

Arsitektur Dual-Control Smart Home Berbasis ESP32 dengan Failover Cloud-Lokal dan Autentikasi Wajah

Tomy Satria Alasi¹⁾, Allwine²⁾, Mutiara S. Simanjuntak³⁾

¹⁾Program Studi Sistem Informasi, STMIK Methodist Binjai, Indonesia

²⁾Program Studi Ilmu Komputer, Universitas Lampung, Indonesia

³⁾Departemen Teknik Elektro dan Komputer,

National Kaohsiung University of Science and Technology, Taiwan

^{1,2,3)}Asosiasi Informatika Sumatera Utara, Indonesia

tomysatriaalasi@live.com; allwine@fmipa.unila.ac.id; i110154114@n kust.edu.tw;

Abstrak

Ketergantungan penuh pada layanan cloud menurunkan ketersediaan smart home ketika koneksi Internet terganggu, sementara kontrol suara tanpa autentikasi membuka peluang eksekusi perintah oleh pengguna yang tidak berwenang. Penelitian ini merancang dan mengevaluasi prototipe smart home berbiaya rendah yang membagi kendali ke dua jalur: jalur online melalui aplikasi Flutter dan Firebase Realtime Database serta jalur lokal melalui aturan sensor, voice assistant Vosk, dan autentikasi wajah. ESP32 memproses sensor HC-SR04, LDR, sensor hujan, dan DHT11; mengendalikan servo pagar, servo jemuran, lampu melalui relay, serta menampilkan status pada LCD. ESP32-CAM dan pustaka *face_recognition* memverifikasi identitas sebelum sistem menerima perintah suara. Penelitian menggunakan metode prototipe selama tiga bulan dengan inti pengembangan sepuluh minggu. Pengujian mencakup 38 skenario fungsional: 18 skenario keputusan sensor, lima pembacaan suhu, tujuh perintah suara, dua skenario autentikasi wajah, dan enam fungsi aplikasi-cloud. Seluruh skenario menghasilkan keluaran sesuai aturan yang ditetapkan (38/38 atau 100% keberhasilan fungsional). Pagar terbuka pada jarak 3–6 cm dan tertutup pada 8–15 cm dengan ambang 7 cm. Lampu aktif mulai nilai LDR 2400 dengan ambang 2350, sedangkan jemuran masuk sampai nilai sensor hujan 3400 dan keluar mulai 3600 dengan ambang 3500. Pembacaan DHT11 menghasilkan rata-rata 29,8 °C, simpangan baku sampel 0,84 °C, dan rentang 2 °C. Jalur online menunjukkan waktu respons observasional 1–2 detik. Kebaruan penelitian terletak pada integrasi kontrol cloud, kontrol lokal berbasis sensor dan suara, serta autentikasi wajah berurutan dalam satu prototipe ESP32. Hasil membuktikan kelayakan fungsi, tetapi belum membuktikan akurasi sensor terkalibrasi, word error rate, false acceptance rate, ketahanan jaringan, atau keamanan produksi.

Kata Kunci: Smart Home; Esp32; Kontrol Online–Offline; Vosk; Pengenalan Wajah; Firebase

I. PENDAHULUAN

Smart home menggabungkan sensor, aktuator, jaringan, perangkat lunak, dan layanan data. Integrasi tersebut meningkatkan kenyamanan. Namun, integrasi juga menambah ketergantungan pada konektivitas dan mekanisme autentikasi. Ketika seluruh keputusan ditempatkan di cloud, gangguan Internet dapat menghentikan fungsi yang sebenarnya dapat diproses secara lokal. Edge dan fog computing menawarkan pemrosesan yang lebih dekat dengan sumber data. Pendekatan ini dapat menurunkan latensi, mengurangi trafik, dan menjaga layanan yang membutuhkan respons cepat [1], [2].

Kebutuhan pemrosesan lokal juga muncul pada antarmuka suara. Gondi dan Pratap menunjukkan bahwa pengenalan suara luring dapat dijalankan pada perangkat edge [3]. Zhu et al. menggabungkan jaringan sensor nirkabel dengan pengenalan suara pada lingkungan smart home [4]. Wang et al. menguji kontrol suara pada 50 partisipan dengan 100 perintah per partisipan [5]. Penelitian tersebut menegaskan manfaat kontrol suara. Namun, keberhasilan pengenalan tetap dipengaruhi oleh perangkat, kosakata, kebisingan, aksen, dan jarak mikrofon.

Kemudahan kontrol suara tidak otomatis menjamin keamanan. Perintah yang membuka pagar atau mengaktifkan perangkat harus dibatasi kepada pengguna yang sah. Xie et al. membahas perlindungan privasi data wajah pada arsitektur edge [6]. Tok et al. menggabungkan pengenalan wajah dan one-time password untuk autentikasi smart home [7]. Ma et al. serta Uppuluri dan Lakshmeeswari menempatkan autentikasi perangkat, autentikasi pengguna, dan kesepakatan kunci sebagai bagian penting komunikasi smart home [8], [9]. Kajian keamanan juga menunjukkan risiko pada firmware, kredensial, protokol, dan konektivitas perangkat berbiaya rendah [10], [11].

