Jurnal Quancom
Vol.4, No.1, Juni 2026, pp. 9~15
e-ISSN: 2988-0998
P-ISSN: 2988-1005
DOI : https://doi.org/10.62375/d13myx30

Implementasi Face Recognition dan Algoritma Otp Pada Akses Keamanan Monitoring Pembangkit Listrik

Yesha Aishya Aprila[1], Mardhiah Masril[2]*, Sepsa Nur Rahman[3], Firdaus[4]
[1234] Sistem Komputer, Universitas Putra Indonesia 'YPTK" Padang
mardhiah_m@upiyptk.ac.id*

Article Info

Article history:

Received 25 Mei 2026
Revised 13 Juni 2026
Accepted 29 Juni 2026

Keyword:

Face Recognition, OTP, IoT, Power Generation, Security System.

ABSTRACT

The development of digital technology demands smarter and more integrated security systems, particularly for critical infrastructure such as power plants, which play a crucial role in national energy distribution. Power plant monitoring systems that still use conventional authentication methods like static passwords and RFID have weaknesses such as the risk of theft, forgery, and access misuse. Furthermore, the lack of integration with Internet of Things (IoT) systems means that the monitoring process is not fully real-time and potentially causes delays in detecting intrusions and security threats. This situation highlights the need for a layered security system capable of accurately and dynamically verifying user identity. This research aims to implement facial recognition technology and the Time-Based One-Time Password (TOTP) algorithm as a layered authentication system for IoT-based power plant monitoring. The system is designed to combine facial biometric verification with a time-based OTP code that can be generated independently of an internet connection. The integration of these two methods is expected to improve access security by minimizing the risk of identity spoofing, credential theft, and cyberattacks. The methods used include system design, hardware and software implementation, and performance testing of authentication and IoT integration. The expected outcome of this research is the creation of a more adaptive, reliable security system capable of recording access activity in real time. Therefore, the implementation of IoT-based facial recognition and TOTP can be an effective solution for enhancing protection for power plant monitoring systems, which are vital national assets.

PENDAHULUAN

Pada era digital saat ini, kebutuhan terhadap sistem keamanan yang lebih cerdas dan terintegrasi semakin meningkat, terutama pada infrastruktur kritis seperti pembangkit listrik yang menjadi tulang punggung distribusi energi nasional. Fenomena meningkatnya ancaman keamanan, baik berupa akses ilegal, pencurian data operasional, maupun sabotase sistem, menuntut penerapan teknologi yang mengikuti perkembangan zaman, dimana teknologi tersebut harus mampu memonitoring kondisi secara *real-time* dan memberikan proteksi berlapis terhadap akses fisik maupun digital, seperti teknologi *embedded system*, *automatic control* ataupun *Internet of Thing (IoT)* [1] [2] [3].

Meskipun teknologi keamanan terus berkembang, sistem monitoring pembangkit listrik yang ada saat ini masih menghadapi beberapa masalah mendasar terkait keamanan akses dan keandalan identifikasi operator. Sebagian besar sistem masih mengandalkan metode otentikasi konvensional seperti password statis, kartu identitas RFID, atau akses manual yang rentan terhadap pencurian, pemalsuan, dan penyalahgunaan oleh pihak yang tidak berwenang. Tidak adanya mekanisme verifikasi berlapis menyebabkan potensi celah keamanan, dimana seseorang dapat masuk ke sistem hanya dengan memiliki informasi login atau kartu akses yang dicuri. Selain itu, proses monitoring pada pembangkit listrik masih belum terintegrasi dengan internet, sehingga pengawasan kondisi operasional dilakukan secara manual dan tidak *real-time*, yang berisiko menimbulkan keterlambatan

deteksi gangguan atau tindakan kriminal. Kelemahan-kelemahan ini mengindikasikan perlunya sistem keamanan yang lebih modern, adaptif, serta mampu memverifikasi identitas pengguna secara biometrik dan dinamis, sehingga akses terhadap sistem pembangkit listrik benar-benar terbatas pada personel yang sah dan terjamin.

