

ANALISIS KINERJA SISTEM PROTEKSI AKSES BERBASIS *FINGERPRINT* PADA MESIN PENGISIAN BOTOL OTOMATIS BERBASIS *IOT*

Muhammad Sulthan Rizqullah¹, Iskandar Lutfi², Amperawan³

^{1,2,3} Politeknik Negeri Sriwijaya; Jl. Sriwijaya Negara Bukit Besar Palembang Sumatera Selatan 30139, Telp. +620711353414

Keywords:

Fingerprint;

IoT;

Proteksi akses;

AS608;

ESP32.

Correspondent Email:

msulthannr11@gmail.com

Abstrak-Mesin pengisian botol otomatis dapat diimplementasikan menggunakan teknologi *Internet of Things* (IoT) dan untuk menghindari penyalahgunaan mesin, diperlukan fitur perlindungan akses tambahan yang memastikan hanya operator yang ditetapkan yang memiliki kemampuan untuk bekerja dengan sistem ini. Karya ini mengevaluasi kinerja sistem perlindungan akses berbasis pengenalan sidik jari dengan menggunakan sensor *AS608*, yang diimplementasikan pada mikrokontroler *ESP32* dan menggunakan protokol *MQTT*. Sistem ini dievaluasi berdasarkan kriteria seperti *False Acceptance Rate* (FAR), *False Rejection Rate* (FRR), akurasi identifikasi, waktu respons, dan pemantauan secara *real-time*. Pengujian dilakukan terhadap 10 pengguna terdaftar dengan total 500 percobaan autentikasi. Hasil pengujian menunjukkan nilai *FAR* sebesar 0,4%, *FRR* sebesar 1,2%, akurasi identifikasi sebesar 98,4%, dan waktu respons rata-rata sebesar 1,34 detik. Hasil ini menunjukkan bahwa sistem dapat digunakan untuk melindungi akses ke mesin industri yang ringan.



Copyright © 2026 The Author(s), Published by Jurnal Informatika dan Teknik Elektro Terapan. This is an open-access article distributed under the terms of the Creative Commons Attribution-NonCommercial 4.0 International License (CC BY-NC 4.0).

Abstract-Automatic bottle filling machines can be implemented using *Internet of Things* (IoT) technology and to avoid misuse of the machine, additional access protection features are required that ensure only designated operators have the ability to work with this system. This work evaluates the performance of a fingerprint recognition-based access protection system using the *AS608* sensor, implemented on an *ESP32* microcontroller and using the *MQTT* protocol. The system is evaluated based on criteria such as *False Acceptance Rate* (FAR), *False Rejection Rate* (FRR), identification accuracy, response time, and *real-time* monitoring. Testing was conducted on 10 registered users with a total of 500 authentication attempts. The results showed a *FAR* of 0.4%, *FRR* of 1.2%, identification accuracy of 98.4%, and an average response time of 1.34 seconds., respectively. These results indicate that the system can be used to protect access to light industrial machines.

1. PENDAHULUAN

Perkembangan teknologi pada era Revolusi Industri 4.0 telah mendorong penerapan *Internet of Things* (IoT) dalam berbagai sektor industri, termasuk pada sistem otomasi manufaktur. Integrasi teknologi IoT memungkinkan mesin industri melakukan pemantauan, pengendalian, dan pertukaran data secara *real-time* sehingga meningkatkan efisiensi, produktivitas, dan keandalan proses produksi [1]. Salah satu implementasi otomasi yang banyak digunakan adalah mesin pengisian botol otomatis yang berperan penting dalam

industri minuman, farmasi, dan produk rumah tangga. Mesin ini dituntut memiliki tingkat keandalan dan keamanan yang tinggi karena kesalahan pengoperasian dapat menyebabkan kerusakan peralatan, penurunan kualitas produk, maupun risiko keselamatan kerja [2].

Seiring meningkatnya penggunaan sistem otomasi berbasis IoT, kebutuhan terhadap mekanisme proteksi akses menjadi semakin penting. Sistem keamanan konvensional seperti kata sandi, PIN, dan kartu akses memiliki berbagai keterbatasan, antara lain mudah dibagikan, hilang, atau disalahgunakan oleh

pihak yang tidak berwenang. Sebagai alternatif, teknologi biometrik berbasis sidik jari (*fingerprint*) menawarkan tingkat keamanan yang lebih baik karena memanfaatkan karakteristik biologis yang unik pada setiap individu [3]. Sensor *fingerprint* modern seperti *AS608* telah banyak digunakan pada sistem embedded karena memiliki kemampuan identifikasi yang baik, biaya yang relatif rendah, serta mudah diintegrasikan dengan mikrokontroler seperti *ESP32* [4].

Beberapa penelitian sebelumnya telah menerapkan teknologi *fingerprint* untuk sistem absensi, kontrol akses ruangan, maupun keamanan perangkat berbasis IoT [5], [7]. Penelitian tersebut menunjukkan bahwa penggunaan *fingerprint* mampu meningkatkan keamanan sistem dibandingkan metode autentikasi konvensional. Namun, sebagian besar penelitian masih berfokus pada perancangan dan implementasi sistem, sedangkan analisis kinerja berdasarkan parameter biometrik seperti *False Acceptance Rate* (FAR), *False Rejection Rate* (FRR), akurasi identifikasi, waktu respons, dan konsumsi daya belum dilakukan secara komprehensif. Selain itu, penerapan sistem proteksi akses *fingerprint* pada mesin pengisian botol otomatis berbasis *IoT* masih relatif terbatas.

