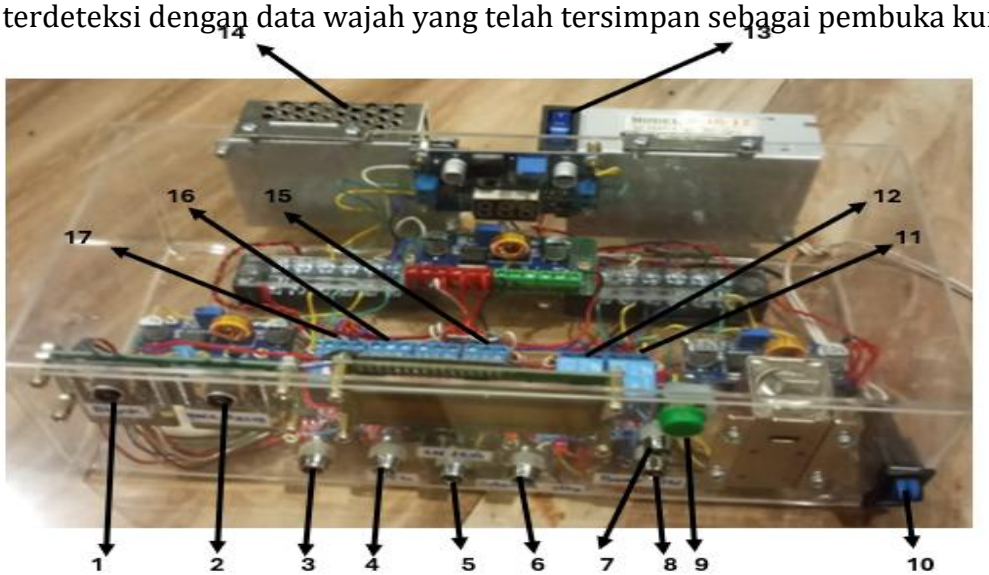
Hasil pengujian juga disajikan dalam bentuk confusion matrix sederhana untuk mempermudah analisis performa sistem.

e. Latency Pembukaan Kunci

Latency pembukaan kunci didefinisikan sebagai waktu tunda sejak wajah terdeteksi oleh kamera hingga aktuator kunci pintu aktif (kondisi terbuka). Pengukuran dilakukan dengan alat ukur waktu berupa stopwatch online yang dapat menghitung hingga milidetik. Pengukuran dihitung ketika perintah mulai dilakukan hingga aktuator melakukan perintah. Pengukuran dilakukan untuk setiap percobaan, kemudian dihitung nilai rata-rata latency.

3. HASIL DAN PEMBAHASAN

Pengujian keseluruhan sistem dilakukan dengan mensimulasikan kondisi penggunaan nyata pada akses pintu gerbang sekolah. Proses pengujian dimulai ketika sistem dinyalakan dan ESP32-CAM berada dalam kondisi siap melakukan pengambilan gambar wajah. Selanjutnya, pengguna berdiri di depan kamera pada jarak tertentu untuk dilakukan proses deteksi dan pengenalan wajah menggunakan metode Multi Task Cascaded Convolutional Network (MTCNN). Sistem kemudian membandingkan wajah yang terdeteksi dengan data wajah yang telah tersimpan sebagai pembuka kunci.



Gambar 5: Foto Keseluruhan Alat

Keterangan
a. ESP32-CAM 2 (Blynk)
b. ESP32-CAM 1 (*Face Recognition* dan monitoring)
c. LED indikaor power on ESP32-CAM 2 (merah)
d. LED indikator bel on (kuning)
e. LED indikator solenoid unlock ESP32-CAM 2 (hijau)
f. LED indikator solenoid stanby (biru)
g. LED indikator solenoid unlock ESP32-CAM 1 (hijau)
h. LED indikator power on ESP32-CAM 1 (merah)
i. Tombol bel
j. Switch on/off
k. Actuator power relay
l. Interlock relay/safety ESP32-CAM 2
m. Switch power supply untuk ESP32-CAM 2
n. Power Supply
o. Relay bel dan buzzer
p. Actuator power relay
q. Interlock relay/safety ESP32-CAM 1

3.1 Hasil Pengujian dan Analisis Face Recognition (Kamera 1)

Tabel 1. Hasil Pengujian Face Recognition (Kamera 1)

NO	NAMA	JARAK (cm)	Dikenali		LATENCY (detik)	AKURASI			
			Ya	Tidak		TP	TN	FP	FN
1	Gita	50	1	0	1,5	1	0	0	0
		75	1	0	1,3	1	0	0	0
		85	TIDAK TERDETEKSI						
		100							
2	Tisha	50	1	0	1,1	1	0	0	0
		75	1	0	1,4	0	0	0	1
		85	TIDAK TERDETEKSI						
		100							
3	Marwah	50	0	1	2	0	1	0	0
		75	0	1	1,8	0	1	0	0
		85	TIDAK TERDETEKSI						
		100							
4	Rafi	50	0	1	1,9	0	1	0	0
		75	0	1	2,2	0	1	0	0
		85	TIDAK TERDETEKSI						
		100							
5	Rere	50	0	1	1,9	0	1	0	0
		75	0	1	1,6	0	1	0	0
		85	TIDAK TERDETEKSI						
		100							
6	Valent	50	0	1	1,8	0	1	0	0
		75	0	1	2,1	0	1	0	0