Kelemahan pada sistem keamanan akses pembangkit listrik saat ini dapat menimbulkan risiko serius terhadap operasional dan ketahanan energi. Akses tidak sah ke sistem monitoring dapat menyebabkan manipulasi data operasional, perubahan parameter kontrol, hingga potensi kerusakan peralatan yang berdampak pada gangguan pasokan listrik. Selain itu, pencurian atau penyalahgunaan data strategis terkait pembangkit dapat membuka peluang bagi tindakan sabotase atau serangan siber yang lebih terencana, yang pada akhirnya merugikan perusahaan maupun masyarakat luas. Ketidakmampuan sistem saat ini dalam melakukan verifikasi identitas secara akurat juga dapat memicu kesalahan operasional akibat masuknya pihak yang tidak kompeten mengakses panel kontrol. Lebih jauh, keterlambatan deteksi gangguan karena sistem monitoring yang tidak *real-time* membuat penanganan masalah menjadi tidak optimal, sehingga meningkatkan risiko pemadaman listrik dan kerugian ekonomi. Oleh karena itu, implementasi teknologi keamanan yang lebih kuat menjadi urgensi untuk memastikan pembangkit listrik beroperasi secara aman, handal, dan terlindungi dari ancaman modern.

Berbagai penelitian terdahulu menunjukkan bahwa pengembangan sistem keamanan berbasis *face recognition* telah meningkatkan perlindungan pada akses sistem keamanan, sistem yang dikembangkan oleh Topan Surya Dinata (2026) berfokus pada penggunaan teknologi *face recognition* dengan monitoring IoT pada rancangan *smart lock* sebagai sistem keamanan modern yang cerdas dan efisien. Hasil penelitian menunjukkan bahwa sistem mampu mendeteksi dan mengenali wajah pada kondisi pencahayaan yang cukup dengan akurasi rata-rata 91%, dan sistem juga berhasil melakukan monitoring IoT melalui telegram dan web dengan delay notifikasi rata-rata 2 detik [4]. Selanjutnya penelitian oleh Amanda Tsabita Putri (2025) dengan implementasi YOLO dalam sistem pengenalan wajah pada brankas, hasil penelitian menunjukkan bahwa sistem keamanan brankas berbasis *face recognition* menggunakan algoritma YOLO yang dikembangkan dalam penelitian ini memiliki tingkat akurasi yang tinggi. Namun belum terdapat fitur notifikasi seperti telegram atau email yang bertujuan untuk memberikan peringatan secara *real-time* dari jarak jauh [5].

Di sisi lain, penelitian oleh Fauzan Prasetyo Eka Putra (2024) berfokus pada penggunaan protokol WebSocket untuk pengiriman OTP pada safebox IoT dengan hasil performa sangat baik, yaitu delay rata-rata 71 ms dan throughput 258 bps menurut standar TIPHON. Meskipun efisien dalam komunikasi, penelitian tersebut belum membahas ketahanan keamanan OTP terhadap serangan digital dan hanya diuji pada lingkungan laboratorium, sehingga performanya belum terverifikasi dalam kondisi jaringan yang beragam [6].

Secara umum, ketiga penelitian mengindikasikan bahwa pengembangan keamanan berbasis *face recognition* dan IoT masih memiliki ruang optimalisasi, khususnya pada integrasi keamanan tambahan, peningkatan efektivitas sensor fisik, dan mekanisme verifikasi berlapis. Pada penelitian ini sistem autentikasi berlapis digunakan untuk mengamankan akses sistem monitoring pembangkit tenaga listrik, hal ini dirasa sangat penting dimana dengan menggabungkan teknologi biometrik *face recognition* dan algoritma yang menghasilkan kode OTP berbasis waktu. Inovasi teknologi khususnya *face recognition* adalah salah satu teknologi kecerdasan buatan (AI) yang signifikan dan berkembang pesat saat ini terutama untuk tujuan keamanan dan penegakan hukum [7]. *Face recognition* memanfaatkan fitur biometrik unik setiap individu, karakteristik atau ciri khas unik dari wajah sehingga sulit dipalsukan, akibatnya dapat meningkatkan keakuratan dan keamanan verifikasi pada security system [8] [9].

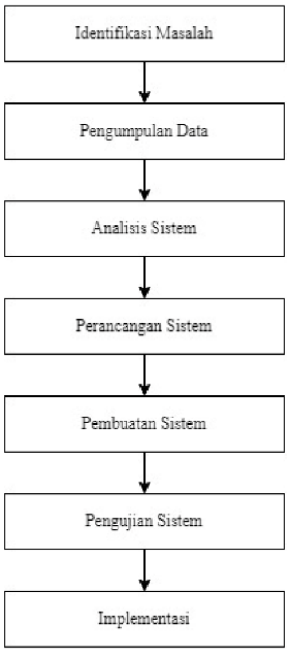
Algoritma *Time Based on Time Password* (OTP) adalah *stream cipher* yang melakukan enkripsi dan dekripsi satu karakter setiap kali. Penggunaan algoritma OTP dalam kriptografi adalah sebagai dasar untuk mengaburkan suatu informasi yang ingin dirahasiakan dengan cara mengacak informasi tersebut sehingga menjadi suatu informasi yang tidak dapat dipahami oleh orang lain [10]. OTP merupakan kode yang digunakan hanya sekali untuk otentikasi pengguna dalam suatu sesi, dimana kode ini tidak dapat digunakan Kembali sehingga memberikan tingkat keamanan yang lebih tinggi [11].