Penelitian terdahulu umumnya mengoptimalkan satu fungsi. Sebagian berfokus pada pemrosesan edge, kontrol suara, autentikasi biometrik, atau keamanan komunikasi. Sebagian lain menekankan konektivitas, konfigurasi aplikasi, manajemen energi, atau deteksi intrusi [12], [13], [14], [15]. Kesenjangan utama terletak pada belum adanya pengujian terpadu atas jalur cloud dan jalur lokal pada satu prototipe ESP32 berbiaya rendah. Kesenjangan tersebut mencakup keberlanjutan fungsi saat cloud tidak tersedia dan pembatasan eksekusi perintah suara berdasarkan verifikasi wajah.

Kebaruan penelitian ini bukan sekadar integrasi beberapa teknologi. Kebaruan dirumuskan sebagai mekanisme dual-control dengan redundansi jalur kendali dan kemampuan failover antara cloud dan kontrol lokal. Jalur cloud menyediakan jangkauan kendali jarak jauh. Jalur lokal mempertahankan otomatisasi sensor dan perintah suara tanpa ketergantungan pada Firebase. Failover pada prototipe berarti fungsi lokal tetap tersedia ketika jalur cloud tidak digunakan atau tidak dapat dijangkau. Failover tidak berarti redundansi perangkat keras penuh, replikasi status tanpa jeda, atau high availability tingkat produksi.

Mekanisme tersebut dievaluasi melalui empat bukti. Pertama, kondisi online normal diuji melalui enam fungsi Flutter–Firebase. Kedua, gangguan jalur cloud direpresentasikan dengan pengoperasian mode lokal tanpa akses ke layanan Internet. Ketiga, keberhasilan perintah dinilai pada aturan sensor, perintah suara, autentikasi wajah, dan kontrol aplikasi. Keempat, latensi jalur online diamati dari pengiriman perintah hingga respons aktuator. Data yang tersedia mendukung kelayakan fungsional. Data belum cukup untuk mengestimasi availability, waktu pemulihan otomatis, atau distribusi latensi.

Kontribusi penelitian mencakup tiga aspek. Pertama, penelitian merumuskan pembagian tugas cloud-lokal yang dapat dipetakan dan diuji. Kedua, penelitian menerapkan urutan wake word, verifikasi wajah, klasifikasi perintah, dan eksekusi aktuator. Ketiga, penelitian menyajikan evaluasi fungsional yang memisahkan keberhasilan skenario dari akurasi, reliabilitas, dan keamanan produksi. Penelitian bertujuan merancang, menerapkan, serta mengevaluasi prototipe tersebut secara proporsional terhadap data uji yang tersedia.

II. TINJAUAN PUSTAKA

2.1. Pembagian Pemrosesan Cloud dan Lokal

Cloud memudahkan akses jarak jauh, sinkronisasi, dan pengelolaan data. Namun, cloud

menambah ketergantungan pada Internet, layanan pihak ketiga, dan waktu perjalanan data. Pemrosesan lokal memindahkan keputusan yang sensitif terhadap waktu atau privasi ke perangkat yang dekat dengan sumber data [1], [2]. Dalam penelitian ini, jalur cloud menangani monitoring dan kendali jarak jauh. Jalur lokal menangani aturan sensor, pengenalan suara, dan verifikasi wajah. Kontrol lokal tetap menggunakan Wi-Fi lokal untuk komunikasi komputer–ESP32. Istilah offline berarti tanpa akses Internet atau Firebase, bukan tanpa jaringan lokal.

2.2. Voice Assistant dan Autentikasi Wajah

Vosk menjalankan pengenalan suara secara lokal. Model luring mengurangi pengiriman audio ke cloud dan menjaga fungsi ketika Internet tidak tersedia [3]. Sistem menggunakan wake word “Halo Jarvis” untuk membuka sesi. Wake word tidak langsung mengaktifkan aktuator. Deteksi tersebut memicu pengambilan citra melalui ESP32-CAM. Sistem Python kemudian membandingkan wajah dengan data terdaftar. Perintah suara hanya diteruskan ke ESP32 apabila hasil verifikasi menyatakan pengguna sah.

Urutan tersebut menerapkan kontrol akses sebelum aksi fisik. Urutan ini lebih aman daripada perintah suara tanpa verifikasi. Namun, autentikasi biometrik tetap membawa risiko privasi, spoofing, dan kesalahan klasifikasi [6], [7]. Sistem produksi harus menambahkan perlindungan data biometrik, liveness detection, faktor kedua, pengelolaan kredensial, dan audit akses.

2.3. Perbandingan State of the Art

Tabel 1 membandingkan delapan penelitian terdahulu dalam daftar pustaka. Penilaian didasarkan pada fitur yang secara eksplisit menjadi bagian implementasi atau evaluasi masing-masing studi. Kode TD berarti tidak dilaporkan sebagai fokus penelitian. Kode T berarti tersedia secara terbatas.

