Rancang Bangun Sistem Keamanan Laboratorium Menggunakan *Face Recognition* Berbasis *Internet of Thing* (IoT)

Nur Afiyat[1*], Ghilmil Mubtadi[1]

[1] Program Studi Teknik Elektro Universitas Qomaruddin, Gresik, Indonesia

* Korespondensi: nurafiyat@uqgresik.ac.id

Received: 22 October 2024
Revised: 28 November 2024
Accepted: 20 December 2024

Citation:
Afiyat, N., & Mubtadi, G. (2024). Rancang bangun sistem keamanan laboratorium menggunakan face recognition berbasis IoT. *QOMARUNA Journal of Multidisciplinary Studies*, *2*(1), 20–41.

ABSTRACT

An Internet of Things (IoT)-based laboratory security system is designed to improve security and monitoring efficiency. This study aims to develop such a system using ESP-32 CAM (Embedded Serial Peripheral Interface 32-bit Camera), a camera module with an ESP32 microcontroller with Wi-Fi connectivity and image processing capabilities for real-time access control and room monitoring. Firebase is a cloud-based facial data storage platform, and the Telegram application is a medium that allows automatic notifications. Access control testing was conducted involving five user samples. The system recorded a facial recognition success rate of 90% (9 out of 10 tests were successful), which is considered "good" based on the accuracy threshold of ≥ 85% for security applications. However, accuracy decreases in non-ideal conditions, such as when the user's distance from the camera exceeds 30 cm or the angle of view of the face is not aligned with the camera. Non-ideal refers to operational situations where optimal parameters, such as distance and facial orientation, are unsatisfied. The notification delivery delay to the Telegram application was tested using Wireshark, with an average time of 18,528 ms, indicating that the system has a fast response in real-time. In addition, the monitoring camera (ESP-32 CAM) successfully sent stable real-time video to the laboratory manager's web without significant interference. The test results show that this system meets the design objectives as an efficient laboratory security solution. Some improvements are needed to improve accuracy under non-ideal conditions and expand monitoring testing to various network scenarios.

Keywords: *IoT, laboratory security, ESP-32 CAM, Firebase, real-time monitoring*

ABSTRAK

Sistem keamanan laboratorium berbasis *Internet of Things* (IoT) dirancang untuk meningkatkan keamanan dan efisiensi pengawasan. Penelitian ini bertujuan merancang sistem ini menggunakan ESP-32 CAM (*Embedded Serial Peripheral Interface* 32-bit *Camera*), yaitu modul kamera dengan mikrokontroler ESP32 yang memiliki konektivitas Wi-Fi dan kemampuan pengolahan citra untuk kontrol akses dan monitoring ruangan secara *real-time*. Firebase digunakan sebagai *platform* penyimpanan data wajah berbasis *cloud*, dan aplikasi Telegram sebagai media pengiriman notifikasi otomatis. Pengujian kontrol akses dilakukan dengan melibatkan 5 sampel pengguna. Sistem mencatat tingkat keberhasilan pengenalan wajah sebesar 90% (9 dari 10 kali pengujian berhasil), yang dianggap "baik" berdasarkan ambang akurasi ≥ 85% untuk aplikasi keamanan. Namun, akurasi menurun pada kondisi non-ideal, seperti ketika jarak pengguna dari kamera melebihi 30 cm atau sudut pandang wajah tidak sejajar dengan kamera. Non-ideal merujuk

pada situasi operasional di mana parameter optimal, seperti jarak dan orientasi wajah, tidak terpenuhi. Delay pengiriman notifikasi ke aplikasi Telegram diuji menggunakan Wireshark, dengan rata-rata waktu sebesar 18,528 ms, menunjukkan sistem memiliki respons cepat secara real-time. Selain itu, kamera monitoring (ESP-32 CAM) berhasil mengirimkan video real-time yang stabil ke web pengelola laboratorium tanpa gangguan signifikan. Hasil pengujian menunjukkan bahwa sistem ini memenuhi tujuan perancangan sebagai solusi keamanan laboratorium yang efisien. Beberapa peningkatan diperlukan untuk meningkatkan akurasi pada kondisi non-ideal dan memperluas pengujian monitoring untuk berbagai skenario jaringan.

Kata kunci: IoT, keamanan laboratorium, ESP-32 CAM, Firebase, *real-time* monitoring

1. Pendahuluan

Keamanan laboratorium adalah aspek penting yang perlu diperhatikan, terutama karena laboratorium sering kali dilengkapi dengan peralatan yang mahal dan sensitif. Kerusakan atau kehilangan peralatan tidak hanya menghambat kelancaran operasional, tetapi juga menyebabkan kerugian finansial yang signifikan. Oleh karena itu, diperlukan sistem keamanan yang andal untuk mencegah kejadian semacam itu.

Perkembangan teknologi telah menghadirkan berbagai solusi untuk meningkatkan keamanan laboratorium. Salah satu metode yang umum digunakan adalah sistem keamanan berbasis *fingerprint.* Meskipun populer, sistem ini memiliki beberapa kelemahan, seperti kendala dalam identifikasi sidik jari akibat faktor kebersihan atau kondisi fisik individu, serta potensi manipulasi data yang menciptakan celah keamanan (Santoso, 2020). Selain itu, metode tradisional seperti kunci fisik, kartu akses, dan kata sandi juga memiliki keterbatasan, seperti risiko kehilangan, lupa, atau pencurian akses.

Dalam menghadapi tantangan tersebut, pengelola laboratorium mulai beralih ke metode yang lebih canggih, seperti *face recognition* dan sistem berbasis Internet of Things (IoT) (Sunardi dkk., 2022). . Teknologi ini dinilai lebih efisien dan sulit dimanipulasi. Dengan perkembangan ini, laboratorium dapat lebih mudah dikelola dan dipantau, sehingga keamanan aset dapat terjaga dengan lebih baik (Syafutra dkk., 2024).

Sistem *face recognition* semakin banyak digunakan dalam berbagai aplikasi keamanan karena karakteristik wajah manusia yang unik dan sulit dipalsukan. Teknologi ini mampu mengenali individu dengan akurasi tinggi, bahkan dalam kondisi pencahayaan yang bervariasi, posisi wajah yang berbeda, atau penggunaan aksesori seperti kacamata. Penggunaan *face recognition* dalam keamanan laboratorium berkembang pesat, terutama ketika dikombinasikan dengan teknologi IoT. Salah satu inovasi populer adalah penggunaan kamera ESP-32 untuk memantau aktivitas laboratorium secara *real-time*. Kamera ini menangkap citra wajah dan mengirimkan notifikasi otomatis ke aplikasi, memungkinkan pengelola menerima peringatan jika ada aktivitas mencurigakan. Integrasi dengan sistem IoT membuat pengawasan lebih efektif, memungkinkan akses jarak jauh untuk memantau fasilitas yang dilengkapi peralatan mahal.

Penelitian oleh (Murjitama dkk., 2024) menunjukkan bahwa sistem *face recognition* berbasis IoT pada penguncian pintu pintar mampu meningkatkan keamanan secara signifikan. Sistem ini memiliki akurasi tinggi dalam mengenali wajah pengguna dan fitur notifikasi real-time yang memberi peringatan jika terjadi akses tidak sah. Selain itu, (Satrio, 2022) uga mengembangkan sistem keamanan rumah berbasis IoT menggunakan Arduino dan kamera CCTV. Sistem ini memungkinkan monitoring keamanan jarak jauh melalui perangkat mobile, memberikan fleksibilitas bagi pengguna dalam menjaga keamanan properti mereka.