Internet of Things (IoT) merupakan teknologi mutakhir yang mengacu pada berbagai perangkat dan sistem yang saling terhubung melalui internet untuk berbagi data [12] [13]. Teknologi ini melibatkan penggunaan sensor dan perangkat lunak komunikasi untuk mengontrol, menghubungkan, dan mentransfer data antarperangkat dengan memanfaatkan jaringan internet sehingga memungkinkan kinerja tanpa pengawasan langsung [14].

Berdasarkan pemaparan diatas maka pada penelitian ini penulis menawarkan pendekatan keamanan yang lebih adaptif dan andal untuk objek vital seperti pembangkit listrik dengan merancang akses keamanan pada monitoring pembangkit listrik dengan menggunakan teknologi *face recognition* untuk memastikan identitas pengguna secara visual sekaligus memberikan lapisan keamanan kriptografis, sehingga lebih tahan terhadap serangan siber, spoofing identitas, maupun gangguan jaringan dengan penerapan Algoritma OTP serta dukungan integrasi teknologi IoT sehingga adanya monitoring secara *real time*.

METODE

Kerangka kerja penelitian menggambarkan tahapan penelitian yang akan dilakukan dengan tujuan menggambarkan detail proses penelitian agar tidak melenceng dari konsep yang sudah ditentukan. Kerangka kerja penelitian ini akan dijadikan pedoman dalam menyelesaikan permasalahan yang ada berdasarkan tahapan yang jelas yaitu identifikasi masalah, pengumpulan data, analisis sistem, perancangan sistem, pengujian sistem dan implementasi [15]. Agar mendapatkan hasil seperti yang diinginkan, kerangka penelitian dapat dilihat pada gambar 1.



Gambar 1. Kerangka kerja penelitian

Kerangka kerja penelitian diatas akan dijelaskan secara rinci dengan tahapan-tahapan sebagai berikut:

A. Identifikasi Masalah

Permasalahan yang telah berhasil diidentifikasi pada sistem monitoring keamanan pembangkit listrik adalah akses keamanan dan identifikasi operator masih dilakukan secara manual yang rentan terhadap pencurian, pemalsuan, dan penyalahgunaan oleh pihak yang tidak berwenang, selain itu proses monitoring pada pembangkit listrik masih belum terintegrasi dengan internet sehingga pemantauan tidak dapat dilakukan secara *real-time*.

B. Pengumpulan Data

Pengumpulan data merupakan tahap penting yang bertujuan memahami secara mendalam terkait potensi dan permasalahan yang terjadi secara tepat, sehingga penelitian ini dapat menghasilkan solusi yang optimal terhadap pemecahan permasalahan yang telah dianalisis sebelumnya.

C. Analisis sistem

Analisis sistem diawali mulai dari menganalisis perangkat input, proses dan output yang diperlukan pada sistem akses keamanan monitoring pembangkit listrik menggunakan teknologi face recognition dan OTP.

D. Perancangan Sistem

Pada tahap ini, dilakukan desain sistem awal terhadap perangkat keras dan perangkat lunak yang akan digunakan, meliputi *context diagram, data flow diagram, blok diagram, flowchart program*.

E. Pembuatan Sistem

Pembuatan sistem dilakukan berdasarkan desain yang telah dirancang sebelumnya, dimulai dari pembuatan hardware kemudian dilanjutkan dengan pembuatan program kontrol.

F. Pengujian Sistem

Pengujian sistem atau uji coba pemakaian merupakan proses pengujian untuk mengetahui apakah sistem kontrol yang dibuat dapat beroperasi sesuai dengan yang diinginkan peneliti dan pengguna.