Berdasarkan kondisi tersebut, penelitian ini bertujuan untuk menganalisis kinerja sistem proteksi akses berbasis *fingerprint* pada mesin pengisian botol otomatis menggunakan sensor *AS608* dan mikrokontroler *ESP32* yang terintegrasi dengan protokol *MQTT*. Evaluasi dilakukan melalui pengukuran *FAR*, *FRR*, akurasi identifikasi, waktu respons, konsumsi daya, serta kemampuan pemantauan data secara real-time. Penelitian ini berfokus pada analisis kinerja sistem proteksi akses berbasis *fingerprint* pada mesin pengisian botol otomatis berbasis IoT berdasarkan parameter FAR, FRR, akurasi identifikasi, waktu respons, dan konsumsi daya. Berdasarkan kondisi tersebut, penelitian ini bertujuan untuk menganalisis kinerja sistem proteksi akses berbasis *fingerprint* pada mesin pengisian botol otomatis menggunakan sensor *AS608* dan mikrokontroler *ESP32* yang terintegrasi dengan protokol *MQTT*. Evaluasi dilakukan melalui pengukuran *FAR*, *FRR*, akurasi identifikasi,

waktu respons, konsumsi daya, serta kemampuan pemantauan data secara real-time. Hasil penelitian diharapkan dapat memberikan informasi mengenai kinerja dan kelayakan penerapan sistem proteksi akses berbasis *fingerprint* pada lingkungan industri berbasis IoT..

2. TINJAUAN PUSTAKA

2.1 Sistem Biometrik *Fingerprint*

Biometrik merupakan teknologi identifikasi dan verifikasi individu berdasarkan karakteristik fisik atau perilaku yang unik. Salah satu metode biometrik yang paling banyak digunakan adalah sidik jari (*fingerprint*) karena memiliki tingkat keunikan yang tinggi, stabil sepanjang hidup, serta mudah diimplementasikan pada berbagai sistem keamanan [7]. Dibandingkan metode autentikasi konvensional seperti kata sandi dan kartu akses, *fingerprint* menawarkan tingkat keamanan yang lebih baik karena karakteristik biometriknya sulit dipalsukan atau dipindah tangankan kepada pihak lain [3].

Teknologi sensor *fingerprint* secara umum terdiri atas sensor optis, kapasitif, dan ultrasonik. Sensor optis bekerja dengan menangkap citra pola sidik jari menggunakan pantulan cahaya, sedangkan sensor kapasitif memanfaatkan perbedaan kapasitansi antara punggung dan lembah sidik jari. Sensor ultrasonik menggunakan gelombang suara untuk menghasilkan citra tiga dimensi permukaan sidik jari. Setiap teknologi memiliki kelebihan dan keterbatasan yang berbeda dalam hal akurasi, ketahanan terhadap kondisi lingkungan, serta biaya implementasi [8].

Pada penelitian ini digunakan sensor *fingerprint AS608* yang termasuk dalam kategori sensor optis. Sensor ini dipilih karena memiliki kemampuan penyimpanan template sidik jari, proses pencocokan yang cepat, serta kemudahan integrasi dengan mikrokontroler *ESP32* melalui komunikasi *UART*. Kinerja sistem *fingerprint* umumnya dievaluasi menggunakan parameter *False Acceptance Rate* (FAR), *False Rejection Rate* (FRR), akurasi identifikasi, dan waktu respons, yang menjadi fokus analisis pada penelitian ini.

2.2 Parameter Evaluasi Kinerja Biometrik

Parameter evaluasi kinerja sistem biometrik *fingerprint* secara standar telah didefinisikan

oleh berbagai lembaga internasional termasuk *National Institute of Standards and Technology* (NIST) dan *International Organization for Standardization* (ISO). Dua parameter paling fundamental adalah *False Acceptance Rate* (FAR) dan *False Rejection Rate* (FRR). FAR didefinisikan sebagai probabilitas sistem menerima individu yang tidak terdaftar atau tidak berwenang sebagai pengguna yang valid, sedangkan FRR didefinisikan sebagai probabilitas sistem menolak individu yang terdaftar dan berwenang sebagai pengguna yang tidak valid [7]. Kedua parameter ini memiliki hubungan trade-off yang inheren: peningkatan *threshold* keamanan (*security level*) akan menurunkan FAR namun meningkatkan FRR, dan sebaliknya. Titik keseimbangan di mana FAR dan FRR bernilai sama disebut *Equal Error Rate* (EER), yang merupakan metrik tunggal yang sering digunakan untuk membandingkan performa keseluruhan dua sistem biometrik yang berbeda [9]. Selain FAR dan FRR, parameter lain yang relevan mencakup waktu respons sistem (dari kontak jari hingga keluaran keputusan), kapasitas *template database* (jumlah maksimum pengguna yang dapat didaftarkan), tingkat *False Reject on First Attempt* (FROA) yang mengukur kemudahan penggunaan, serta *robustness* sistem terhadap variasi kondisi lingkungan seperti perubahan suhu, kelembapan, dan pencahayaan. Pemahaman menyeluruh terhadap parameter-parameter ini krusial untuk merancang sistem biometrik yang sesuai dengan kebutuhan spesifik suatu aplikasi, termasuk pada konteks kontrol akses mesin industri yang menjadi fokus penelitian ini.