Hasil dari kedua penelitian tersebut menegaskan bahwa teknologi IoT dapat mengatasi kelemahan metode keamanan tradisional, seperti kunci fisik atau kata sandi, yang sering kali rentan terhadap manipulasi atau kelalaian pengguna. Dengan integrasi *face recognition* dan IoT, sistem keamanan menjadi lebih andal, efektif, dan responsif terhadap potensi ancaman

Berbagai penelitian telah dilakukan untuk mengembangkan sistem keamanan berbasis **face recognition** menggunakan metode Local Binary Pattern Histogram (LBPH). Misalnya, penelitian oleh (Rama dkk., 2020) yang mengembangkan sistem keamanan brankas berbasis *face recognition* menggunakan parameter Grid X dan Grid Y = 8x8, Neighbors = 8, dan Radius = 1. Penelitian ini menunjukkan hasil akurasi 95,56% dengan waktu komputasi sebesar 2,35 detik pada jarak optimal pengambilan gambar 20 hingga 25 cm. Studi lainnya oleh (Sunardi dkk., 2022) merancang sistem keamanan ruangan berbasis Raspberry Pi dengan kombinasi metode Haar Cascade dan LBPH. Sistem ini mampu mengenali wajah dengan cepat dan mengirim notifikasi melalui aplikasi Telegram kepada pemilik saat mendeteksi aktivitas mencurigakan. Selain itu, penelitian oleh (Bachtiar, 2022) juga mengembangkan sistem dual keamanan untuk pintu rumah dengan integrasi *face recognition* dan sidik jari berbasis IoT. Sistem ini menggunakan kamera ESP-32 dan berhasil menunjukkan bahwa kamera tersebut dapat menangkap wajah dengan baik pada jarak 30 cm hingga 100 cm.

Penelitian sebelumnya meskipun menunjukkan keberhasilan dalam penerapan metode LBPH, masih terdapat beberapa kekurangan yang perlu diperbaiki. (Rama dkk., 2020) melaporkan bahwa citra wajah yang diambil dari jarak terlalu dekat sering kali tampak buram, sementara citra yang diambil dari jarak terlalu jauh tidak selalu dikenali dengan akurat. Pencahayaan juga berperan penting dalam keberhasilan *face recognition*, di mana intensitas cahaya yang tidak memadai dapat mengurangi akurasi sistem. (Sunardi dkk., 2022) mencatat waktu respons sistem yang relatif lambat untuk mengirim notifikasi melalui Telegram, dengan rata-rata waktu komputasi 19,78 detik dalam posisi standby. Selain itu, penelitian (Bachtiar, 2022) mengidentifikasi bahwa keterbatasan kapasitas penyimpanan kamera ESP-32 hanya mampu menyimpan hingga tiga pengguna, sehingga tidak cocok untuk implementasi skala besar. Sinyal router yang tidak stabil juga memengaruhi kecepatan pengiriman data dari kamera ke aplikasi, menyebabkan delay sekitar 3 hingga 6 detik dalam pengiriman notifikasi ke Telegram.

Berdasarkan tinjauan ini, penelitian bertujuan untuk mengembangkan dan menguji sistem keamanan laboratorium berbasis IoT dengan menggunakan ESP-32 CAM untuk pengenalan wajah, Firebase untuk penyimpanan data, dan Telegram untuk notifikasi otomatis, serta mengevaluasi kinerja sistem berdasarkan metrik delay pengiriman notifikasi di Laboratorium Teknik Elektro Universitas Qomaruddin. Integrasi dengan *cloud server* Firebase memungkinkan penyimpanan data secara aman serta sinkronisasi informasi secara *real-time*, sehingga aktivitas laboratorium dapat dipantau dengan cepat dan efisien. Notifikasi tetap dikirimkan meskipun aplikasi Telegram tidak aktif, memberikan fleksibilitas bagi pengelola laboratorium. Sistem ini juga dilengkapi dengan antarmuka berbasis *web browser* yang memungkinkan monitoring ruangan dari mana saja secara *real-time*.

Fokus penelitian ini adalah meningkatkan efisiensi dan keandalan sistem keamanan dengan mengatasi beberapa keterbatasan yang ada pada sistem *face recognition* sebelumnya, seperti pengaruh pencahayaan, jarak pengambilan gambar, dan kecepatan respon. Dengan pengembangan ini, diharapkan sistem keamanan laboratorium dapat beroperasi lebih efektif dan dapat diterapkan di berbagai institusi lain yang membutuhkan sistem pengamanan yang serupa.

2. Tinjauan Pustaka

2.1. Keamanan Laboratorium Berbasis Teknologi

Keamanan laboratorium, terutama yang menyimpan peralatan bernilai tinggi dan data sensitif, sangat penting dan harus diperhatikan dengan serius. Dengan kemajuan teknologi, sistem keamanan berbasis teknologi seperti IoT semakin banyak digunakan untuk meningkatkan efektivitas pengawasan. Menurut (Sufian & Setiyadi, 2021), penerapan IoT memungkinkan integrasi perangkat keamanan seperti sensor gerak, kamera, dan alarm yang terhubung melalui jaringan internet, sehingga dapat dipantau secara *real-time* menggunakan aplikasi Blynk, yang menekankan bahwa monitoring *real-time* melalui aplikasi yang sederhana dan intuitif ini memungkinkan respons yang lebih cepat terhadap ancaman, sehingga keamanan laboratorium menjadi lebih efisien dan terjamin. Hal ini memungkinkan pengelola laboratorium untuk menerima notifikasi otomatis jika ada aktivitas mencurigakan tanpa perlu pengawasan manusia terus-menerus.

Keunggulan utama sistem berbasis teknologi dibandingkan metode manual adalah kemampuannya untuk beroperasi secara otomatis dan lebih efisien. Sistem ini mengatasi keterbatasan tenaga manusia, seperti kelelahan atau kurangnya fokus, yang sering kali menjadi penghambat dalam pengawasan keamanan yang optimal. Selain mendeteksi aktivitas mencurigakan, sistem ini juga dapat diprogram untuk memantau kondisi lingkungan, seperti suhu atau kebocoran gas, yang bisa mengancam keamanan peralatan di laboratorium. Penggunaan teknologi ini tidak hanya meningkatkan keamanan dari ancaman eksternal seperti pencurian, tetapi juga melindungi laboratorium dari potensi bahaya internal. Selain itu, dengan aplikasi seperti Blynk, pengelola dapat memantau laboratorium dari jarak jauh melalui komputer atau smartphone.

2.2. *Face Recognition* dalam Sistem Keamanan

Sistem *face recognition* telah menjadi pilihan utama dalam pengembangan sistem keamanan berbasis biometrik karena kemampuannya untuk mengenali individu dengan akurasi tinggi. Teknologi ini bekerja dengan memetakan karakteristik unik wajah seseorang, seperti bentuk wajah, jarak antar mata, dan bentuk hidung, yang memungkinkan sistem untuk mengenali seseorang secara cepat dan efektif. Menurut (Sunardi dkk., 2022), *face recognition* dalam sistem keamanan modern memberikan tingkat akurasi yang jauh lebih tinggi dibandingkan dengan metode keamanan konvensional, seperti penggunaan kata sandi atau kunci fisik, karena sistem ini mengandalkan fitur biologis yang unik untuk setiap individu. Dengan integrasi teknologi IoT, *face recognition* semakin andal, karena memungkinkan monitoring dan kontrol akses secara real-time serta pengiriman notifikasi otomatis jika terjadi aktivitas yang mencurigakan.

Dalam penelitian lain, (Bachtiar, 2022) menyatakan bahwa sistem *face recognition* berbasis IoT memberikan efisiensi lebih tinggi karena sistem ini mampu beroperasi dalam berbagai kondisi pencahayaan dan lingkungan, tanpa mengurangi keakuratan pengenalan. Lebih jauh lagi, sistem ini dapat dikombinasikan dengan sistem alarm otomatis yang akan memicu tindakan pengamanan jika wajah yang tidak dikenal mencoba mengakses area terlarang. Hal ini menjadikan *face recognition* sebagai salah satu solusi keamanan yang tidak hanya efektif, tetapi juga praktis dan dapat diintegrasikan dengan perangkat lain untuk meningkatkan perlindungan terhadap aset berharga di laboratorium.

Menurut (Suryansah dkk., 2020), LBPH mampu memberikan hasil face recognition yang sangat baik, bahkan pada jarak yang cukup jauh dan dalam kondisi pencahayaan yang kurang optimal. Hal ini menjadikan LBPH sebagai salah satu metode andalan dalam sistem keamanan berbasis face recognition yang memerlukan kinerja real-time dengan keterbatasan hardware, seperti kamera beresolusi rendah atau perangkat IoT.

(Pamungkas dkk., 2023) juga mencatat bahwa LBPH memiliki keunggulan dalam kecepatan komputasi, yang memungkinkan sistem untuk mengenali wajah dalam waktu kurang dari satu detik, menjadikannya ideal untuk aplikasi yang memerlukan respons cepat, seperti sistem presensi atau kontrol akses. Selain itu, LBPH lebih tahan terhadap variasi ekspresi wajah atau sudut pandang, yang sering kali menjadi tantangan dalam metode face recognition lainnya. Hal ini membuat LBPH menjadi solusi yang efisien dan dapat diandalkan dalam berbagai aplikasi keamanan, termasuk di laboratorium yang memerlukan kontrol akses yang ketat dan face recognition yang akurat. Oleh karena itu, LBPH tetap menjadi salah satu teknologi yang paling diandalkan dalam pengembangan sistem keamanan berbasis biometrik, terutama di lingkungan yang menuntut kinerja tinggi dan akurasi pengenalan.