Tabel 1. Perbandingan state of the art mekanisme kontrol dan keamanan

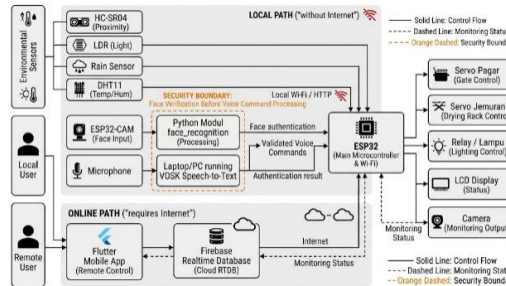
Penelitian	Cloud control	Offline/ local control	Voice assistant	Face authentication	Sensor automation	Failover mechanism	Latency	Security evaluation
Gondi & Pratap [3]	Tidak	Ya	Ya	Tidak	Tidak	Tidak	Ya	Tidak
Zhu et al. [4]	TD	TD	Ya	Tidak	Ya	Tidak	TD	Tidak
Wang et al. [5]	Tidak	T	Ya	Tidak	Tidak	Tidak	TD	Tidak
Xie et al. [6]	Tidak	Tidak	Tidak	Ya	Tidak	Tidak	T	Ya
Tok et al. [7]	Tidak	Tidak	Tidak	Ya	Tidak	Tidak	TD	Ya
Ma et al. [8]	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	T	Ya
Uppuluri & Lakshmeeswari [9]	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	T	Ya
Javed et al. [15]	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	T	Ya
Penelitian ini	Ya	Ya	Ya	Ya	Ya	Ya	T	T

Tabel 1 menunjukkan bahwa penelitian keamanan [6]–[9], [15] menyediakan evaluasi keamanan, tetapi tidak mengintegrasikannya dengan failover cloud-lokal, voice assistant, otomatisasi sensor, dan kendali aktuatur pada satu prototipe. Penelitian kontrol suara [3]–[5] juga tidak menawarkan perpindahan jalur cloud-lokal yang diuji bersama autentikasi. Dengan demikian, perbedaan penelitian ini terletak pada kombinasi failover fungsional dan evaluasi keamanan terpadu. Evaluasi keamanan pada penelitian ini masih terbatas pada gerbang autentikasi wajah dan penolakan pengguna yang tidak terdaftar.

III. METODE PENELITIAN

3.1. Desain Penelitian

Penelitian menggunakan metode prototipe. Metode ini dipilih karena perangkat keras, logika kendali, aplikasi, dan antarmuka suara harus disempurnakan secara iteratif. Kegiatan inti berlangsung selama sepuluh minggu dalam rentang penelitian sekitar tiga bulan. Tahapan penelitian mencakup identifikasi kebutuhan, perancangan, pembangunan prototipe, iterasi penyempurnaan, dan pengujian fungsional. Unit analisis adalah skenario fungsi pada prototipe, bukan pengguna atau rumah sebenarnya.

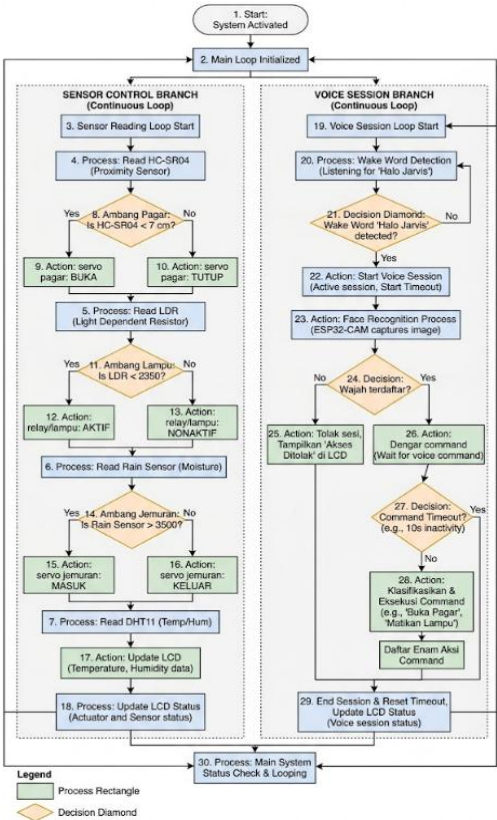


Gambar 1. Arsitektur dual-control dan batas keamanan sistem

3.2. Arsitektur Dual-Control

Arsitektur memiliki dua jalur kendali. Pada jalur online, aplikasi Flutter menulis perintah ke Firebase Realtime Database. ESP32 membaca perubahan data, mengaktifkan aktuatur, lalu mengirimkan status dan data sensor. Aplikasi menggunakan data tersebut untuk monitoring jarak jauh. ESP32-CAM menyediakan fungsi pengambilan gambar yang ditampilkan pada aplikasi. Pada jalur offline, ESP32 membaca HC-SR04, LDR, DHT11, dan sensor hujan. Keputusan dihasilkan oleh aturan ambang. Jalur ini tidak memerlukan Firebase. Voice assistant juga berjalan lokal pada komputer. Vosk mengubah suara menjadi frasa perintah. Komputer dan ESP32 berkomunikasi melalui Wi-Fi lokal. Failover bekerja pada tingkat jalur layanan. Ketika jalur cloud tersedia, pengguna dapat memilih kontrol jarak jauh. Ketika akses Internet atau Firebase tidak tersedia, loop sensor pada ESP32 tetap berjalan. Perintah suara juga tetap tersedia selama

komputer dan ESP32 berada pada jaringan lokal yang sama. Mekanisme ini tidak memindahkan sesi cloud secara otomatis dan tidak menjamin sinkronisasi status tanpa kehilangan data.