2.3 Modul Sensor Sidik Jari AS608

Modul sensor sidik jari AS608 diproduksi oleh GROW Technology dan merupakan salah satu modul *fingerprint optis* paling populer dalam komunitas pengembang sistem *embedded* karena kombinasi harga terjangkau, kemampuan teknis yang memadai, dan dokumentasi yang relatif lengkap. Secara teknis, AS608 mengintegrasikan sensor *optis* resolusi tinggi, prosesor DSP (*Digital Signal Processor*) untuk pemrosesan citra, dan memori flash internal untuk penyimpanan hingga 300 *template* sidik jari [4]. Proses autentikasi berlangsung sepenuhnya di dalam modul

melalui dua tahap: pertama, akuisisi dan pemrosesan citra sidik jari untuk menghasilkan representasi fitur; kedua, pencocokan fitur tersebut dengan *template* yang tersimpan dalam *database* internal menggunakan algoritma proprietari. Modul berkomunikasi dengan mikrokontroler melalui protokol UART (*Universal Asynchronous Receiver-Transmitter*) menggunakan paket data berformat biner dengan kecepatan baud default 57600 bps. AS608 mendukung lima tingkat keamanan (*Security Level* 1-5) yang menentukan *threshold* skor kecocokan minimum untuk menerima autentikasi: *level* rendah lebih permisif namun berisiko FAR tinggi, *level* tinggi lebih ketat namun berisiko FRR tinggi. Untuk aplikasi kontrol akses industri, *Security Level* 3 umumnya direkomendasikan sebagai kompromi optimal antara keamanan dan kemudahan penggunaan. Modul ini juga mendukung dua mode operasi: mode verifikasi satu-ke-satu (1:1) yang mencocokkan citra baru dengan *template* spesifik berdasarkan ID yang diberikan, dan mode identifikasi satu-ke-banyak (1:N) yang mencocokkan citra baru dengan seluruh *template* dalam *database* secara otomatis.

2.4 ESP32 dan Platform IoT

Mikrokontroler ESP32 yang dikembangkan oleh Espressif Systems merupakan platform SoC (System on Chip) yang menggabungkan prosesor dual-core Xtensa LX6 berkecepatan hingga 240 MHz dengan modul Wi-Fi 802.11 b/g/n dan Bluetooth 4.2/BLE dalam satu chip yang terintegrasi [5]. Kemampuan komputasi yang memadai, konektivitas nirkabel terintegrasi, dan ekosistem pengembangan yang kaya menjadikan ESP32 pilihan dominan untuk implementasi sistem IoT tingkat menengah. Dalam konteks integrasi dengan AS608, ESP32 bertindak sebagai kontroler utama yang mengatur alur autentikasi, mengelola logika kontrol aktuator, dan menangani komunikasi data ke infrastruktur IoT. Antarmuka hardware UART pada ESP32 tersedia di beberapa pasang pin GPIO, memberikan fleksibilitas dalam desain PCB. Internet of Things (IoT) sebagai paradigma teknologi mengacu pada jaringan objek fisik yang dilengkapi sensor, perangkat lunak, dan konektivitas jaringan untuk memungkinkan pertukaran data dan interaksi dengan lingkungan digital secara otonom [10].

Dalam aplikasi keamanan industri, *platform IoT* memungkinkan pemantauan status akses secara *real-time* dari lokasi terpusat, analisis pola akses historis untuk deteksi anomali, serta integrasi dengan sistem manajemen produksi yang lebih besar. Protokol *MQTT* (*Message Queuing Telemetry Transport*) merupakan protokol komunikasi *publish-subscribe* berbasis *TCP/IP* yang dirancang khusus untuk perangkat dengan sumber daya terbatas dan jaringan bandwidth rendah, menjadikannya standar *de facto* untuk komunikasi data pada sistem *IoT edge* [11].

2.5 Penelitian Terkait

Beberapa penelitian terkait telah memberikan landasan yang relevan bagi penelitian ini. Raharjo et al. [12] mengimplementasikan sistem absensi karyawan berbasis *fingerprint* menggunakan NodeMCU *ESP8266* dan modul *R305* yang terhubung ke *server database MySQL* melalui jaringan lokal, melaporkan akurasi pengenalan 96,7% namun tidak menganalisis dampak kondisi lingkungan terhadap kinerja sistem. Abdurrohman et al. [13] mengembangkan sistem kontrol pintu otomatis berbasis *ESP32* dengan sensor *fingerprint* yang terintegrasi dengan notifikasi Telegram, memperoleh waktu respons rata-rata 1,8 detik namun tidak dilengkapi analisis konsumsi daya yang komprehensif. Yudhana et al. [14] menganalisis kinerja modul *fingerprint ZFM60* pada berbagai kondisi kelembapan relatif, menemukan degradasi akurasi yang signifikan (dari 97,2% pada *RH* 40% menjadi 89,4% pada *RH* 85%), yang menekankan pentingnya evaluasi lingkungan untuk aplikasi industri. Sementara itu, Setianingsih et al. [15] mengintegrasikan sistem biometrik *fingerprint* dengan *SCADA* untuk monitoring akses pada fasilitas produksi, namun implementasinya menggunakan sensor grade industri berbiaya tinggi yang tidak terjangkau untuk usaha kecil dan menengah. Perbedaan fundamental penelitian yang disajikan dalam makalah ini dari penelitian-penelitian di atas terletak pada: (1) konteks spesifik integrasi pada mesin pengisian botol otomatis; (2) analisis sistematis pengaruh dua kondisi lingkungan yang merepresentasikan kondisi industri nyata; (3) penggunaan komponen berbiaya rendah (*AS608* + *ESP32*) yang dikombinasikan dengan *platform IoT* berbasis *MQTT open-source*; serta

(4) evaluasi kelayakan teknis berdasarkan standar kinerja biometrik internasional.