2.3. Integrasi IoT dalam Sistem Keamanan

IoT dalam sistem keamanan laboratorium telah mengubah cara pengawasan dan monitoring keamanan dilakukan. IoT memungkinkan perangkat seperti kamera CCTV, sensor gerak, dan sistem kunci elektronik untuk terhubung melalui jaringan internet, menciptakan sistem keamanan yang cerdas dan terintegrasi. Hal ini memungkinkan pengelola laboratorium untuk memantau kondisi keamanan dari jarak jauh secara *real-time*.

Menurut (Sufian & Setiyadi, 2021), penerapan IoT dalam sistem keamanan ruangan memungkinkan perangkat-perangkat keamanan memberikan notifikasi otomatis saat ada aktivitas mencurigakan, sehingga pengelola dapat merespons dengan cepat terhadap potensi ancaman.

Keunggulan dari integrasi IoT ini terletak pada kemampuannya untuk menyimpan dan mengelola data secara otomatis di *cloud*, yang memungkinkan akses rekaman CCTV atau log aktivitas kapan saja melalui perangkat mobile. Selain itu, (Humam & Triawan, 2024) menyatakan bahwa penggunaan IoT dalam sistem keamanan dengan perangkat ESP32CAM dan sensor gerak memberikan fleksibilitas dalam monitoring keamanan secara jarak jauh serta efisiensi tinggi dalam pengelolaan keamanan. Sistem ini memungkinkan kontrol terhadap perangkat keamanan seperti kunci pintu atau alarm melalui aplikasi *mobile*. Dengan IoT, keamanan laboratorium menjadi lebih tanggap dan efisien, memungkinkan pengelola untuk melindungi aset penting dari ancaman potensial dengan cara yang lebih canggih dan mudah dioperasikan.

2.4. *Smart* CCTV Berbasis IoT untuk Monitoring *Real-Time*

Penggunaan *Smart* CCTV yang terintegrasi dengan teknologi IoT telah menjadi solusi yang sangat efektif untuk pengawasan keamanan di laboratorium. Sistem ini memungkinkan pengelola untuk memonitoring kondisi laboratorium secara *real-time* dari jarak jauh, menggunakan perangkat *mobile* seperti *smartphone* atau komputer.

Menurut (Satrio, 2022), *Smart* CCTV berbasis IoT mampu mendeteksi gerakan atau aktivitas mencurigakan dan mengirimkan notifikasi otomatis kepada pengelola, yang memungkinkan respons cepat terhadap potensi ancaman keamanan. Selain itu, sistem ini juga mendukung penyimpanan data di *cloud*, sehingga semua rekaman video dapat diakses kapan saja untuk analisis lebih lanjut. Hal ini memudahkan pengelola untuk memeriksa kembali kejadian yang terjadi di laboratorium tanpa harus berada di lokasi secara fisik.

(Samsinar dkk., 2023) menyatakan bahwa penggunaan *Smart* CCTV berbasis IoT juga memungkinkan integrasi dengan sensor lain, seperti sensor gerak atau sensor pintu, yang secara otomatis dapat memicu alarm jika ada aktivitas mencurigakan. Keunggulan utama dari *Smart* CCTV ini adalah kemampuannya untuk memberikan monitoring yang lebih efektif dan efisien, tanpa memerlukan pengawasan langsung dari operator manusia. Dengan adanya sistem ini, pengelola laboratorium dapat dengan mudah memantau dan mengamankan aset-aset penting dari ancaman, sekaligus mengurangi kebutuhan tenaga pengawas secara signifikan. Implementasi *Smart* CCTV berbasis IoT di laboratorium memberikan solusi monitoring yang fleksibel, responsif, dan efisien untuk menjaga keamanan fasilitas dan aset bernilai tinggi.

2.5. Quality of Service (QoS)

QoS adalah konsep penting dalam jaringan untuk memastikan performa layanan optimal, terutama untuk aplikasi yang membutuhkan transmisi data *real-time*, seperti komunikasi suara, video, atau sistem keamanan berbasis IoT. Salah satu parameter utama QoS adalah *delay*, yaitu waktu tunda saat data dikirim dari satu titik ke titik lain. *Delay* sangat krusial karena berdampak langsung pada kinerja aplikasi yang sensitif terhadap waktu. Dalam sistem pengawasan, misalnya, *delay* yang tinggi dapat menyebabkan keterlambatan pengiriman data, sehingga mengurangi efektivitas respons terhadap ancaman keamanan.

Menurut (Alzi & Haeruddin, 2022), QoS berfungsi untuk meminimalkan *delay* dengan memprioritaskan data kritis, seperti notifikasi keamanan, agar data tersebut dapat dikirim lebih cepat. Selain itu, QoS mengelola *delay* dengan mengoptimalkan jalur transmisi data guna menghindari kemacetan jaringan.

Sementara itu, (Fibriani dkk., 2020) menjelaskan bahwa dalam sistem berbasis IoT, pengelolaan *delay* sangat penting untuk memastikan data *real-time*, seperti gambar atau video dari kamera pengintai, tiba tanpa penundaan signifikan. Oleh karena itu, pengelolaan *delay* menjadi fokus utama dalam implementasi QoS, terutama pada aplikasi yang memerlukan respons cepat, seperti sistem keamanan IoT, yang membutuhkan transmisi data yang stabil dan tanpa gangguan untuk meningkatkan keandalan operasional (Setiawan dkk., 2023).

$$\text{Delay} = \frac{\text{Total Delay}}{\text{Total Paket yang diterima}} \quad (1)$$

Tabel 1. Delay standar TIPHON

Katagori Delay	Delay (ms)	Indeks
Sangat Bagus	<150	4
Bagus	150 – 300	3
Sedang	300 – 450	2
Jelek	>450	1

3. Metode

Penelitian ini bertujuan untuk mengembangkan dan menguji sistem keamanan laboratorium berbasis IoT yang menggunakan hardware berupa kamera ESP-32 CAM, *selenoid door lock*, dan mikrokontroler NodeMCU untuk kontrol akses masuk, serta kamera ESP-32 CAM untuk monitoring ruangan. Sistem ini didukung oleh konektivitas jaringan internet melalui *access point*, dengan aplikasi Telegram digunakan untuk notifikasi akses masuk, serta Firebase sebagai *platform* penyimpanan data berbasis *cloud*. Monitoring ruangan dilakukan secara *real-time* yang bisa diakses melalui *web browser* oleh pengelola laboratorium.

3.1. Desain Sistem

Sistem keamanan laboratorium ini memiliki dua fungsi utama: kontrol akses masuk dan monitoring ruangan. Untuk kontrol akses, digunakan satu buah kamera ESP-32 CAM yang dipasang di pintu laboratorium. Kamera ini berfungsi untuk mengambil citra wajah dari pengguna yang akan memasuki laboratorium. Data yang diambil oleh kamera dikirimkan langsung untuk diproses, dan jika akses diizinkan, *selenoid door lock* akan diaktifkan secara otomatis untuk membuka pintu. Seluruh proses ini didukung oleh jaringan internet melalui *access point*, yang memungkinkan komunikasi antar perangkat. Sementara itu, untuk monitoring ruangan, digunakan kamera ESP-32 CAM yang ditempatkan di dalam laboratorium. Kamera ini mengirimkan video secara *real-time* yang dapat diakses melalui web browser oleh pengelola laboratorium, memungkinkan monitoring kondisi ruangan laboratorium secara jarak jauh dan *real-time*.