		85	TIDAK TERDETEKSI						
		100							
7	Ratih	50	0	1	1,5	0	1	0	0
		75	0	1	1,9	0	1	0	0
		85	TIDAK TERDETEKSI						
		100							
8	Fadel	50	0	1	1,8	0	1	0	0
		75	0	1	2	0	1	0	0
		85	TIDAK TERDETEKSI						
		100							
9	Saka	50	0	1	2,1	0	1	0	0
		75	0	1	2,5	0	1	0	0
		85	TIDAK TERDETEKSI						
		100							
10	Raka	50	0	1	1,8	0	1	0	0
		75	0	1	2,3	0	1	0	0
		85	TIDAK TERDETEKSI						
		100							

Berikut ini perhitungan Recall, Presisi, F1-Score, Latency dan Akurasi berdasarkan tabel:

Recall $= \frac{TP}{TP+FN} \; x \; 100\ \% = \frac{4}{4+1} = 80\ \%$

Presisi $= \frac{TP}{TP+FP} \; x \; 100\ \% = \frac{4}{4+0} = 100\ \%$

F1-Score $= 2 \text{ x } \frac{Presisi \; x \; Recall}{Presisi+Recall} \; x \; 100\ \% = 2 \text{ x } \frac{1 \; x \; 0{,}8}{1 \; + \; 0{,}8} \; x \; 100\ \% = 88{,}9\ \%$

Akurasi $= \frac{(TP+TN)}{(TP+TN+FP+FN)} x100\ \% = \frac{4+15}{4+15+0+1} \; x \; 100\ \% = 95\ \%$

Latency $= \frac{jumlah \; Latency}{jumlah \; percobaan \; yang \; terdeteksi} = \frac{36{,}5}{20} = 1{,}8$ detik

Analisa hasil pengujian ESP32-CAM sebagai *face recognition*, sebagai berikut:

Berdasarkan hasil evaluasi, sistem menunjukkan presisi 100%, berarti tidak ada orang asing (False Positive) yang bisa masuk. Sistem tidak pernah salah mengenali wajah orang lain sebagai wajah yang dikenali.

Sedangkan untuk recall 80% artinya ketika wajah yang dikenali mungkin akan sering mengalami momen di mana kunci pintu tidak terbuka meskipun wajah sudah di depan kamera. Wajah harus menyesuaikan posisi, pencahayaan, atau mencoba ulang agar sistem berhasil mengenali.

F1-Score 88,9% memberi tahu bahwa secara keseluruhan, sistem berada di level "Sangat Baik". Nilai ini menunjukkan bahwa sistem mampu menjaga keamanan dengan sangat ketat (Presisi) tanpa terlalu banyak mengorbankan kenyamanan pengguna (Recall).

Hasil pengujian menunjukkan bahwa sistem mampu mengenali pengguna yang terdaftar dan menolak pengguna yang tidak terdaftar pada jarak 50–75 cm dengan latency rata-rata 1,8 detik, yang ditandai dengan nilai True Positive dan True Negative tanpa adanya False Positive. Hal ini membuktikan bahwa tujuan penelitian dalam aspek keamanan akses pintu telah tercapai, karena sistem tidak memberikan akses kepada pengguna yang tidak sah. Meskipun pada jarak 85 cm dan 100 cm sistem tidak mampu mendeteksi wajah, keterbatasan ini tidak menghilangkan capaian tujuan penelitian, melainkan menunjukkan adanya batasan jarak operasional sistem.

3.2 Hasil Pengujian dan Analisis Kontrol dengan Aplikasi Blynk (Kamera 2)

Tabel 2. Hasil Pengujian Kontrol dengan Aplikasi Blynk (Kamera2)

Sesi	No	Perintah dari Blynk	Status Tamu	Status Relay	Status Solenoid	Latency (detik)	Hasil (Sukses/Gagal)
1	1	Take photo	Dikenali	OFF	Locked	30	Sukses
	2	Unlocked	Dikenali	ON	Unlocked	2,4	Sukses
	3	Locked	Dikenali	OFF	Locked	2	Sukses
2	4	Take photo	Dikenali	OFF	Locked	17	Sukses
	5	Unlocked	Dikenali	ON	Unlocked	1,3	Sukses
	6	Locked	Dikenali	OFF	Locked	1,4	Sukses
3	7	Take Photo	Tidak dikenali	OFF	Locked	19	Sukses
4	8	Take Photo	-	OFF	Locked	>60	Gagal
5	9	Take photo	Dikenali	OFF	Locked	31,3	Sukses
	10	Unlocked	Dikenali	ON	Unlocked	4	Sukses
	11	Locked	Dikenali	OFF	Locked	3,3	Sukses
6	12	Take photo	-	OFF	Locked	>60	Gagal
7	13	Take photo	Tidak dikenali	OFF	Locked	17,7	Sukses
8	14	Take photo	Dikenali	OFF	Locked	21,2	Sukses
	15	Unlocked	Dikenali	ON	Unlocked	1	Sukses
	16	Locked	Dikenali	OFF	Locked	1,2	Sukses
9	17	Take photo	Dikenali	OFF	Locked	29	Sukses
	18	Unlocked	Dikenali	ON	Unlocked	1	Sukses
	19	Locked	Dikenali	OFF	Locked	1	Sukses
10	20	Take photo	-	OFF	Locked	>60	Gagal