3. METODE PENELITIAN

3.1 Rancangan Penelitian

Penelitian ini menggunakan metode eksperimen untuk mengukur dan menganalisis kinerja sistem proteksi akses berbasis *fingerprint*. Rancangan penelitian terdiri atas lima tahap utama yang dilaksanakan secara sekuensial. Tahap pertama adalah studi literatur dan analisis kebutuhan, di mana dilakukan kajian mendalam terhadap spesifikasi teknis komponen, standar evaluasi sistem biometrik, dan arsitektur sistem *IoT* yang relevan. Tahap kedua adalah perancangan sistem, yang mencakup perancangan skematik rangkaian elektronik, pemilihan komponen, dan desain arsitektur perangkat lunak. Tahap ketiga adalah implementasi, yaitu perakitan perangkat keras, penulisan *firmware mikrokontroler*, konfigurasi infrastruktur *IoT*, dan integrasi seluruh subsistem. Tahap keempat adalah pengujian dan pengumpulan data, yang dilaksanakan berdasarkan protokol pengujian yang telah dirancang sebelumnya dengan melibatkan 10 responden dalam dua sesi kondisi lingkungan yang berbeda. Tahap kelima adalah analisis data dan evaluasi, di mana data yang terkumpul diolah secara statistik dan hasil kinerja sistem dibandingkan dengan standar yang berlaku serta dengan hasil penelitian sejenis yang dipublikasikan sebelumnya. Penelitian dilaksanakan di Laboratorium Sistem Kendali dan Otomasi, yang dilengkapi dengan peralatan pengukuran terstandar termasuk osiloskop digital, multimeter presisi, dan sistem pengkondisi lingkungan untuk mensimulasikan kondisi industri.

3.2 Perancangan Perangkat Keras

Perangkat keras sistem terdiri atas beberapa komponen utama yang dipilih berdasarkan kebutuhan sistem dan kemudahan integrasi dengan perangkat yang digunakan. Komponen pertama adalah *mikrokontroler ESP32-DevKitC* versi 4 berbasis chip *ESP32-WROOM-32* sebagai unit pemrosesan pusat yang menjalankan logika sistem, mengelola komunikasi dengan modul *fingerprint*, mengontrol aktuator, dan menangani koneksi jaringan [5]. Komponen kedua adalah modul sensor sidik jari *optis AS608* yang bertugas melakukan akuisisi citra, ekstraksi fitur, dan

pencocokan *template* sidik jari secara otonom [4]. Komponen ketiga adalah relai elektromekanis 5V/10A yang berfungsi sebagai aktuator untuk menghubungkan atau memutuskan suplai daya ke mesin pengisian, dengan isolasi elektris antara sirkuit kontrol dan sirkuit daya mesin. Komponen keempat adalah modul catu daya switching 220V AC ke 5V DC/3A yang memastikan pasokan daya stabil untuk seluruh sistem. Komponen kelima adalah LED indikator tiga warna (merah, hijau, biru) yang memberikan umpan balik visual kepada operator tentang status autentikasi. Sensor *AS608* dihubungkan ke *ESP32* melalui antarmuka *UART2* pada pin *GPIO16* sebagai RX dan *GPIO17* sebagai TX, dengan level tegangan logika 3,3V yang kompatibel langsung. Relai dihubungkan melalui modul *driver* transistor untuk menghindari beban berlebih pada pin *GPIO ESP32* yang memiliki kapasitas arus terbatas sebesar 12 mA per pin.

3.3 Perancangan Perangkat Lunak

Firmware ESP32 dikembangkan menggunakan *Arduino Framework* dalam lingkungan pengembangan *Platform IO* pada *Visual Studio Code*, yang dipilih karena kemudahan pengelolaan dependensi *library* dan kemampuan *debugging* yang lebih baik dibandingkan *Arduino IDE* standar. Tiga *library* utama yang digunakan adalah: (1) *Adafruit Fingerprint Sensor Library* versi 2.0.7 untuk komunikasi protokol dengan modul *AS608*; (2) *PubSubClient* versi 2.8.0 untuk implementasi klien *MQTT*; dan (3) *WiFiClientSecure* bawaan *ESP32* untuk koneksi *TLS* opsional. Arsitektur *firmware* terdiri atas tiga modul fungsional utama yang dieksekusi dalam *loop* utama *mikrokontroler*. Modul pertama adalah *Fingerprint Authentication Manager* yang mengelola seluruh interaksi dengan sensor *AS608* mulai dari deteksi kehadiran jari, pemicu akuisisi citra, inisiasi pencocokan *template*, hingga interpretasi kode hasil. Modul kedua adalah *Actuator Control Module* yang menerima sinyal dari modul autentikasi dan mengontrol keluaran relai beserta indikator *LED* sesuai dengan logika keamanan yang telah diprogram, termasuk fitur *auto-lock* setelah durasi akses tertentu. Modul ketiga adalah *IoT Communication Handler* yang bertanggung jawab atas manajemen koneksi *Wi-Fi* dan

MQTT, serialisasi data kejadian autentikasi ke format *JSON*, serta publikasi data tersebut ke *broker MQTT*. Seluruh parameter sistem seperti *SSID Wi-Fi*, alamat *broker*, topik *MQTT*, dan durasi akses dikonfigurasi melalui file konfigurasi terpisah untuk memudahkan *deployment* dan pemeliharaan sistem di lapangan.