3.1.1. Diagram Blok Sistem

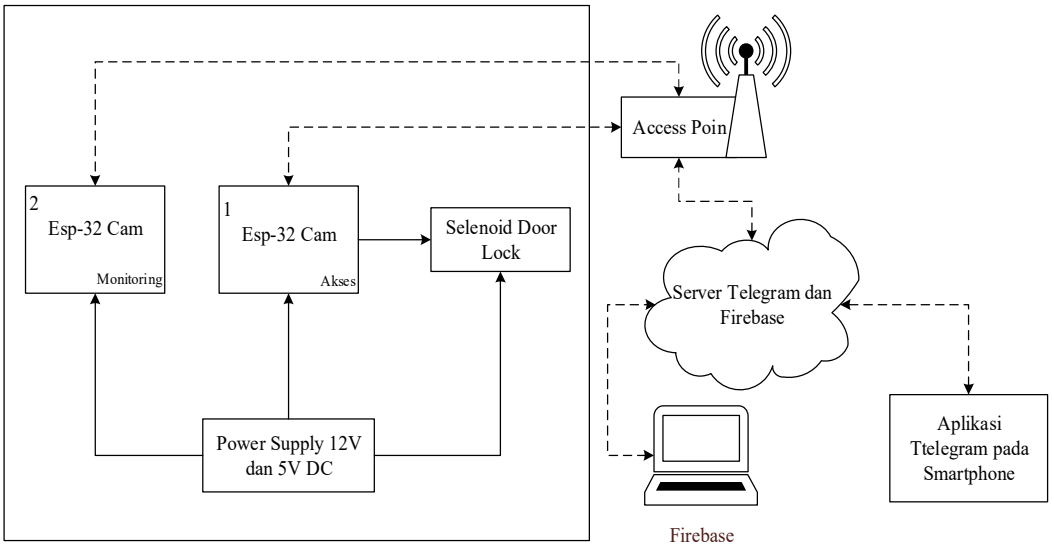
Pengembangan dimulai dengan membuat diagram blok sistem. Diagram blok sistem digunakan untuk menggambarkan hubungan antar komponen dalam sistem dalam bentuk blok atau kotak. Tujuan dari diagram ini adalah untuk memudahkan pengembangan dan pembuatan alat sehingga tercipta sebuah sistem yang sesuai dengan kebutuhan. Untuk integrasi secara *wire* ditunjukkan dengan garis yang berkesinambungan, sedangkan intergrasi secara *wireless* ditunjukkan dengan garis putus-putus pada Gambar 1.

Penjelasan dari diagram blok sistem diatas adalah sebagai berikut:

- *Power supply*, digunakan untuk memberikan sumber tegangan pada kedua ESP-32 CAM dan *selenoid door lock*.
- ESP32-CAM adalah modul kamera yang berbasis pada chip ESP32, yang merupakan mikrokontroler dengan konektivitas Wi-Fi dan Bluetooth. ESP32-CAM dilengkapi dengan kamera dan kemampuan untuk melakukan berbagai pemrosesan gambar dan video, serta komunikasi melalui internet menggunakan konektivitas Wi-Fi yang sudah ada pada modul ini. ESP-32 CAM 1 digunakan untuk kamera akses laboratorium. ESP-32 CAM 1 ini selaku kamera akses membandingkan citra hasil tangkapan kamera dengan *database* Firebase. Selanjutnya ESP-32 CAM 2 digunakan untuk monitoring di dalam ruangan laboratorium,

kamera ESP-32 CAM 2 tersebut mengirimkan video secara *real-time*, yang diakses menggunakan *web browser* dan hasil *recod* video akan disimpan pada SD *card*.

- *Selenoid door lock*, Merupakan kunci pintu elektrik berbasis selenoid yang dapat digunakan untuk membuat sistem keamanan. *Selenoid door lock* ini bekerja pada tegangan 12V dan didesain dengan lubang *mounting* untuk memudahkan saat pemasangan sekrup ke pintu.
- *Access point*, digunakan untuk menyediakan koneksi internet pada sistem.
- Aplikasi Telegram pada *smartphone*, digunakan untuk menerima notifikasi data akses laboratorium melalui jaringan internet
- Firebase berfungsi sebagai *database* yang menyimpan semua hasil pengambilan citra wajah dari kamera akses masuk untuk *face recognition*, memungkinkan penyimpanan data secara aman serta sinkronisasi informasi secara *real-time*.



Gambar 1. Diagram blok sistem

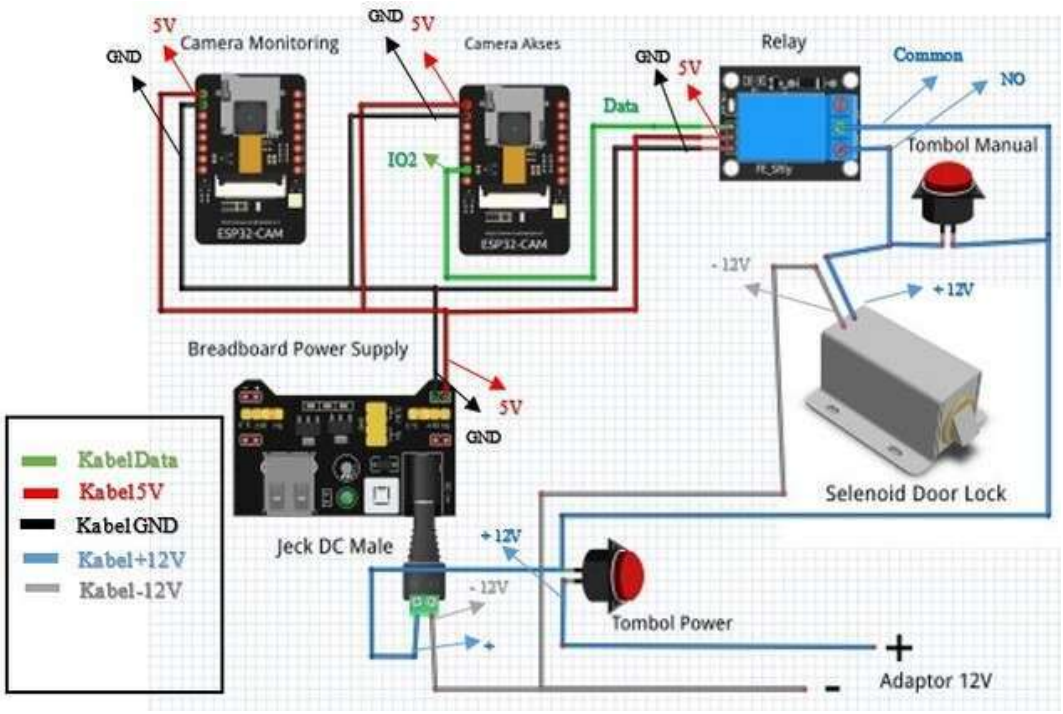
3.1.2. Perancangan Sistem Elektrik

Pada perancangan sistem elektrik, dilakukan perancangan pengkabelan dari komponen perangkat elektrik yang digunakan. ESP-32 CAM 1 berfungsi sebagai sistem akses ruangan, di mana hasil tangkapan citra wajah akan dikirimkan ke aplikasi Telegram dan juga memberikan notifikasi ke Telegram. Selain itu, tombol buka kunci dari dalam ruangan laboratorium berfungsi untuk menggerakkan *selenoid door lock* agar pintu dapat dibuka tanpa perlu melakukan pengambilan citra wajah. Selanjutnya untuk ESP-32 CAM 2 berfungsi sebagai perangkat monitoring ruangan. *Relay* 1 *channel* yang terhubung dengan *selenoid door lock* digunakan untuk mengunci pintu Laboratorium Teknik Elektro Universitas Qomaruddin. Gambar 2 memperlihatkan perancangan sistem elektrik yang telah dibuat.

Sambungan pin pada rangkaian sistem elektrik adalah sebagai berikut:

- Pin 5V ESP-32 CAM 2 pada kamera monitoring dihubungkan ke Pin 5V *Breadboard Power Supply*.
- Pin Gnd ESP-32 CAM 2 pada kamera monitoring dihubungkan ke Pin Gnd *Breadboard Power Supply*.
- Pin 5V ESP-32 CAM 1 pada kamera akses dihubungkan ke Pin 5V *Breadboard Power Supply*.
- Pin Gnd ESP-32 CAM 1 pada kamera akses dihubungkan ke Pin Gnd *Breadboard Power Supply*.
- Pin IO2 ESP-32 CAM 1 pada kamera akses dihubungkan ke Pin IN pada *relay*.