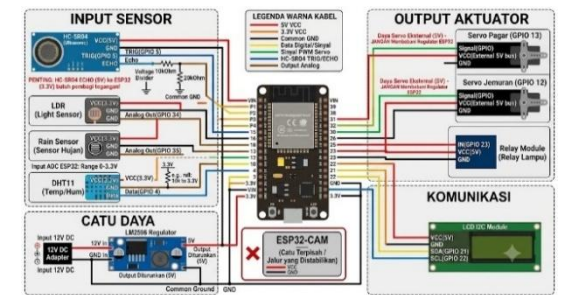
Gambar 2. Alur keputusan online, offline, dan perpindahan jalur kendali

3.3. Perangkat dan Logika Kendali

Tabel 2. Komponen utama sistem

Komponen	Fungsi
ESP32	Pusat kontrol, pembacaan sensor, komunikasi Wi-Fi, dan aktuasi.
ESP32-CAM	Akuisisi citra untuk monitoring dan verifikasi wajah.
HC-SR04	Deteksi jarak objek di depan pagar; ambang 7 cm.
LDR	Nilai ADC relatif untuk kendali lampu; ambang 2350.
Sensor hujan	Nilai ADC untuk kendali jemuran; ambang 3500.
DHT11	Pembacaan suhu lingkungan prototipe.
Flutter dan Firebase	Monitoring, sinkronisasi status, dan kendali jarak jauh.
Vosk dan Python	Pengenalan suara luring dan verifikasi wajah.

Aturan pagar: pagar terbuka jika $d < 7$ cm dan tertutup jika $d \geq 7$ cm. Variabel d adalah jarak yang dibaca HC-SR04. Aturan lampu: lampu hidup jika nilai LDR ≥ 2350 dan mati jika nilai LDR < 2350 . Nilai tersebut merupakan ADC relatif. Aturan jemuran: jemuran masuk jika $R < 3500$ dan keluar jika $R \geq 3500$. Variabel R adalah nilai ADC sensor hujan.



Gambar 3. Skema perangkat keras dan pemetaan koneksi

3.4. Prosedur Voice Assistant dan Autentikasi

Mikrofon merekam ucapan pengguna. Vosk memantau wake word “Halo Jarvis”. Ketika wake word terdeteksi, sistem Python meminta citra dari ESP32-CAM. Pustaka face_recognition membandingkan representasi wajah dengan data yang telah didaftarkan. Jika wajah terverifikasi, sistem membuka sesi perintah. Perintah yang tersedia adalah membuka atau menutup pagar, menghidupkan atau mematikan lampu, serta mengeluarkan atau memasukkan jemuran. Jika wajah tidak terverifikasi, sesi ditolak dan tidak ada perintah yang dikirim ke ESP32.

3.5. Skenario Pengujian

Tabel 3. Matriks pengujian fungsional

Modul	n	Input/kondisi	Kriteria
HC-SR04–pagar	6	3, 5, 6, 8, 10, 15 cm	Keluaran sesuai ambang 7 cm
LDR–lampu	6	ADC 1200–2800	Keluaran sesuai ambang 2350
Sensor hujan–jemuran	6	ADC 2500–4095	Keluaran sesuai ambang 3500
DHT11	5	Pembacaan 29–31 °C	Nilai terbaca dan dapat diringkas
Voice assistant	7	Wake word + enam perintah	Frasa dikenali dan aksi sesuai
Autentikasi wajah	2	Terdaftar/tidak terdaftar	Izin diberikan/ditolak
Flutter–Firebase	6	Monitoring dan kontrol	Fungsi online berjalan

Jumlah 38 menunjukkan cakupan skenario. Nilai tersebut bukan jumlah pengulangan independen untuk estimasi akurasi. Pengujian kondisi normal dilakukan saat Flutter, Firebase, Internet, dan ESP32 terhubung. Pengujian gangguan koneksi direpresentasikan dengan pengoperasian fungsi lokal tanpa menggunakan Firebase. Latensi online diamati secara langsung. Timestamp mentah, jitter, packet loss, dan waktu pemulihan failover belum direkam.

3.6. Analisis Data

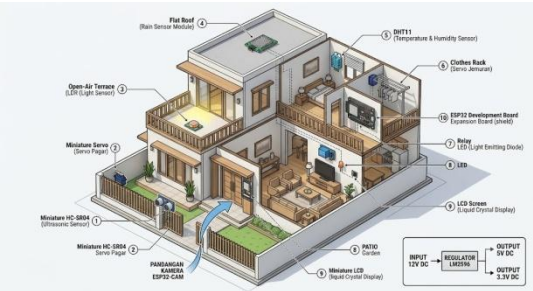
Analisis menggunakan statistik deskriptif dan pemeriksaan konsistensi aturan. Setiap skenario dinilai lulus apabila keluarannya sesuai dengan kondisi yang telah ditetapkan. Data suhu diringkas dengan rata-rata, median, minimum, maksimum, rentang, simpangan baku sampel, dan koefisien variasi. Untuk sensor berbasis ambang, analisis juga memeriksa margin titik uji terdekat terhadap ambang.