3.4 Infrastruktur IoT

Infrastruktur *IoT* yang dibangun untuk mendukung sistem ini terdiri atas *broker MQTT Mosquitto* versi 2.0 yang di-deploy pada layanan *cloud VPS* berbasis *Ubuntu Server 22.04*, *dashboard* pemantauan *real-time* menggunakan *Node-RED* versi 3.1 yang terhubung langsung ke *broker MQTT*, serta *database time-series InfluxDB* versi 2.7 untuk penyimpanan data log jangka panjang yang dapat diquery untuk analisis historis. Setiap kejadian autentikasi yang terjadi pada sistem diterbitkan (*publish*) oleh *ESP32* ke topik *MQTT* yang telah ditentukan dalam format *payload JSON* yang memuat: *timestamp* kejadian dalam format *ISO 8601*, identifikasi mesin (*machine ID*), identifikasi pengguna (*user ID*), hasil autentikasi (berhasil/gagal/*timeout*), nomor urut percobaan, dan tingkat skor pencocokan yang dikembalikan oleh modul *AS608*. *Node-RED* bertugas sebagai jembatan antara *broker MQTT* dan *InfluxDB*, sekaligus menghosting antarmuka *dashboard* visualisasi yang menampilkan statistik akses *real-time*. Fitur keamanan tambahan yang diimplementasikan meliputi: mekanisme *rate-limiting* yang memblokir percobaan autentikasi lebih dari 5 kali dalam 2 menit sebagai proteksi terhadap *brute-force*; alarm otomatis yang dikirimkan melalui *Telegram Bot API* apabila terdeteksi 3 kali autentikasi gagal berturut-turut; serta enkripsi *TLS* opsional untuk komunikasi *MQTT* pada *deployment* dengan kebutuhan keamanan lebih tinggi.

3.5 Protokol Pengujian

Protokol pengujian kinerja dirancang mengacu pada standar evaluasi sistem biometrik *NIST SP 500-290 (Fingerprint Vendor Technology Evaluation)* dan pedoman *ISO/IEC 19795-1:2021* yang mengatur metodologi pengujian biometrik. Sepuluh responden dengan komposisi yang beragam dalam hal jenis kelamin, rentang usia (22-45

tahun), dan tipe kulit direkrut setelah menandatangani formulir persetujuan (*informed consent*). Setiap responden menjalani proses *enrollmen* dengan mendaftarkan tiga *template* sidik jari per jari untuk meningkatkan kualitas referensi. Sesi pengujian terdiri atas dua kondisi: Kondisi A (Normal) dengan kelembapan relatif laboratorium 45-55% *RH*, suhu 23-26°C, dan jari dalam kondisi bersih dan kering; serta Kondisi B (Simulasi Industri) dengan kelembapan relatif 65-80% *RH* yang diatur menggunakan *humidifier*, simulasi getaran mekanis 8-12 Hz menggunakan *vibrator*, dan jari dalam kondisi sedikit lembap akibat paparan kelembapan udara. Setiap responden melakukan 25 percobaan autentikasi valid pada setiap kondisi, sehingga total percobaan adalah 10 responden $\times$ 25 percobaan $\times$ 2 kondisi = 500 percobaan. Parameter yang diukur dan dihitung meliputi *FAR* (percobaan diterima tidak sah / total percobaan), *FRR* (percobaan ditolak sah / total percobaan), akurasi keseluruhan ((total percobaan - total kesalahan) / total percobaan $\times$ 100%), rata-rata waktu respons per percobaan, dan konsumsi daya dalam kondisi *idle* serta aktif menggunakan *power meter* digital.

4. HASIL DAN PEMBAHASAN

4.1 Hasil Pengujian Akurasi dan Tingkat Kesalahan

Pengujian sistem dilaksanakan selama 14 hari kerja dengan mengikuti protokol yang telah ditetapkan, dan seluruh data dikumpulkan secara otomatis oleh sistem logging *IoT* yang dibangun. Dari total 500 percobaan autentikasi

valid yang dilakukan oleh 10 responden terdaftar, sistem mencatat 2 kejadian false rejection pada kondisi normal dan 6 kejadian false rejection pada kondisi simulasi industri. Untuk kejadian false acceptance, sistem tidak mencatat satupun kejadian pada kondisi normal, dan hanya 2 kejadian pada kondisi simulasi industri di mana jari yang lembap dari pengguna yang berbeda menghasilkan skor kecocokan yang melampaui *threshold* pada *Security Level* 3. Nilai *FAR* rata-rata keseluruhan dua kondisi adalah 0,4% dan *FRR* rata-rata adalah 1,2%, sehingga akurasi keseluruhan sistem mencapai 98,4%. Nilai *FAR* 0,4% berada jauh di bawah batas maksimum 1,0% yang ditetapkan oleh standar *NIST* untuk sistem biometrik kelas produksi [8], menunjukkan bahwa sistem memiliki tingkat keamanan yang baik berdasarkan hasil pengujian yang dilakukan.. Nilai *FRR* 1,2% juga berada di bawah batas 2,0% yang sama, mengindikasikan bahwa kemudahan penggunaan sistem (*usability*) terjaga pada *level* yang dapat diterima tanpa mengorbankan keamanan secara signifikan. Komparasi antara dua kondisi pengujian menunjukkan bahwa kondisi lingkungan industri (kelembapan tinggi dan getaran) memberikan dampak yang lebih signifikan terhadap *FRR* (naik dari 0,8% menjadi 1,6%) dibandingkan terhadap *FAR* (naik dari 0% menjadi 0,8%), yang mengindikasikan bahwa degradasi kualitas citra lebih berdampak pada kemampuan verifikasi pengguna terdaftar daripada pada *discriminability* terhadap pengguna tidak terdaftar.