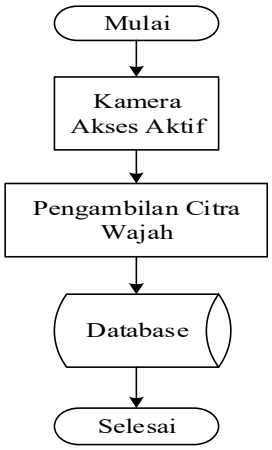
- Pin VCC *Relay* dihubungkan ke Pin + *Breadboard Power Supply*.
- Pin Gnd *Relay* dihubungkan ke Pin - *Breadboard Power Supply*.
- *Breadboard Power Supply* Jack DC Male + dihubungkan ke kaki *Push Bottom WithLock*, kaki satunya *Push Bottom WithLock* dihubungkan ke + *Adaptor* 12 Volt DC.
- *Breadboard Power Supply* Jack DC Male - dihubungkan ke - *Adaptor* 12 Volt DC.
- Kabel + *Selenoid Door Lock* dihubungkan ke Jack DC Male + dan *Push Bottom WithLock*.
- Kabel - *Selenoid Door Lock* dihubungkan ke Jack DC Male -
- Tombol Manual, untuk membuka *Selenoid Door Lock* dari dalam ruangan laboratorium tanpa harus *scan* wajah terlebih dahulu.



Gambar 2. Sambungan pin rancangan sistem elektrik

3.1.3. Pengembangan Software

Pengembangan *software* untuk rancang bangun sistem akses dan keamanan laboratorium menggunakan *face recognition* berbasis IoT merupakan bagian penting dalam mengoperasikan sistem akses dan keamanan Laboratorium Teknik Elektro Universitas Qomaruddin. Dalam perancangan *software* ini, diperlukan *flowchart* yang menggambarkan alur kerja sistem serta *software* yang akan digunakan untuk memastikan sistem dapat berfungsi secara optimal sesuai dengan spesifikasi yang dirancang.



Gambar 3. Flowchart input database

Penjelasan dari *flowchart* input *database* Gambar 3 sebagai berikut :

- Kamera Akses Aktif, pada tahap ini kamera aktif untuk memperoleh citra wajah personal yang sudah ditentukan untuk diberi izin akses ke laboratorium.
- Pengambilan Citra wajah, setiap individu setidaknya memiliki data wajah lebih dari satu untuk hasil yang lebih akurat, juga dikasih penamaan atau ID untuk pembeda setiap data wajah. Setiap satu wajah diambil 5 *sample*. Pengambilan citra wajah untuk *database* tidak harus menggunakan kamera ESP-32 CAM 1 bisa juga dengan kamera *smartphone* atau jenis kamera lainya.
- *Database*, tahap ini bertujuan untuk mengekstraksi data wajah dari citra guna membangun *database*. Proses ini memerlukan beberapa citra sebagai *database*, dengan data fitur wajah yang digunakan untuk membandingkan dan mengenali individu dalam citra. Fungsi *face*-API digunakan untuk mengunggah citra dan membangun database, di mana fungsi *detectSingleFace* berperan dalam mendeteksi wajah dari citra. Setelah itu, fitur wajah diekstraksi menggunakan *withFaceLandmarks* dan diubah menjadi deskripsi yang dapat dibaca melalui metode *withFaceDescriptor*. Selanjutnya, *faceMatcher* dibuat sebagai *instance* menggunakan konstruktor *FaceMatcher* dengan menyediakan semua data yang telah diekstraksi dari citra dalam *database*. Citra hasil tangkapan kamera akses ESP-32 CAM 1 kemudian akan dibandingkan dengan file sampel citra wajah yang tersimpan di *cloud database*.

Flowchart selanjutnya menjelaskan alur kerja sistem kamera akses dan kamera monitoring pada sistem keamanan laboratorium. Pada bagian kamera akses, alur dimulai dengan pengambilan citra wajah oleh kamera ESP-32 CAM 1 yang dipasang di pintu masuk. Citra yang diambil kemudian diproses, dan jika wajah pengguna sesuai dengan data yang tersimpan, pintu akan terbuka otomatis melalui *selenoid door lock*. Sistem juga mengirimkan notifikasi ke aplikasi Telegram untuk memberi tahu pengelola bahwa akses telah diberikan. Sementara itu, pada bagian kamera monitoring, kamera ESP-32 CAM 2 di dalam laboratorium bekerja secara terus-menerus dengan mengirimkan video secara *real-time* ke web pengelola melalui koneksi internet.

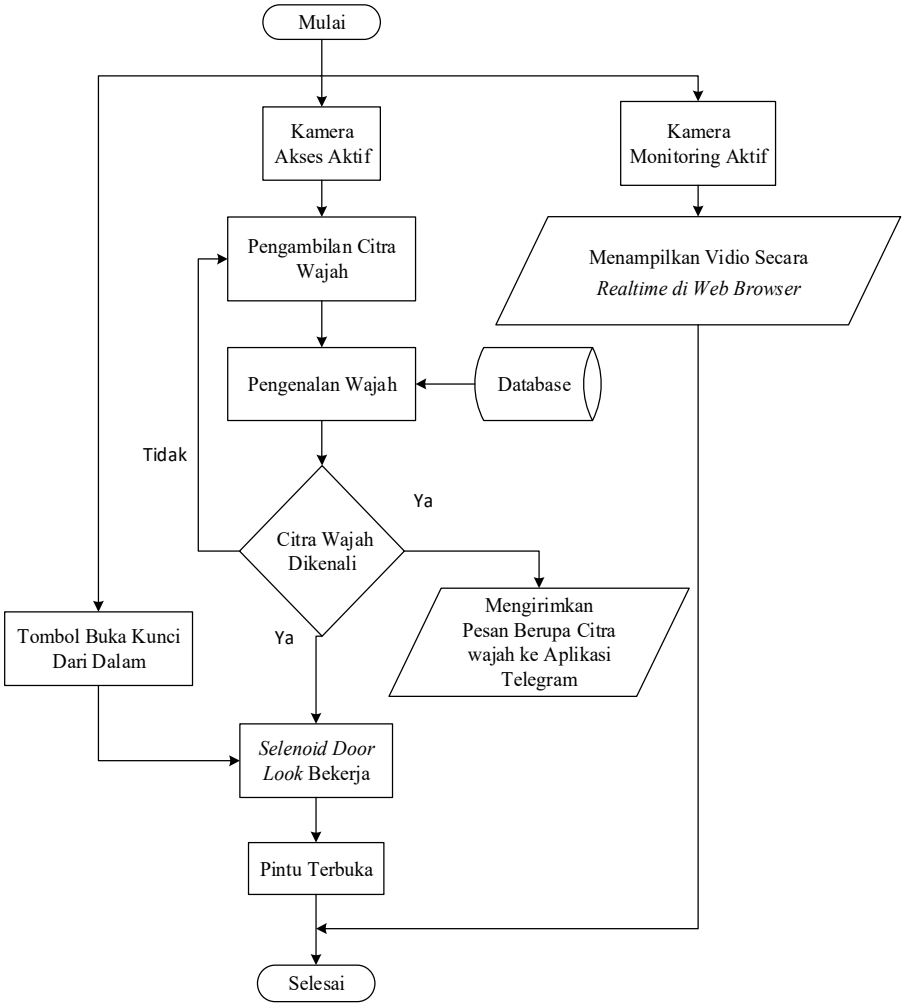
Penjelasan dari *flowchart* cara kerja sistem yang dirancang pada Gambar 4 adalah sebagai berikut:

- Kamera Akses Aktif, pada tahap ini kamera dinyalakan, sistem akan terus menerus atau secara *real-time* melakukan pendeteksian. Apabila sistem mendeteksi adanya wajah manusia maka kamera ESP-32 CAM 1 akan menangkap citra wajah tersebut.
- Pengambilan Citra Wajah, pada tahap ini sistem menangkap citra wajah yang mendekati kamera akses, sistem akan mengenali wajah tersebut.
- Pengenalan Wajah, sistem akan mencocokkan citra yang ditangkap dengan data yang tersimpan di *database*. Jika citra yang ditangkap dan diproses tidak cocok dengan data di *database*, pintu akan tetap dalam kondisi tertutup. Namun, jika citra yang diproses cocok dengan data di *database*,

selenoid door lock akan membuka pintu, dan notifikasi berupa gambar akan dikirimkan melalui aplikasi Telegram.