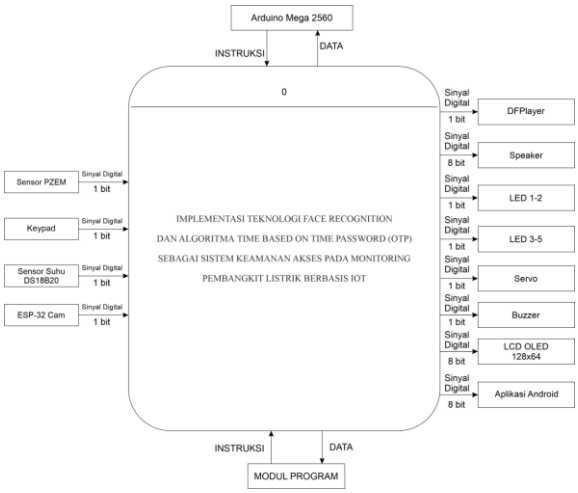
G. Implementasi

Pada tahap ini, implementasi sistem diawali dengan menempatkan sistem ke dalam situasi atau kondisi lingkungan yang menyerupai kondisi nyata untuk melihat kinerja sistem secara langsung. Tujuan dari tahapan ini adalah untuk memastikan bahwa sistem mampu beroperasi sesuai dengan fungsi yang diharapkan serta menjadi solusi terdahap masalah yang telah diidentifikasi sebelumnya.

HASIL DAN PEMBAHASAN

A. Context Diagram

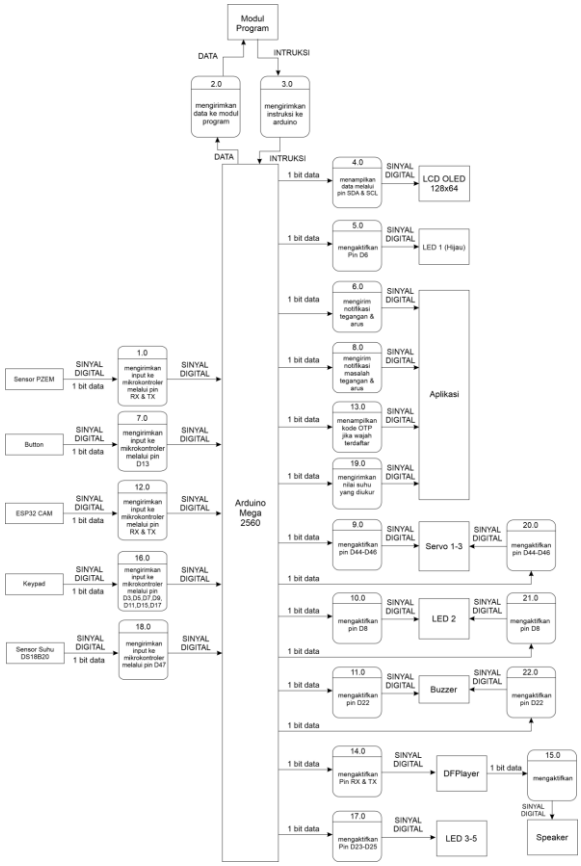
Context diagram ini digunakan untuk memudahkan dalam proses penganalisaan sistem yang dirancang secara keseluruhan. *Context diagram* berfungsi sebagai media yang mendefinisikanbatasan ruang lingkup secara jelas dan memetakan interaksi antara sistem dengan *external entity*, dimana *Context diagram* terdiri dari satu proses dan beberapa buah *external entity.*



Gambar 2. Context diagram

H. *Data flow Diagram*

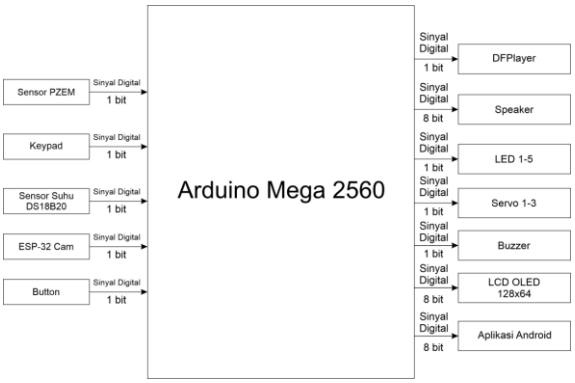
Data flow diagram (DFD) adalah gambaran yang lebih rinci dari sistem yang dirancang. DFD bertujuan untuk memetakan secara visual bagaimana aliran data dan instruksi dari input sensor, melalui proses logika, hingga ke output sistem.