Tabel 1. Rekapitulasi Hasil Pengujian Parameter Kinerja Sistem

Parameter Kinerja	Kondisi A (Normal)	Kondisi B (Industri)	Rata-rata Gabungan	Standar NIST
<i>False Acceptance Rate</i> / <i>FAR</i> (%)	0,0	0,8	0,4	< 1,0
<i>False Rejection Rate</i> / <i>FRR</i> (%)	0,8	1,6	1,2	< 2,0
Akurasi Keseluruhan (%)	99,2	97,6	98,4	> 95,0
Rata-rata Waktu Respons (detik)	1,21	1,47	1,34	< 3,0
Konsumsi Daya - <i>Idle</i> (<i>mW</i>)	185	185	185	-

Konsumsi Daya - Aktif Maks (mW)	412	412	412	-
-------------------------------------	-----	-----	-----	---

4.2 Analisis Waktu Respons Autentikasi

Hasil pengukuran waktu respons autentikasi menunjukkan karakteristik waktu respons sistem Berdasarkan hasil pengujian, waktu respons sistem masih berada pada rentang yang dapat diterima untuk aplikasi kontrol akses pada mesin pengisian botol otomatis. Seluruh nilai waktu respons yang diperoleh berada di bawah 3 detik sehingga tidak memberikan hambatan yang berarti terhadap proses operasional. Distribusi waktu respons pada kondisi ini mendekati distribusi normal dengan sedikit *skewness* ke kanan yang disebabkan oleh beberapa percobaan yang memerlukan proses akuisisi ulang karena posisi jari yang kurang optimal. Pada kondisi simulasi industri, waktu respons meningkat dengan rentang 0,93 detik hingga 2,31 detik, rata-rata 1,47 detik dengan standar deviasi 0,24 detik. Peningkatan rata-rata

waktu respons sebesar 0,26 detik (+21,5%) pada kondisi industri terutama disebabkan oleh penurunan kualitas kontras citra akibat kelembapan, yang mengakibatkan modul *AS608* memerlukan satu hingga dua kali proses akuisisi tambahan sebelum menghasilkan representasi fitur yang memenuhi *threshold* kualitas internal modul. Meski demikian, seluruh waktu respons yang terukur-bahkan pada kondisi paling tidak menguntungkan sekalipun-masih berada di bawah ambang 3 detik yang umumnya dianggap sebagai batas toleransi pengguna untuk sistem kontrol akses dalam konteks industri berdasarkan literatur ergonomi kerja [16]. Berdasarkan hasil pengujian, waktu respons sistem masih berada pada rentang yang dapat diterima untuk aplikasi kontrol akses pada mesin pengisian botol otomatis. menjadikannya layak untuk implementasi praktis di lapangan.

Tabel 2. Statistik Distribusi Waktu Respons Autentikasi per Kondisi Pengujian

Kondisi Pengujian	Min (detik)	Maks (detik)	Rata-rata (detik)	Std. Dev (detik)
Kondisi A - Normal	0,87	1,82	1,21	0,18
Kondisi B - Industri	0,93	2,31	1,47	0,24
Gabungan (A + B)	0,87	2,31	1,34	0,22

4.3 Analisis Pengaruh Kondisi Lingkungan

Analisis terhadap dampak kondisi lingkungan industri terhadap kinerja sistem menunjukkan beberapa faktor yang memengaruhi kinerja sistem fingerprint pada lingkungan industri. Pertama, kelembapan relatif tinggi (65-80% RH) terbukti menjadi faktor lingkungan yang paling berpengaruh terhadap kualitas citra sidik jari, terutama karena pembentukan kondensasi tipis pada permukaan kaca sensor yang mengurangi kontras antara *ridge* dan *valley* pada pola sidik jari. Hal ini konsisten dengan temuan Yudhana et al. [14] yang melaporkan degradasi akurasi signifikan pada kelembapan di atas 75% RH. Kedua, getaran mekanis pada rentang 8-12 Hz terbukti berkontribusi pada peningkatan FRR terutama melalui mekanisme mikro-gerak lateral jari selama proses akuisisi berlangsung, meskipun dampaknya lebih kecil dibandingkan kelembapan. Hasil pengujian menunjukkan

bahwa penggunaan pelindung sensor, pembaruan template sidik jari secara berkala, dan penyesuaian tingkat keamanan dapat membantu mempertahankan kinerja sistem pada kondisi lingkungan yang memiliki kelembapan dan getaran lebih tinggi. bahwa implementasi tiga langkah mitigasi-(a) penambahan penutup kaca anti-kondensasi hidropobik pada sensor housing, (b) *re-enrollment* periodik untuk memperbarui *template database*, dan (c) penyesuaian *Security Level* ke nilai 2 pada kondisi lingkungan ekstrem-secara efektif mempertahankan akurasi sistem di atas 97% bahkan pada kondisi paling menantang yang diuji. Hasil pengujian menunjukkan bahwa kondisi lingkungan perlu dipertimbangkan dalam perancangan sistem fingerprint, terutama pada lingkungan industri yang memiliki tingkat kelembapan dan getaran yang relatif tinggi. Investigasi lebih lanjut tentang penggunaan

sensor *fingerprint kapasitif* atau *ultrasonik*, yang secara teori lebih tahan terhadap kelembapan, direkomendasikan sebagai arah penelitian lanjutan.