- Kamera Monitoring Aktif, pada tahap ini kamera monitoring aktif secara real-time berbasis Iuntuk memonitoring ruangan Laboratorium Dasar Elektronika.
- Menampilkan Video Secara *Real-time* di *Web Browser*, tahap ini kamera monitoring menampilkan vidio secara *real-time* di web pengelolah Laboratorium Teknik Elektro Universitas Qomaruddin.
- Tombol Kunci dari Dalam, pada tahap ini tombol digunakan untuk membuka kunci dari dalam ruangan laboratorium tanpa harus mengambil citra wajah dari kamera akses ESP-32 CAM 1.

Pengembangan *software* dalam sistem ini dilakukan menggunakan Arduino IDE, yang berfungsi untuk memprogram *hardware* ESP-32 CAM. Selain itu, konfigurasi juga perlu dilakukan pada Firebase, *platform cloud* yang digunakan untuk pengelolaan *database* citra wajah. Firebase diatur untuk menyimpan data hasil pengambilan citra dan memfasilitasi integrasi dengan *hardware* untuk mendukung pemrosesan data secara *real-time*. Di samping itu, konfigurasi pada aplikasi Telegram juga diperlukan untuk mengaktifkan fitur notifikasi, sehingga setiap akses yang berhasil atau tidak berhasil akan mengirimkan pemberitahuan otomatis ke pengguna melalui Telegram, memastikan pengelola selalu mendapat informasi terkait status keamanan laboratorium.

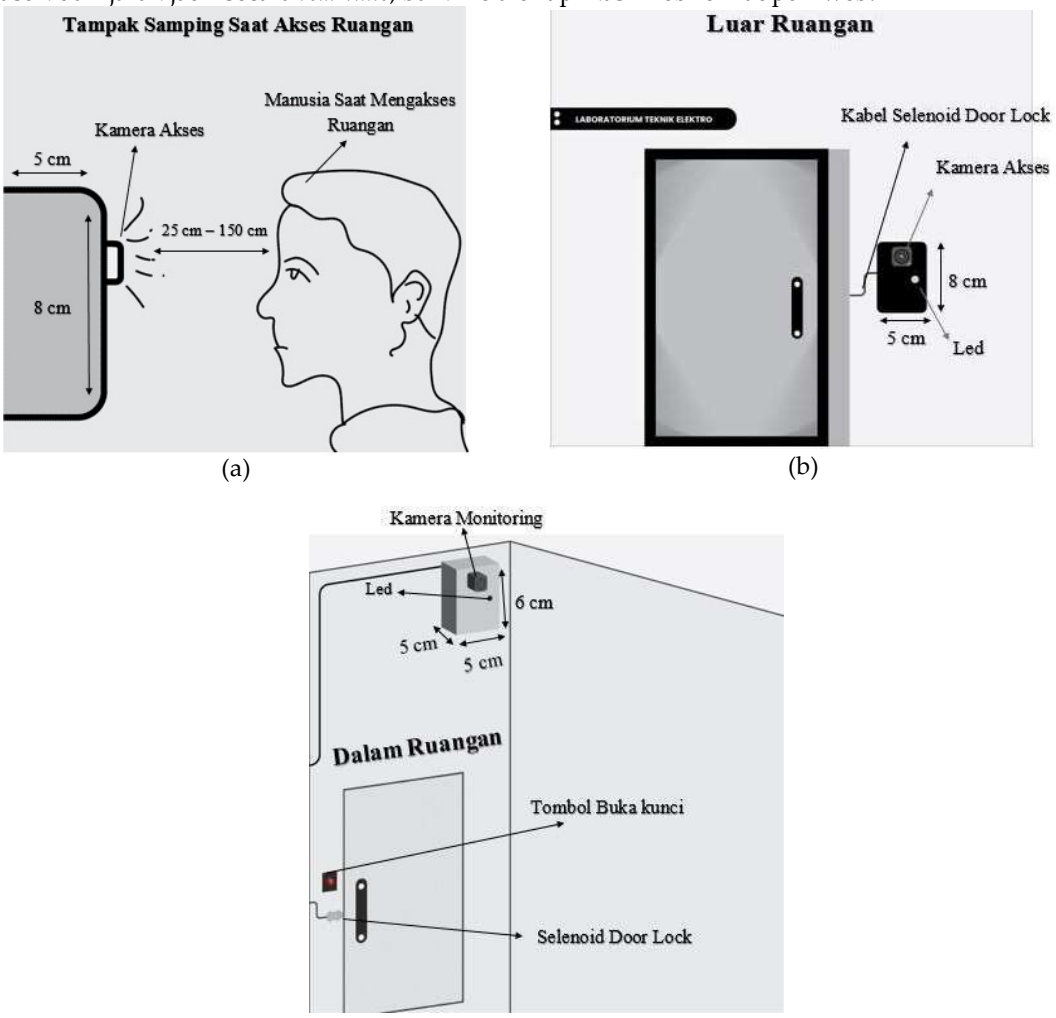


Gambar 4. *Flowchart* cara kerja sistem yang dirancang

3.2. Implementasi Sistem

Implementasi sistem dilakukan dengan mengintegrasikan seluruh *hardware* dan *software* yang mendukung sistem keamanan laboratorium berbasis IoT. Kamera ESP-32 CAM 1 yang digunakan untuk akses masuk dipasang di pintu laboratorium untuk mengambil citra wajah pengguna. Setelah citra wajah diambil, data akan diproses dan disimpan di Firebase, *platform cloud* yang berfungsi sebagai *database* untuk menyimpan hasil pengambilan citra. Selain itu, kamera ESP-32 CAM 2 ditempatkan di dalam laboratorium untuk keperluan monitoring, yang mengirimkan video secara *real-time* ke web pengelola laboratorium melalui koneksi internet.

Aplikasi Telegram dikonfigurasi untuk mengirimkan notifikasi otomatis kepada pengelola setiap kali ada upaya akses ke laboratorium. Dengan memanfaatkan konektivitas internet melalui *access point*, sistem ini memungkinkan pengelola untuk memantau aktivitas di laboratorium dan mengelola akses masuk dari jarak jauh secara *real-time*, baik melalui aplikasi mobile maupun web.



Gambar 5. Rencana penempatan sistem: (a) Kamera akses tampak samping; (b) Kamera akses ditempatkan di depan pintu laboratorium; (c) Kamera monitoring, selenoid door lock, dan tombool buka kunci dari dalam ruangan laboratorium.

3.2.1. Pengujian Kontrol Akses Masuk dan Delay Pengiriman Notifikasi

Pengujian dilakukan untuk memastikan kamera ESP-32 CAM 1 di pintu laboratorium mampu menangkap citra wajah pengguna dengan baik. Lima peserta diuji dengan mencocokkan citra wajah

mereka ke database Firebase untuk menentukan akses masuk. Hasilnya menunjukkan keakuratan sistem dalam mengenali wajah dan memastikan pintu hanya terbuka bagi individu yang terdaftar.

Pengujian delay notifikasi melalui Telegram dilakukan untuk mengevaluasi kecepatan pengiriman informasi real-time terkait upaya akses, baik berhasil maupun gagal. Hal ini memastikan sistem memberikan respons cepat untuk mendukung pemantauan segera..

(a)

(b)

Gambar 6. Realisasi penempatan sistem: (a) Kamera akses ditempatkan di depan pintu laboratorium; (b) Selenoid door lock, dan tombool buka kunci dari dalam ruangan laboratorium; (c) Kamera monitoring ditempatkan di dalam ruangan laboratorium.

3.2.2. Pengujian Monitoring Ruangan

Pengujian selanjutnya dilakukan pada sistem monitoring ruangan laboratorium untuk mengevaluasi kinerja kamera ESP-32 CAM 2 yang ditempatkan di dalam laboratorium. Pengujian ini masih terbatas pada memastikan apakah monitoring video dapat ditampilkan secara *real-time* melalui koneksi internet. Kamera diuji untuk melihat apakah video dapat dikirimkan dan ditampilkan secara langsung di web pengelola laboratorium. Hasil dari pengujian ini memungkinkan pengelola untuk memantau kondisi laboratorium dari jarak jauh secara *real-time*.

4. Hasil dan Pembahasan

Hasil pengujian dipaparkan berdasarkan dua aspek utama, yaitu kontrol akses masuk yang menggunakan kamera ESP-32 CAM 1 dan *delay* pengiriman notifikasi, serta monitoring ruangan menggunakan kamera monitoring ESP-32 CAM 2.