Penelitian tidak menghitung akurasi, Word Error Rate, False Acceptance Rate, False Rejection Rate, confidence interval, packet loss, atau distribusi latensi karena data mentah yang diperlukan belum tersedia.

IV. HASIL DAN PEMBAHASAN

4.1. Implementasi Prototype

Prototype berupa miniatur rumah dua lantai. Sistem mengintegrasikan ESP32, ESP32-CAM, sensor, servo, relay/LED, LCD, aplikasi Flutter, Firebase, Vosk, dan face_recognition. LCD menampilkan status lokal. Aplikasi menampilkan nilai sensor, status perangkat, tombol kontrol, perubahan mode, dan fungsi kamera. Sistem menyediakan otomatisasi sensor, perintah suara lokal, dan kendali aplikasi jarak jauh.



Gambar 4. Implementasi prototype smart home



Gambar 5. Antarmuka aplikasi Flutter

4.2. Pengujian Dual-Control dan Failover

Tabel 4. Hasil pengujian jalur kendali dan failover

Kondisi	Jalur yang tersedia	Temuan	Latensi/pemulihan
Online normal	Flutter–Firebase–ESP32 tersedia	6 fungsi online sesuai rancangan	1–2 detik; observasional
Gangguan jalur cloud	Firebase tidak digunakan; mode lokal aktif	18 keputusan sensor, 5 pembacaan suhu, 7 frasa, dan 2 kondisi wajah sesuai rancangan	Tidak direkam
Pemulihan jalur cloud	Koneksi kembali tersedia	Dapat kembali ke mode online	Waktu pemulihan belum diuji

Pada kondisi online normal, aplikasi menulis perintah ke Firebase. ESP32 membaca perubahan, mengaktifkan aktuator, dan memperbarui status. Enam fungsi online menghasilkan keluaran sesuai rancangan. Waktu respons diamati sekitar 1–2 detik. Rentang ini belum dapat dianggap sebagai distribusi

latensi karena jumlah pengulangan dan timestamp mentah tidak tersedia.

Pada kondisi gangguan jalur cloud, sistem beroperasi melalui jalur lokal. Otomatisasi sensor tetap diproses oleh ESP32. Voice assistant dan autentikasi wajah berjalan pada komputer lokal. Hasil menunjukkan bahwa fungsi lokal tidak memerlukan Firebase. Temuan ini membuktikan failover fungsional pada skenario prototipe. Temuan belum membuktikan failover otomatis tanpa jeda. Waktu deteksi gangguan, waktu perpindahan, kehilangan perintah, dan konsistensi status setelah pemulihan belum diukur

4.3. Hasil Otomatisasi Sensor

Tabel 5. Pengujian HC-SR04 dan pagar		
Jarak (cm)	Pagar	Margin dari 7 cm
3	Terbuka	4 cm di bawah
5	Terbuka	2 cm di bawah
6	Terbuka	1 cm di bawah
8	Tertutup	1 cm di atas
10	Tertutup	3 cm di atas
15	Tertutup	8 cm di atas

Enam titik menghasilkan kondisi pagar sesuai aturan. Titik 6 cm dan 8 cm berjarak 1 cm dari ambang. Data tersebut menunjukkan konsistensi logika pada titik yang diuji. Data belum mengukur repeatability, bias, atau ketidakpastian sensor. Titik 7 cm juga belum diuji secara langsung.

Tabel 6. Pengujian LDR dan lampu		
Nilai ADC	Lampu	Margin dari 2350
1200	Mati	1150 di bawah
1800	Mati	550 di bawah
2200	Mati	150 di bawah
2400	Hidup	50 di atas
2600	Hidup	250 di atas
2800	Hidup	450 di atas

Lampu mati pada nilai 2200 dan hidup pada nilai 2400. Margin terkecil adalah 50 count pada sisi hidup. Noise ADC yang mendekati margin tersebut dapat mengubah keputusan. Hysteresis dan moving average diperlukan untuk mengurangi osilasi. Nilai LDR belum dikalibrasi terhadap lux.

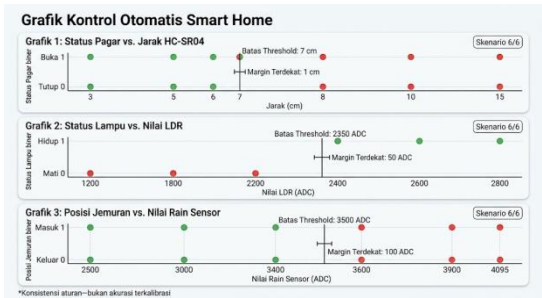
Tabel 7. Pengujian sensor hujan dan jemuran		
Nilai ADC	Kondisi	Jemuran
2500	Hujan	Masuk
3000	Hujan	Masuk
3400	Hujan	Masuk
3600	Tidak hujan	Keluar
3900	Tidak hujan	Keluar

Nilai ADC	Kondisi	Jemuran
4095	Tidak hujan	Keluar

Nilai 3400 menghasilkan posisi masuk. Nilai 3600 menghasilkan posisi keluar. Kedua titik berjarak 100 count dari ambang 3500. Sensor resistif dapat mengalami residu air, korosi, dan drift. Sistem nyata perlu menggunakan debounce, konfirmasi beberapa pembacaan, dan posisi aman ketika data ambigu.