4.4 Kinerja Subsistem *IoT* dan Pemantauan *Real-Time*

Kinerja subsistem *IoT* dan pemantauan *real-time* dievaluasi secara terpisah melalui pengukuran latensi transmisi data, keandalan koneksi, dan fungsionalitas *dashboard*. Latensi transmisi data dari *ESP32* ke *broker MQTT* diukur sebagai selisih antara *timestamp* lokal *ESP32* saat publikasi dan *timestamp* penerimaan yang dicatat oleh *broker*-memiliki rata-rata 87 ms dengan standar deviasi 23 ms pada kondisi koneksi *Wi-Fi* 2,4 GHz dengan kekuatan sinyal -65 dBm (RSSI). Latensi ini jauh di bawah persyaratan *real-time* aplikasi monitoring industri yang umumnya menetapkan ambang batas 500 ms [11]. Selama periode pengujian 14 hari, sistem *IoT* mencatat uptime koneksi sebesar 99,1% dengan 3 kejadian *disconnection* yang semuanya berhasil dipulihkan secara otomatis oleh mekanisme *reconnection* yang diimplementasikan dalam *firmware* dalam waktu kurang dari 30 detik. *Dashboard Node-RED* berhasil menampilkan data akses *real-time*, tabel log historis yang dapat difilter berdasarkan rentang waktu dan ID pengguna, serta grafik tren kinerja sistem. Fitur notifikasi Telegram berhasil mengirimkan 4 peringatan selama sesi pengujian, semua terpicu oleh skenario pengujian simulasi akses tidak sah yang telah direncanakan, dengan latensi notifikasi rata-rata 1,2 detik dari kejadian trigger hingga pesan diterima di *smartphone*. Data autentikasi yang tersimpan pada basis data dapat digunakan untuk proses pemantauan dan analisis aktivitas akses secara berkala.

4.5 Analisis Konsumsi Daya Sistem

Analisis konsumsi daya sistem dilakukan menggunakan *power meter* digital HIOKI PW3360 yang dikalibrasi pada tegangan suplai 5V DC. Sistem diidentifikasi memiliki tiga kondisi operasi dengan profil daya yang berbeda: kondisi *idle* (*waiting for finger*), kondisi akuisisi aktif (*sensor memindai dan memproses citra*), dan kondisi aktuasi (*relai aktif mengalirkan daya ke mesin*). Pada kondisi *idle*, *ESP32* dengan *Wi-Fi* aktif dalam mode *light sleep* mengonsumsi arus rata-rata 37 mA,

sehingga daya *idle* total sistem termasuk modul *AS608 (standby)* dan rangkaian pendukung adalah 185 mW. Pada kondisi akuisisi aktif, konsumsi arus meningkat menjadi rata-rata 68 mA terutama akibat aktivasi LED inframerah internal sensor *AS608* dan aktivitas pemrosesan prosesor *ESP32* yang meningkat, menghasilkan konsumsi daya 340 mW. Ketika relai aktif (*aktuator mesin hidup*), penambahan konsumsi koil relai sebesar 72 mW membawa total konsumsi sistem ke puncak 412 mW. Nilai konsumsi daya yang diperoleh menunjukkan bahwa sistem dapat beroperasi dengan kebutuhan energi yang relatif rendah dan memungkinkan implementasi *backup power* menggunakan baterai LiPo 3,7V kapasitas 5000 mAh yang dapat menyediakan operasi sistem selama minimal 8 jam dalam kondisi paling boros (asumsi 50% *duty cycle* aktuasi), cukup sebagai jembatan saat terjadi gangguan pasokan listrik utama. Dibandingkan dengan sistem keamanan berbasis PC atau *SCADA* yang dikaji oleh Setianingsih et al. [15] dengan konsumsi daya 45 W, sistem yang dikembangkan dalam penelitian ini jauh lebih efisien dalam hal konsumsi energi, menjadikannya pilihan yang lebih berkelanjutan (*sustainable*) untuk aplikasi berskala kecil dan menengah.

5. KESIMPULAN

Penelitian ini menganalisis kinerja sistem proteksi akses berbasis *fingerprint* pada mesin pengisian botol otomatis berbasis *IoT* menggunakan sensor *AS608* dan mikrokontroler *ESP32*. Berdasarkan hasil pengujian terhadap 500 percobaan autentikasi, sistem memperoleh nilai FAR sebesar 0,4%, FRR sebesar 1,2%, akurasi identifikasi sebesar 98,4%, dan waktu respons rata-rata sebesar 1,34 detik. Hasil tersebut menunjukkan bahwa sistem memiliki tingkat keamanan dan keandalan yang baik untuk aplikasi kontrol akses pada mesin industri ringan. Pengujian juga menunjukkan bahwa kondisi lingkungan berupa kelembapan dan getaran dapat memengaruhi performa sistem, namun pengaruhnya masih berada dalam batas yang dapat diterima. Selain itu, integrasi *MQTT* memungkinkan pemantauan status autentikasi secara *real-time*. Pada penelitian selanjutnya, evaluasi dapat diperluas dengan penggunaan

jenis sensor fingerprint lain serta pengujian pada lingkungan industri yang lebih beragam.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Laboratorium Sistem Kendali dan Otomasi Program Studi Teknik Elektro Politeknik Negeri Sriwijaya atas penyediaan fasilitas pengujian dan instrumen pengukuran, kepada seluruh responden yang telah berpartisipasi dalam sesi pengujian, serta kepada pihak-pihak yang memberikan dukungan terhadap terlaksananya penelitian ini.