4.1. Hasil Pengujian Kontrol Akses Masuk dan *Delay* Pengiriman Notifikasi

Pengujian kontrol akses masuk dilakukan dengan melibatkan lima orang sebagai sampel untuk mengevaluasi kinerja kamera ESP-32 CAM 1 yang dipasang di pintu laboratorium. Hasil pengujian menunjukkan bahwa kamera mampu menangkap citra wajah pengguna dengan baik, yang kemudian dibandingkan dengan data yang tersimpan di *database* Firebase. Secara umum, sistem berhasil mengenali wajah pengguna dengan akurasi yang tinggi, dan akses hanya diberikan kepada individu yang terdaftar dalam database. Namun, pada uji coba untuk orang ke-3, terjadi dua kali kesalahan pengenalan wajah, di mana citra yang diambil dikenali sebagai orang lain sehingga akses ditolak. Hal ini disebabkan oleh jarak yang terlalu jauh dan pandangan yang tidak diarahkan langsung ke kamera, yang memengaruhi akurasi sistem.

Pada empat sampel lainnya, sistem mampu mengenali wajah dengan benar dan memberikan akses sesuai dengan data yang tersimpan di *database*. Hal ini menunjukkan bahwa sistem berfungsi dengan baik dalam kondisi yang optimal. Namun, faktor eksternal seperti jarak dan sudut pandang pengguna perlu diperhatikan untuk memastikan kinerja sistem yang lebih akurat. Hasil pengujian kontrol akses ini dirangkum dalam tabel 2 hingga tabel 6, yang mencakup detail akurasi pengenalan wajah dan respons sistem terhadap upaya akses. Berdasarkan evaluasi tersebut, dapat disimpulkan bahwa sistem kontrol akses berfungsi sesuai perancangan dengan tingkat akurasi yang memadai untuk digunakan dalam skenario nyata.

Pengujian *delay* pengiriman notifikasi melalui aplikasi Telegram juga menunjukkan hasil yang memuaskan. Notifikasi otomatis terkait upaya akses masuk, baik yang berhasil maupun yang gagal, berhasil diterima oleh pengelola laboratorium secara *real-time*. Pengujian ini mengukur waktu pengiriman notifikasi menggunakan aplikasi Wireshark, di mana data delay diambil sebanyak 10 kali uji coba. Rata-rata *delay* yang didapatkan dari pengujian ini adalah 18,528 ms, dengan notifikasi terkirim dalam waktu kurang dari 1 detik setelah upaya akses dilakukan. Hal ini membuktikan bahwa sistem mampu memberikan respons cepat dalam situasi yang memerlukan pemantauan segera, seperti upaya akses yang tidak diizinkan.

Tabel 2. Hasil pengujian kontrol akses masuk orang pertama

Citra wajah orang ke 1 di *database*	Citra hasil *face recognition* dengan pengujian sebanyak 10 kali	Jumlah izin akses masuk yang diberikan sistem	
		Dikenali, akses diizinkan	Tidak dikenali, akses ditolak
	1  2  3  4  5 	10	0
	6  7  8  9  10 		

Tabel 3. Hasil pengujian kontrol akses masuk orang kedua

Citra wajah orang ke 2 di *database*	Citra hasil *face recognition* dengan pengujian sebanyak 10 kali		Jumlah izin akses masuk yang diberikan sistem	
			Dikenali, akses diizinkan	Tidak dikenali, akses ditolak
	1 	6 	10	0
	2 	7 		
	3 	8 		
	4 	9 		
	5 	10 		

Tabel 4. Hasil pengujian kontrol akses masuk orang ketiga

Citra wajah orang ke 3 di *database*	Citra hasil *face recognition* dengan pengujian sebanyak 10 kali	Jumlah izin akses masuk yang diberikan sistem	
		Dikenali, akses diizinkan	Tidak dikenali, akses ditolak
	1  2  3  4  5 	8	2
	6  7  8  9  10 		

Tabel 5. Hasil pengujian kontrol akses masuk orang ke 4

Citra wajah orang ke 4 di *database*	Citra hasil *face recognition* dengan pengujian sebanyak 10 kali	Jumlah izin akses masuk yang diberikan sistem	
		Dikenali, akses diizinkan	Tidak dikenali, akses ditolak
	1  2  3  4  5 	10	0
	6  7  8  9  10 		

Tabel 6. Hasil pengujian kontrol akses masuk orang ke 5

Citra wajah orang ke 4 di *database*	Citra hasil *face recognition* dengan pengujian sebanyak 10 kali	Jumlah izin akses masuk yang diberikan sistem	
		Dikenali, akses diizinkan	Tidak dikenali, akses ditolak
	1  2  3  4  5 	6  7  8  9  10 	10	0

Tabel 7. *Delay* pengiriman notifikasi ke aplikasi Telegram uji coba ke 1

No.	*Delay* 1 (s)	*Delay* 2 (s)	*Delay* 2 – *Delay* 1 (ms)
1	0	0	0
2	0	0	0
3	0,002712	0	0,00271
4	0,002712	0,002712	0
5	0,005321	0,002712	0,00261
6	0,005321	0,005321	0
7	0,005321	0,005321	0
8	0,005321	0,005321	0
9	0,006819	0,005321	0,0015
10	0,010614	0,006819	0,0038
11	0,010614	0,010614	0
12	0,011589	0,010614	0,00098
13	0,011589	0,011589	0
14	0,013667	0,011589	0,00208
15	0,015377	0,013667	0,00171
…	…	…	…
613	8.732.899	8.728.999	3900
614	8.972.513	8.732.899	239614
	Total *Delay*		8972513
	Rata-rata *Delay*		14589,5

$$\text{rata-rata delay} = \frac{\sum \text{delay 2} - \sum \text{delay1}}{\text{jumlah paket didapat}}$$

$$= \frac{8972513 \text{ ms}}{615}$$

$$= 14589{,}5 \text{ ms}$$

$$= \frac{14589{,}5 \text{ ms}}{1000}$$

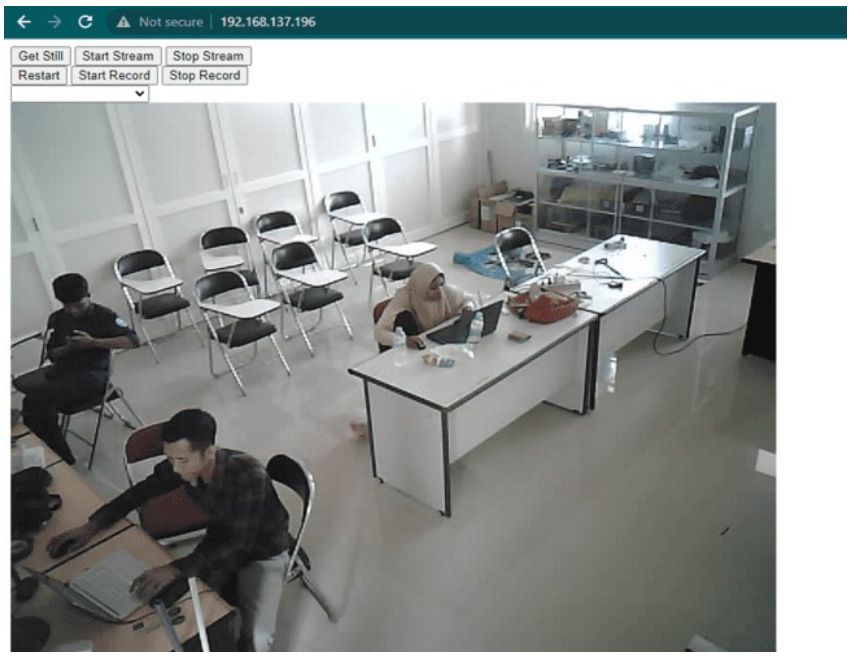
$$= 14{,}58945 \text{ ms}$$

Tabel 8. Hasil pengujian *delay* pengiriman notifikasi ke aplikasi Telegram secara keseluruhan

Uji coba ke -	Rata-rata *delay* (ms)	Uji coba ke -	Rata-rata *delay* (ms)
1	14,59	6	10,09
2	36,23	7	35,6
3	9,95	8	44,67
4	4,26	9	3,85
5	24,12	10	1,92
Total		185,28	
Rata-rata *Delay*		**18,528**	

4.2. Hasil Pengujian Monitoring Ruangan

Hasil pengujian sistem monitoring ruangan laboratorium menunjukkan bahwa kamera ESP-32 CAM 2 yang ditempatkan di dalam laboratorium mampu mengirimkan video secara *real-time* melalui koneksi internet. Pengujian ini dilakukan untuk memastikan bahwa video monitoring dapat ditampilkan secara langsung di web pengelola laboratorium tanpa adanya gangguan atau keterlambatan yang signifikan. Berdasarkan hasil pengujian, video berhasil dikirimkan dan ditampilkan dengan baik di web, sehingga memungkinkan pengelola untuk memantau kondisi laboratorium dari jarak jauh secara *real-time*.