Tabel 8. Statistik pembacaan DHT11	
Ukuran	Nilai
Jumlah data	5
Rata-rata	29,8 °C
Median	30 °C
Minimum–maksimum	29–31 °C
Simpangan baku sampel	0,84 °C
Koefisien variasi	2,81%

Lima pembacaan berada pada rentang 29–31 °C. Variasi dalam jendela pengamatan terbatas relatif kecil. Namun, data tidak disertai termometer referensi, waktu pengukuran, atau kondisi lingkungan. Hasil hanya menunjukkan bahwa DHT11 menghasilkan data yang dapat ditampilkan dan dipantau.



Gambar 6. Respons aktuator dan margin titik uji terhadap ambang

4.4. Hasil Voice Assistant dan Autentikasi Wajah

Tabel 9. Pengujian perintah suara		
Frasa	Aksi	Hasil
Halo Jarvis	Membuka sesi	Sesuai
Buka pagar	Pagar membuka	Sesuai
Tutup pagar	Pagar menutup	Sesuai
Hidupkan lampu	Lampu aktif	Sesuai
Matikan lampu	Lampu nonaktif	Sesuai
Keluarkan jemuran	Jemuran keluar	Sesuai
Masukkan jemuran	Jemuran masuk	Sesuai

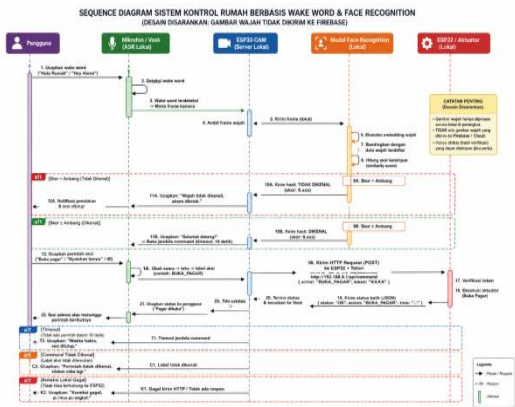
Vosk mengenali wake word dan enam perintah pada skenario uji. Sistem memberikan fungsionalitas yang konsisten pada skenario uji terbatas. Tujuh frasa tidak cukup untuk menyatakan akurasi pengenalan

suara. Pengujian belum mencakup variasi penutur, aksen, kebisingan, jarak mikrofon, atau kata yang mirip.

Tabel 10. Pengujian keamanan berbasis autentikasi wajah

Kondisi	Kebijakan	Hasil
Wajah terdaftar	Sesi perintah diizinkan	Diterima
Wajah tidak terdaftar	Sesi perintah ditolak	Ditolak

Deteksi wake word memicu verifikasi wajah. Sistem Python memberi token izin secara logis hanya ketika wajah cocok dengan data terdaftar. Perintah suara kemudian dipetakan ke aksi dan dikirim ke ESP32. Wajah yang tidak terdaftar menghasilkan penolakan. Pengujian ini menunjukkan kontrol akses fungsional. Dua kondisi belum cukup untuk mengukur False Acceptance Rate, False Rejection Rate, spoofing, replay, atau liveness.



Gambar 7. Urutan wake word, verifikasi wajah, dan eksekusi perintah

4.5. Evaluasi Keamanan Terpadu

Evaluasi keamanan menghubungkan identitas pengguna dengan keputusan aktuatur. Batas kepercayaan ditempatkan antara hasil pengenalan wajah dan pengiriman perintah. Pendekatan ini mencegah wake word menjadi satu-satunya syarat untuk mengaktifkan perangkat. Evaluasi juga memisahkan data sensor, status, kontrol, dan kamera pada struktur Firebase. Pemisahan tersebut membantu validasi dan audit. Namun, konfigurasi prototipe belum dapat dianggap aman untuk produksi.

Sistem produksi memerlukan identitas pengguna yang dapat diaudit, aturan Firebase berbasis peran, validasi nilai, App Check, TLS, rotasi kredensial, audit log, pembatasan laju perintah, dan penyimpanan biometrik yang terlindungi. Pengujian penetrasi, replay, spoofing, firmware tampering, dan denial-of-service juga diperlukan. Literatur menunjukkan bahwa autentikasi pengguna saja tidak menutup kelemahan perangkat dan jaringan [8]–[11], [15].

4.6. Pembahasan Kritis

Hasil mendukung pembagian fungsi cloud-lokal pada prototipe berbiaya rendah. Cloud menyediakan jangkauan kendali dan monitoring. Jalur lokal menyediakan kontinuitas untuk fungsi yang dapat diselesaikan tanpa cloud. Perpindahan ini mengurangi satu titik ketergantungan pada tingkat fungsi. Perpindahan belum menghilangkan ketergantungan pada catu daya, ESP32, komputer lokal, atau Wi-Fi lokal.