DAFTAR PUSTAKA

- [1] H. Groover, *Automation, Production Systems, and Computer-Integrated Manufacturing*, 4th ed. Hoboken, NJ: Prentice Hall, 2015. [Online]. Available: <https://www.pearson.com/en-us/subject-catalog/p/automation-production-systems-and-computer-integrated-manufacturing/P200000003484>
- [2] Y. Mehmood, F. Ahmad, I. Yaqoob, A. Adnane, M. Imran, and S. Guizani, "Internet-of-Things-Based Smart Cities: Recent Advances and Challenges," *IEEE Commun. Mag.*, vol. 55, no. 9, pp. 16-24, Sep. 2017. doi: 10.1109/MCOM.2017.1600514
- [3] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, *Handbook of Fingerprint Recognition*, 3rd ed. London: Springer, 2022. doi: 10.1007/978-3-540-74175-1
- [4] GROW Technology, "AS608 Optical Fingerprint Sensor Module User Manual," Ver. 2.1, GROW Technology Co., Ltd., Shenzhen, China, 2021. [Online]. Available: <https://cdn-learn.adafruit.com/assets/assets/000/083/783/original/R503-fingerprint-module-user-manual.pdf>
- [5] Espressif Systems, "ESP32 Technical Reference Manual," Ver. 5.2, Espressif Systems, Shanghai, China, 2023. [Online]. Available: https://www.espressif.com/sites/default/files/documentation/esp32_technical_reference_manual_en.pdf
- [6] R. Ramli, Z. Zulkifli, and M. S. Saad, "Performance Evaluation of Optical Fingerprint Sensor Under Varying Humidity Conditions for Industrial Access Control," *Int. J. Adv. Sci. Eng. Inf. Technol.*, vol. 12, no. 3, pp. 1045-1051, 2022. doi: 10.18517/ijaseit.12.3.15432
- [7] A. K. Jain, A. Ross, and S. Prabhakar, "An Introduction to Biometric Recognition," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 14, no. 1, pp. 4-20, Jan. 2004. doi: 10.1109/TCSVT.2003.818349
- [8] National Institute of Standards and Technology (NIST), "Fingerprint Vendor Technology Evaluation (FpVTE) 2012," NIST Interagency Report 8034, Gaithersburg, MD, USA, 2014. [Online]. Available: <https://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.8034.pdf>
- [9] ISO/IEC, "Information Technology - Biometric Performance Testing and Reporting - Part 1: Principles and Framework," ISO/IEC 19795-1:2021, International Organization for Standardization, Geneva, Switzerland, 2021. [Online]. Available: <https://www.iso.org/standard/73515.html>
- [10] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A Survey," *Comput. Networks*, vol. 54, no. 15, pp. 2787-2805, Oct. 2010. doi: 10.1016/j.comnet.2010.05.010
- [11] OASIS Standard, "MQTT Version 5.0," OASIS Standard, Apr. 2019. [Online]. Available: <https://docs.oasis-open.org/mqtt/mqtt/v5.0/mqtt-v5.0.html>
- [12] D. Raharjo, S. Nugroho, and T. Widodo, "Sistem Absensi Fingerprint Berbasis NodeMCU dan MySQL Server pada Lingkungan Perkantoran," *JITET*, vol. 9, no. 2, pp. 156-163, Jul. 2021. doi: 10.23960/jitet.v9i2.2156
- [13] M. Abdurrohman, M. F. Putra, and D. Kurniawan, "Rancang Bangun Sistem Kontrol Akses Pintu Menggunakan ESP32 dan Sensor Fingerprint Berbasis Notifikasi Telegram," *Jurnal Teknik Informatika dan Sistem Informasi*, vol. 8, no. 1, pp. 245-256, Apr. 2022. doi: 10.28932/jutisi.v8i1.4289
- [14] A. Yudhana, I. Riadi, and F. Ridho, "Analisis Kinerja Modul Fingerprint ZFM60 pada Variasi Kelembapan Relatif untuk Aplikasi Identifikasi Biometrik," *Jurnal Nasional Teknik Elektro dan Teknologi Informasi (JNTETI)*, vol. 11, no. 3, pp. 178-185, Aug. 2022. doi: 10.22146/jnteti.v11i3.4102
- [15] C. Setianingsih, M. D. Farhan, and A. Heryana, "Sistem Monitoring Akses Terintegrasi Fingerprint dan SCADA pada Fasilitas Produksi Berbasis IoT," *Jurnal Infotel*, vol. 14, no. 2, pp. 112-122, May 2022. doi: 10.20895/infotel.v14i2.754
- [16] H. Fitts and R. L. Posner, *Human Performance*. Belmont, CA: Brooks/Cole Publishing, 1967; see also ISO 9241-110:2020, "Ergonomics of Human-System Interaction," 2020. [Online]. Available: <https://www.iso.org/standard/75258.html>
- [17] P. Wibowo and N. Azizah, "Dashboard Pemantauan IoT Real-Time Menggunakan

Node-RED dan InfluxDB untuk Sistem
Keamanan Industri," JITET, vol. 11, no. 3, pp.
201-209, Nov. 2023. doi:
10.23960/jitet.v11i3.3201