Berikut ini perhitungan Latency berdasarkan tabel :

Latency take photo $= \frac{jumlah\ Latency\ take\ photo}{jumlah\ percobaan\ yang\ terdeteksi} = \frac{165,2}{7} =$ 23,6 detik

Latency unlocked $= \frac{jumlah\ Latency\ unlocked}{jumlah\ percobaan\ yang\ terdeteksi} = \frac{9,7}{5} =$ 1,9 detik

Latency locked $= \frac{jumlah\ Latency\ locked}{jumlah\ percobaan\ yang\ terdeteksi} = \frac{8,9}{5} =$ 1,8 detik

Berikut ini perhitungan Akurasi kesuksessan sistem menjalankan perintah dari Blynk berdasarkan tabel :

Akurasi $= \frac{Hasil\ sukses}{Jumlah\ percobaan} x100\ \% = \frac{17}{20}\ x\ 100\ \% = 85\ \%$

Analisa hasil pengujian Blynk sebagai akses kontrol jarak jauh, sebagai berikut:

3.3 Analisis Latency Sistem

Latency take photo selama 23,6 detik termasuk waktu yang lama untuk menunggu pintu terbuka. Ini adalah hambatan utama (*bottleneck*) sistem. Kemungkinan besar ukuran file foto terlalu besar atau kecepatan *upload* perangkat (seperti ESP32-CAM) ke

server Blynk sangat lambat. Pengguna jarak jauh akan mengalami "lag" yang parah. Saat foto muncul di *smartphone*, orang yang berdiri di depan pintu mungkin sudah pergi karena merasa sistem tidak bekerja. Namun bisa diatasi jika orang yang berdiri itu video call dengan pemegang aplikasi Blynk tanpa harus menggunakan fitur take photo.
Sedangkan latency unlocked selama 1,9 detik dan locked 1,8 detik tergolong baik. Setelah perintah "Unlocked" atau "Locked" dikirim dari Blynk, respon aktuator (selenoid) tergolong cepat. Jeda di bawah 2 detik masih sangat bisa diterima untuk kontrol jarak jauh.

3.4 Analisis Akurasi Kesuksesan Sistem dalam Menjalankan Perintah Blynk

Berdasarkan perhitungan akurasi, sistem berhasil menjalankan 17 dari 20 percobaan, sehingga diperoleh nilai akurasi sebesar 85%. Nilai ini menunjukkan bahwa mayoritas perintah yang dikirimkan melalui aplikasi Blynk dapat diterima dan dieksekusi dengan baik oleh sistem kunci pintu.

4. KESIMPULAN

Sistem akses pintu gerbang sekolah berhasil dibangun dengan mengintegrasikan teknologi *face recognition* menggunakan metode MTCNN dan Internet of Things (IoT) sebagai media kontrol dan monitoring dalam kondisi pencahayaan normal dan posisi wajah depan. Sistem ini pun dapat membedakan wajah yang terdaftar dan tidak terdaftar, di mana wajah yang dikenali akan mengaktifkan relay dan solenoid untuk membuka gerbang, sedangkan wajah yang tidak dikenali tidak diberikan akses. Sehingga, penerapan sistem ini dapat meningkatkan keamanan, efisiensi, dan otomatisasi akses pintu gerbang sekolah dibandingkan dengan sistem konvensional.

5. DAFTAR PUSTAKA

Helmud, E. *et al.* (2024) “Classification Comparison Performance of Supervised Machine Learning Random Forest and Decision Tree Algorithms Using Confusion Matrix,” *Jurnal Sisfokom (Sistem Informasi dan Komputer)*, 13(1), pp. 92–97. Available at: https://doi.org/10.32736/sisfokom.v13i1.1985.

Sayyidah Khalillah, T. *et al*. (2025) "Studi Literatur: Peran Manajemen Sekuriti di Lingkungan Pendidikan Sebagai Perlindungan Siswa,” *Triwikrama: Jurnal Multidisiplin Ilmu Sosial*, Volume 6, Number 9. Available at: https://repository.ubharajaya.ac.id/32793/1/Peran%20manajemen%20sekuriti%20dilingkungan%20pendidikan%20sebagai%20perlindungan%20siswa.pdf (Accessed: November 22, 2025).

Zulfikar, R. *et al.* (2023) “Rancang Bangun Keamanan Pintu Otomatis Menggunakan Face Recognition Berbasis Internet Of Things (IoT),” *JTEIN: Jurnal Teknik Elektro Indonesia*, 4(2), pp. 445–453. Available at: https://doi.org/10.24036/jtein.v4i2.385.