Gambar 3. Data flow diagram

I. *Blok Diagram*

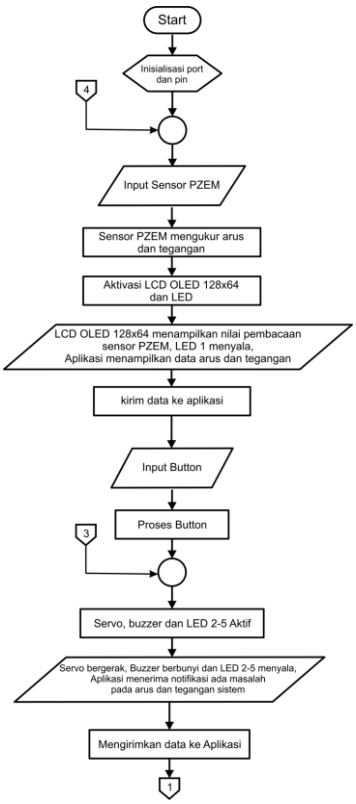
Berdasarkan *Data Flow Diagram* pada gambar 3, untuk mengetahui komponen-komponen yang digunakan pada sistem secara grafis ringkas sehingga lebih mudah dipahami, dimana alur input, proses dan output sistem akan tergambar pada blok diagram yang ditampilkan pada gambar 4.



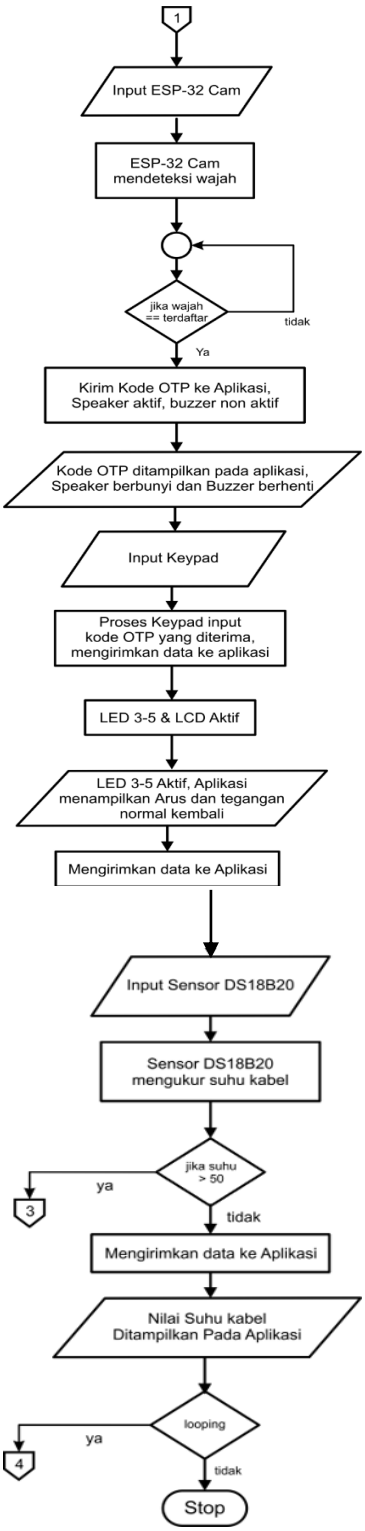
Gambar 4. Blok diagram

J. *Flowchart Program*

Flowchat program menggambarkan alur logika dan instruksi program dari sistem secara terstruktur, agar alur kerja sistem berjalan dengan baik, flowchat penelitian ditunjukkan pada gambar 5 dan gambar 6.

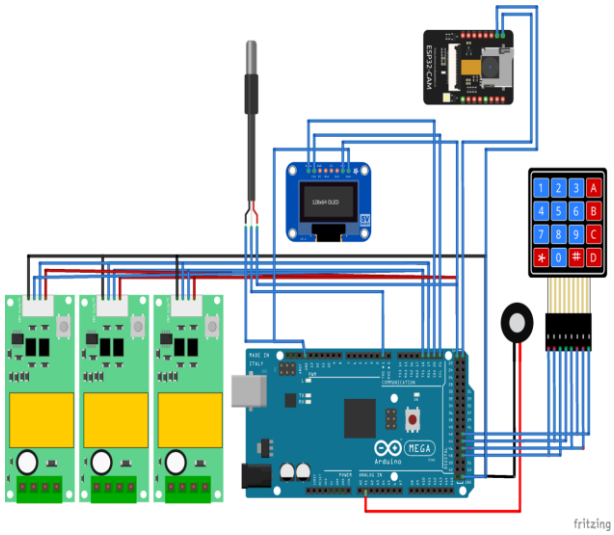


Gambar 5. Flowchat program (1)