Perbandingan pada Tabel 1 menunjukkan posisi kontribusi. Studi suara [3]–[5] menilai pengenalan atau interaksi, tetapi tidak menguji failover bersama autentikasi wajah. Studi keamanan [6]–[9], [15] memperkuat privasi, autentikasi, atau deteksi intrusi, tetapi tidak menggabungkan jalur kontrol cloud-lokal dan otomatisasi sensor pada satu prototipe. Penelitian ini menyatukan dimensi tersebut. Klaim ini terbatas pada delapan penelitian pembanding dalam daftar pustaka.

Angka 38 dari 38 hanya menunjukkan bahwa setiap skenario menghasilkan keluaran yang diharapkan. Angka tersebut tidak menunjukkan akurasi populasi atau reliabilitas jangka panjang. Nilai ambang LDR dan sensor hujan masih berupa tuning prototipe. Latensi online masih berupa observasi rentang. Evaluasi suara dan wajah juga belum memiliki ukuran kesalahan. Oleh karena itu, hasil paling tepat dinyatakan sebagai konsistensi fungsi pada skenario uji terbatas.

4.7. Ancaman terhadap Validitas

Tabel 11. Ancaman terhadap validitas

Validitas	Ancaman
Internal	Posisi, tegangan, noise, dan urutan uji dapat memengaruhi sensor.
Konstruk	Status sesuai mengukur fungsi, bukan akurasi, reliabilitas, atau keamanan penuh.
Eksternal	Miniatur belum merepresentasikan beban, cuaca, dan interferensi rumah nyata.
Statistik	Titik uji sedikit dan belum memiliki pengulangan independen.
Keamanan	Belum ada penetration test, spoofing test, atau audit konfigurasi.

V. KESIMPULAN DAN SARAN

5.1. Kesimpulan

1. Penelitian menghasilkan prototipe smart home berbasis ESP32 dengan mekanisme dual-control. Jalur online menghubungkan Flutter, Firebase, dan ESP32. Jalur lokal menjalankan otomatisasi sensor serta voice assistant Vosk. Deteksi wake word memicu verifikasi wajah melalui ESP32-CAM dan sistem Python. Perintah suara hanya dieksekusi ketika wajah terverifikasi.
2. Kontribusi ilmiah terletak pada redundansi jalur kendali dan failover fungsional dari cloud ke

kontrol lokal. Enam fungsi online berjalan dengan respons observasional sekitar 1–2 detik. Ketika layanan cloud tidak digunakan, fungsi lokal tetap menghasilkan keluaran sesuai rancangan. Pengujian mencakup 18 keputusan sensor-aktuator, lima pembacaan suhu, tujuh frasa suara, dua kondisi autentikasi, dan enam fungsi aplikasi-cloud. Sistem memberikan fungsionalitas yang konsisten pada skenario uji terbatas.

- Hasil tidak dapat ditafsirkan sebagai bukti akurasi sensor, high availability, keamanan produksi, atau pengenalan biometrik yang tervalidasi. Pengujian belum mengukur waktu perpindahan failover, packet loss, distribusi latensi, Word Error Rate, False Acceptance Rate, dan False Rejection Rate. Dengan batas tersebut, prototipe layak digunakan sebagai dasar eksperimen lanjutan, bukan sebagai sistem siap instalasi.

5.2. Saran Penelitian Lanjutan

- Pengujian berikutnya wajib menggunakan minimal 30 pengulangan pada setiap titik pengukuran. Pengulangan perlu dipadatkan di sekitar threshold. Hasil perlu memuat rata-rata, simpangan baku, galat, repeatability, interval kepercayaan, dan tingkat keberhasilan.
- HC-SR04 perlu dibandingkan dengan penggaris atau laser distance meter. DHT11 perlu dibandingkan dengan termometer terkalibrasi. Sensor LDR wajib dikalibrasi menggunakan lux meter agar nilai ADC dapat dipetakan ke intensitas cahaya fisik.
- Sensor hujan wajib dikalibrasi berdasarkan intensitas atau volume air yang terukur. Prosedur harus mengendalikan durasi pembasahan, luas permukaan, waktu pengeringan, residu air, dan perubahan resistansi.
- Performa voice assistant harus diukur dengan Word Error Rate, Command Success Rate, False Activation Rate, False Rejection Rate, dan latensi end-to-end. Pengujian perlu mencakup beberapa penutur, variasi aksen, tingkat kebisingan, dan jarak mikrofon.
- Pengujian face recognition perlu melibatkan banyak identitas dan kondisi pencahayaan. Metrik wajib mencakup False Acceptance Rate dan False Rejection Rate. Pengujian juga perlu mencakup foto cetak, layar ponsel, video replay, masker, perubahan sudut, dan liveness detection.
- Failover perlu diuji dengan pemutusan Internet, ketidaktersediaan Firebase, putus Wi-Fi lokal, restart ESP32, packet loss, dan penurunan tegangan. Metrik harus mencakup detection time, switchover time, recovery time, lost command, availability, dan konsistensi status setelah koneksi pulih.
- Keamanan perlu diperkuat melalui autentikasi berlapis, aturan akses berbasis peran, TLS, App Check, validasi payload, rotasi kredensial, audit log, pembatasan laju, dan pengujian penetrasi. Data wajah dan embedding tidak boleh dikirim ke cloud tanpa kebutuhan serta perlindungan yang jelas.