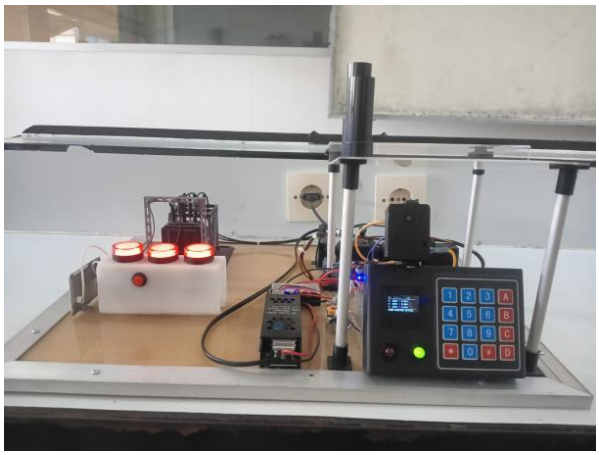
Gambar 6. Flowchat program (2)

K. Desain Rangkaian Hardware



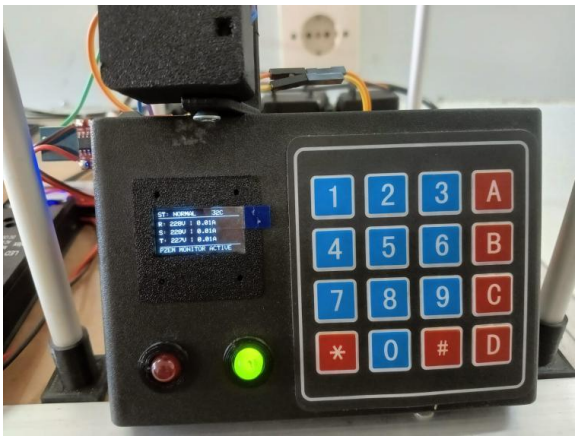
Gambar 7. Rangkaian sistem

Ketika sistem mulai diaktifkan dan berada dalam kondisi normal, sistem akan memastikan bahwa arus dan tegangan berada pada batas aman. Hal ini ditandai dengan menyala nya LED 1 berwarna hijau sebagai indikator utama, serta LED 3 hingga LED 5 yang berfungsi sebagai prototype lampu juga ikut menyala.



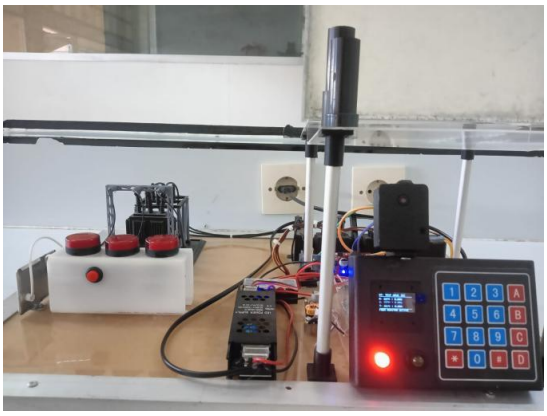
Gambar 8. Kondisi sistem stand by

Pada saat yang sama, LCD OLED 128x64 akan aktif dan menampilkan berbagai informasi penting dari sistem. Layar ini menampilkan hasil pembacaan sensor PZEM berupa nilai arus dan tegangan pada Phase 1 hingga Phase 3, serta hasil pembacaan sensor suhu DS18B20 berupa nilai suhu pada sistem. Selain itu, seluruh data tersebut juga dapat dipantau melalui aplikasi monitoring yang menampilkan status sistem secara *real-time*, termasuk nilai arus, tegangan, suhu, serta kode OTP berupa token.



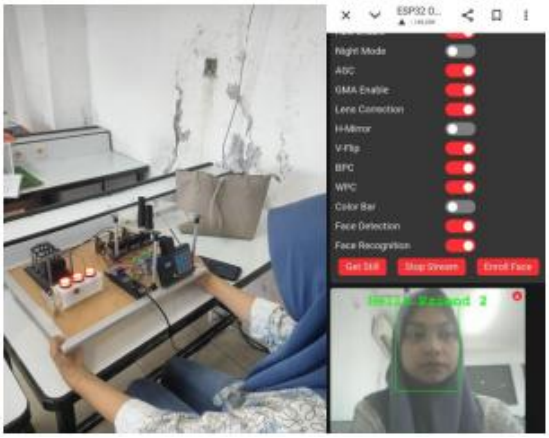
Gambar 9. Tampilan LCD

Namun, ketika sistem mendeteksi kondisi tidak normal, seperti lonjakan arus atau peningkatan suhu, maka sistem akan langsung merespons secara otomatis. LED 1 (hijau) akan mati dan digantikan oleh LED 2 (merah) yang menyala sebagai tanda bahaya. Bersamaan dengan itu, servo akan aktif untuk memutuskan aliran listrik, buzzer akan berbunyi sebagai alarm peringatan, dan LED 3 hingga LED 5 akan mati. Pada aplikasi monitoring, kondisi ini ditandai dengan status "TRIP_ARUS" yang menunjukkan adanya gangguan pada sistem kelistrikan.



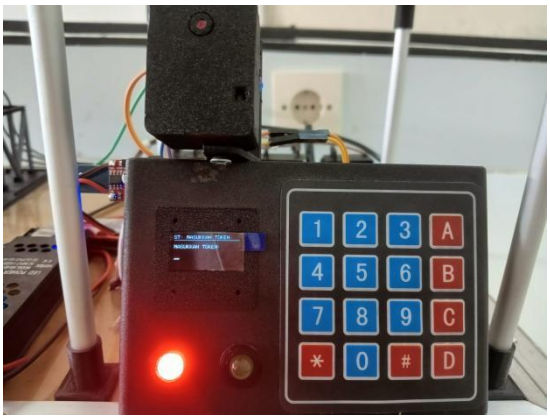
Gambar 10. Sistem mendeteksi kondisi tidak normal

Dalam kondisi tersebut, sistem keamanan berbasis autentikasi akan diaktifkan. User yang memiliki wewenang terhadap akses sistem keamanan monitoring pembangkit listrik diminta melakukan verifikasi melalui proses *face recognition* untuk melakukan scanning wajah. Jika wajah user terdaftar dalam sistem, maka sistem akan mengirimkan kode OTP berupa token ke aplikasi.



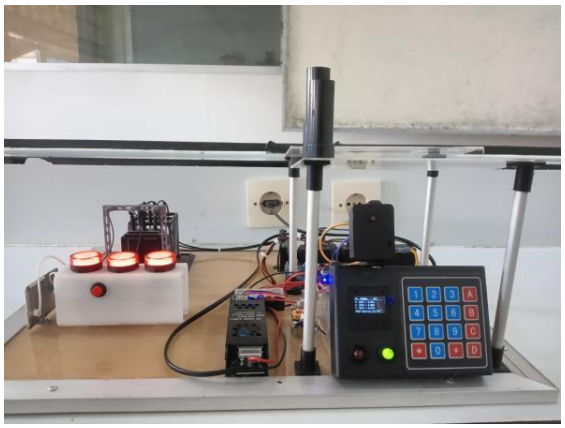
Gambar 11. Tampilan verifikasi keamanan dengan *face recognation*

Selanjutnya, LCD OLED akan menampilkan perintah kepada user untuk memasukkan kode OTP yang telah diterima. User kemudian memasukkan token tersebut melalui keypad yang tersedia pada input sistem.



Gambar 12. Input kode otp

Apabila kode OTP yang dimasukkan sesuai atau benar, maka sistem akan kembali ke kondisi normal. Hal ini ditandai dengan LED hijau yang kembali menyala, serta LED 3 hingga LED 5 yang aktif kembali sebagai indikator bahwa aliran listrik telah pulih dan sistem kembali beroperasi dengan aman.



Gambar 13. Tampilan sistem setelah verifikasi keamanan benar

SIMPULAN

Berdasarkan hasil dan analisis sebelumnya, maka dapat diambil kesimpulan sebagai berikut. Arduino Mega 2560 dapat mengontrol sistem dengan baik. ESP32-CAM dapat mendeteksi wajah user yang mendapat wewenang secara akurat dan sistem dapat mengirim kode OTP melalui aplikasi sehingga mampu memberikan autentikasi awal yang aman sebelum mengakses sistem monitoring pembangkit listrik. Sensor PZEM dapat membaca parameter energi listrik seperti tegangan,arus dan daya secara *real-time* dengan baik. Sensor Suhu DS18B20 dapat memberikan informasi kondisi suhu perangkat listrik dengan baik. Keypad dapat berfungsi dengan baik dalam menerima input kode OTP. LCD 20x4 dapat menampilkan informasi status sistem. Buzzer dapat memberikan peringatan suara yang efektif ketika terdeteksi akses yang tidak sah atau saat terjadi kondisi berbahaya pada panel listrik. Aplikasi dapat berfungsi dengan baik sebagai penerima informasi yang dikirimkan sistem kepada user.

DAFTAR PUSTAKA

[1] A. Malfaresa, M. Masril, O. E. Putra, H. Awal, and B. Hendrik, "Inovasi Sistem Kontrol Akses Gerbang Kantor Pemerintahan Berbasis Teknologi Multisensor Dan Deteksi Plat Nomor Kendaraan," *J. Quancom*, vol. 2, no. 2, 2024.