Ketersediaan Artefak Pengujian

Demonstrasi prototipe dan pengujian tersedia sebagai materi tambahan pada <https://www.youtube.com/watch?v=1KdujqpxvGI>.

DAFTAR PUSTAKA

- [1] M. Laroui, B. Nour, H. Moun gla, M. A. Cherif, H. Afifi, and M. Guizani, 2021, *Edge And Fog Computing For Iot: A Survey On Current Research Activities & Future Directions*,” Computer Communications, vol. 180, pp. 210–231, DOI: 10.1016/j.comcom.2021.09.003
- [2] M. Ashouri, P. Davidsson, and R. Spalazzese, 2021, *Quality Attributes In Edge Computing For The Internet Of Things: A Systematic Mapping Study*, Internet of Things, vol. 13, art. 100346. DOI: 10.1016/j.iot.2020.100346
- [3] S. Gondi and V. Pratap, 2021, *Performance Evaluation of Offline Speech Recognition on Edge Devices*, Electronics, vol. 10, no. 21, art. 2697. DOI: 10.3390/electronics10212697
- [4] J. Zhu, D. Wang, and Y. Zhao, 2024, *Design Of Smart Home Environment Based On Wireless Sensor System And Artificial Speech Recognition*, Measurement: Sensors, vol. 33, art. 101090, 2024. DOI: 10.1016/j.measen.101090
- [5] S. C. Wang, W. K. Wong, and T. S. Min, 2022, *Voice Control Smart Home Electrical Appliances for Visually Impaired Person*, Journal of Engineering Technology and Applied Physics, vol. 4, no. 2, pp. 11–20, 2022. DOI: 10.33093/jetap..4.2.3
- [6] Y. Xie, P. Li, N. Nedjah, B. B. Gupta, D. Taniar, and J. Zhang, 2023, *Privacy Protection Framework For Face Recognition In Edge-Based Internet Of Things*, Cluster Computing, vol. 26, pp. 3017–3035, DOI: 10.1007/s10586-022-03808-8
- [7] Y. X. Tok, N. Katuk, and A. S. C. M. Arif, 2021, *Smart Home Multi-Factor Authentication Using Face Recognition and One-Time Password on Smartphone*, International Journal of Interactive Mobile Technologies, vol. 15, no. 24, pp. 32–48. DOI: 10.3991/ijim.v15i24.25393
- [8] Q. Ma, H. Tan, and T. Zhou, 2023, *Mutual Authentication Scheme For Smart Devices In Iot-Enabled Smart Home Systems*, Computer Standards & Interfaces, vol. 86, art. 103743, DOI: 10.1016/j.csi.2023.103743
- [9] S. Uppuluri and G. Lakshmeeswari, 2023, *Secure User Authentication And Key Agreement Scheme For Iot Device Access Control Based Smart Home Communications*, Wireless Networks, vol. 29, no. 3, pp. 1333–1354, 2023. DOI: 10.1007/s11276-022-03197-1

- [10] G. Vardakis, G. Hatzivasilis, E. Koutsaki, and N. Papadakis, 2024, *Review of Smart-Home Security Using the Internet of Things*, Electronics, vol. 13, no. 16, art. 3343, 2024. DOI: 10.3390/electronics13163343
- [11] K. Murat, D. Topyła, K. Zdulski, M. Marzęcki, J. Bieniasz, D. Paczesny, and K. Szczypiorski, 2024, *Security Analysis of Low-Budget IoT Smart Home Appliances Embedded Software and Connectivity*, Electronics, vol. 13, no. 12, art. 2371. DOI: 10.3390/electronics13122371
- [12] H. M. Youssef, R. A. Osman, and A. A. El-Bary, 2024, *Efficient Connectivity in Smart Homes: Enhancing Living Comfort through IoT Infrastructure*, Sensors, vol. 24, no. 9, art. 2761, 2024. DOI: 10.3390/s24092761
- [13] Y.-W. Lin, Y.-B. Lin, Y.-F. Wu, and P.-H. Shen, 2025, *VoiceTalk: A No-Code Approach for Creating Voice-Controlled Smart Home Applications*, IEEE Open Journal of the Computer Society, vol. 6, pp. 874–883, 2025. DOI: 10.1109/OJCS.2025.3576725
- [14] H.-C. Jo, H.-A. Park, S.-Y. Kwon, and K.-H. Cho, 2024, *Home Energy Management Systems (HEMSs) with Optimal Energy Management of Home Appliances Using IoT*, Energies, vol. 17, no. 12, art. 3009. DOI: 10.3390/en17123009
- [15] A. Javed, A. Ehtsham, M. Jawad, M. N. Awais, A.-u.-H. Qureshi, and H. Larijani, 2024, *Implementation of Lightweight Machine Learning-Based Intrusion Detection System on IoT Devices of Smart Homes*, Future Internet, vol. 16, no. 6, art. 200, 2024. DOI: 10.3390/fi16060200