[2] L. Andriani, R. Devita, H. Awal, and M. Masril, "Optimalisasi Pemanfaatan Android pada Sistem Peringatan dan Monitoring Keamanan Perlintasan Kereta Api," *J. Quancom*, vol. 2, no. 1, 2024.

[3] R. M. Burhan, R. Noviardi, M. A. Masril, and Firmansyah, "Application of YOLOv8 Algorithm for Coral Reef Disease Detection," *J. Rekayasa Sist. dan Teknol. Inf.*, vol. 9, no. 5, pp. 1091–1099, 2025.

[4] T. S. Winata, D. Hasminta, S. Maha, and S. Lock, "Impression : Jurnal Teknologi dan Informasi Rancang Bangun Smart Lock Berbasis ESP32-CAM dengan Face," *Impr. J. Teknol. dan Informas*, vol. 5, no. 1, pp. 108–117, 2026.

[5] A. T. Putri, I. Salamah, and M. M. Rose, "Implementasi Sistem Keamanan Brankas Berbasis Face Recognition Menggunakan Algoritma YOLO dengan Verifikasi Fingerprint," *J. Technol. Informatics*, vol. 7, no. 2, pp. 161–174, 2025.

[6] F. Prasetyo, E. Putra, F. Muslim, N. Hasanah, R. Paradina, and R. Alim, "Jurnal Sistim Informasi dan Teknologi Analisis Komparasi Protokol Websocket dan MQTT Dalam Proses Push Notification," *J. Sistim Inf. dan Teknol.*, vol. 5, no. 4, pp. 63–72, 2024, doi: 10.60083/jsisfotek.v5i4.325.

[7] H. Murdani, E. L. Bella, and A. Fatwanto, "pada layanan sirkulasi perpustakaan," *Daluang J. Libr. Inf. Sci.*, vol. 4, no. 2, pp. 82–96, 2024, doi: 10.21580/daluang.v4i2.2024.21976.

[8] T. Huyo, R. Bakar, and A. D. Wowor, "Implementasi Algoritma Face Recognation Menggunnakan Face-API.JS pada Sistem Verifikasi SIM Digital," *Idealis Indones. J. Inf. Syst.*, vol. 8, no. 2, pp. 236–247, 2025.

[9] M. F. Yasykur, W. A. Saputra, F. Informatika, and J. Tengah, "Implementasi Face Recognation Pada Sistem Presensi Mahasiswa Menggunakan Metode SSD dan LBPH," *J. Pendidik. Teknol. Inf.*, no. April, pp. 63–74, 2024.

[10] N. Manalu, "TIN : Terapan Informatika Nusantara Modifikasi Metode One-Time Pad Dan Chaostic Function Untuk Mengamankan Pesan TIN : Terapan Informatika Nusantara," *TIN Terap. Inform. Nusant.*, vol. 3, no. 1, pp. 1–4, 2022, doi: 10.47065/tin.v3i1.1699.

[11] I. H. Cahyadi *et al.*, "Perancangan sistem otentikasi berbasis one time passworsd (otp) dengan algoritma rsa sebagai metode autentikasi: implementasi menggunakan bahasa pemrograman phyton," *TRIPLE A J. Pendidik. Teknol. Inf.*, vol. 2, no. 1, pp. 8–13, 2023.

[12] M. R. Husada, J. E. Candra, L. Hernando, and M. A. Masril, "Perancangan Sistem Pencatat Kecepatan Angin Untuk Studi Kelayakan Pembangunan Pembangkit Listrik Tenaga Bayu (PLTB) Berbasis Internet of Things (IoT)," *J. Quancom*, vol. 3, no. 2, 2025.

[13] B. Hendrik *et al.*, "Rancang Bangun Alat Ukur Kadar Protein Pada Makanan Pokok Berbasis Iot Dengan Kendali BOT Telegram," *J. Ilmu Komput. Dan Inform.*, vol. 2, no. 4, pp. 295–301, 2026.

[14] A. Syahfitri, "Internet of Things (IoT), Sejarah , Teknologi , dan Penerapannya," *Uranus J. Ilm. Tek. Elektro, Sains dan Inform.*, vol. 3, no. 1, pp. 113–120, 2025.

[15] G. Risyadi, M. Masril, and R. H. Zain, "Inovasi Helm Infanteri Terintegrasi Battlefield Management System Untuk Monitoring Area Pertempuran Secara Real-Time," *J. Quancom*, vol. 3, no. 2, 2025.