Gambar 7. Tampilan Tampilan monitoring ruangan laboratorium pada web browser

Namun, pengujian ini masih terbatas pada penilaian apakah video dapat ditampilkan secara *real-time* atau tidak, tanpa analisis lebih lanjut terkait kualitas video atau kecepatan *streaming* dalam kondisi jaringan yang berbeda. Secara keseluruhan, hasil ini menunjukkan bahwa sistem monitoring ruangan berfungsi sesuai dengan perancangan, memberikan pengelola kemampuan untuk melakukan pemantauan jarak jauh secara efektif dan terus menerus.

4.3. Pembahasan

Hasil pengujian menunjukkan bahwa sistem keamanan laboratorium berbasis IoT berfungsi sesuai dengan perancangan. Pengujian kontrol akses menunjukkan bahwa kamera ESP-32 CAM 1 mampu menangkap citra wajah pengguna dengan akurasi yang cukup tinggi. Namun, faktor eksternal seperti jarak dan sudut pandang memengaruhi hasil pengenalan wajah. Pada uji coba individu ke-3, terjadi kesalahan pengenalan akibat jarak yang terlalu jauh dan posisi pemindaian yang kurang optimal. Hal ini menegaskan bahwa sistem bekerja lebih baik jika jarak dan posisi pemindaian diperhatikan. Secara keseluruhan, sistem menunjukkan kinerja memadai, di mana akses diberikan hanya kepada individu yang terdaftar di database, dengan hasil pengujian yang konsisten.

Pengujian delay pengiriman notifikasi melalui aplikasi Telegram menunjukkan performa yang memuaskan. Rata-rata delay sebesar 18,528 ms memastikan notifikasi terkirim dalam waktu kurang dari 1 detik setelah upaya akses dilakukan. Respons cepat ini memastikan pengelola laboratorium mendapatkan informasi real-time tentang upaya akses, baik yang berhasil maupun gagal, sehingga memungkinkan tindakan segera dalam situasi kritis.

Sementara itu, pengujian monitoring ruangan menunjukkan bahwa kamera ESP-32 CAM 2 mampu mengirimkan video secara *real-time* tanpa gangguan signifikan. Video berhasil ditampilkan di web pengelola laboratorium, memungkinkan pemantauan jarak jauh yang efektif. Meskipun pengujian ini belum mencakup analisis mendalam tentang kualitas video atau kecepatan streaming dalam berbagai kondisi jaringan, hasil awal menunjukkan sistem berfungsi dengan baik sebagai solusi pemantauan laboratorium secara real-time.

Sistem yang dikembangkan menunjukkan peningkatan signifikan dibandingkan sistem serupa, terutama dalam hal kecepatan notifikasi, dengan delay rata-rata 18,528 ms, lebih cepat dari rata-rata 30 ms pada sistem lain. Implementasi sistem pengenalan wajah dan notifikasi real-time memungkinkan pengelola laboratorium memantau akses ruangan secara otomatis tanpa keterlibatan langsung, sehingga menghemat waktu dan tenaga serta meminimalkan kesalahan manusia.

Potensi penerapan sistem ini tidak hanya terbatas pada laboratorium. Teknologi ini dapat diadaptasi untuk sektor lain, seperti perkantoran atau industri, yang membutuhkan standar keamanan tinggi. Integrasi antara pengenalan wajah dan notifikasi instan menjadikan sistem ini solusi keamanan yang efisien, mudah diimplementasikan, dan sangat sesuai untuk berbagai jenis fasilitas.

5. Kesimpulan

Berdasarkan hasil pengujian yang telah dilakukan, Sistem keamanan laboratorium berbasis IoT dengan kamera ESP-32 CAM, Firebase, dan Telegram berhasil memenuhi tujuan perancangan. Sistem kontrol akses mengenali wajah pengguna dengan akurasi baik, meski ada beberapa kesalahan akibat jarak dan sudut pandang. Pengujian *delay* pengiriman notifikasi menunjukkan bahwa notifikasi dikirim secara *real-time* dengan rata-rata *delay* sebesar 18,528 ms, memastikan respons cepat terhadap upaya akses masuk.

Sistem monitoring laboratorium menunjukkan kinerja optimal dengan kamera ESP-32 CAM 2 yang mampu mengirimkan video real-time ke web pengelola tanpa gangguan signifikan. Fitur ini memberikan akses visual langsung, memungkinkan pengawasan keamanan secara efektif kapan saja tanpa perlu berada di lokasi fisik.

Secara keseluruhan, sistem keamanan ini telah menunjukkan performa yang baik dan siap untuk diimplementasikan dalam skenario nyata. Beberapa faktor seperti posisi dan jarak pengguna saat pemindaian wajah perlu diperhatikan untuk memastikan kinerja yang optimal. Dengan sedikit peningkatan, sistem ini dapat menjadi solusi yang andal untuk menjaga keamanan laboratorium berbasis IoT secara efisien dan *real-time*.

Untuk pengembangan sistem di masa depan, pengujian lebih lanjut di kondisi pencahayaan yang sangat rendah atau saat pengguna mengenakan masker dapat dilakukan untuk meningkatkan tingkat akurasi. Selain itu, algoritma pengenalan wajah bisa lebih dioptimalkan untuk mengurangi kesalahan dalam situasi non-ideal. Salah satu keterbatasan penelitian ini adalah penggunaan hanya satu metrik (*delay* notifikasi) untuk menilai performa sistem. Ke depannya, penilaian terhadap faktor lain seperti tingkat akurasi, ketahanan sistem terhadap gangguan, dan kepuasan pengguna perlu dilakukan untuk memberikan gambaran yang lebih komprehensif tentang kinerja sistem.

Ucapan Terima Kasih

Kami mengucapkan terima kasih yang sebesar-besarnya kepada rekan-rekan sejawat serta para mahasiswa di Program Studi Teknik Elektro, Universitas Qomaruddin, atas dukungan, kerja sama, dan kontribusi yang sangat berharga dalam penelitian ini. Bantuan dan dedikasi yang diberikan telah berperan penting dalam penyelesaian artikel ini dengan baik.

Pernyataan Konflik Kepentingan

Para penulis menyatakan tidak ada potensi konflik kepentingan terkait dengan penelitian, penulisan, dan/atau publikasi dari artikel ini.

Daftar Pustaka

Alzi, A., & Haeruddin, H. (2022). Pengaruh manajemen bandwidth terhadap QoS dengan standar TIPHON pada alur monitoring SNMP. Jurnal Ilmiah Teknologi Informasi Asia. Retrieved from https://jurnal.stmikasia.ac.id/index.php/jitika/article/view/883

Bachtiar, A. H. (2022). Rancang bangun dual keamanan sistem pintu rumah menggunakan pengenalan wajah dan sidik jari berbasis IoT (Internet of Things). Power Elektronik: Jurnal Orang Elektro, 11(1), Article 1. https://doi.org/10.30591/polektro.v11i1.3137

Fibriani, I., Widjonarko, Bayu, A., & Ciptaning, P. (2020). Analisa sistem monitoring greenhouse berbasis Internet of Things (IoT) pada jaringan 4G LTE. SinarFe7, 3(1), Article 1. Retrieved from https://journal.fortei7.org/index.php/sinarFe7/article/view/295

Humam, F., & Triawan, M. A. (2024). Sistem keamanan ruangan menggunakan ESP32CAM dan sensor gerak berbasis IoT. Infotek: Jurnal Informatika dan Teknologi, 7(2), Article 2. https://doi.org/10.29408/jit.v7i2.26109

Murjitama, F. L., Raihan, H. N., Adiwijaya, R. P., Ramadan, D. F., Pasaribu, B. I., Silalahi, B. A., Tasman, N. N., Dwijayanti, S. A., Panjaitan, U. P. S., & Purwanto, Y. S. (2024). The smart door lock using face recognition access based on Internet of Things (IoT). Teknika, 13(2), Article 2. https://doi.org/10.34148/teknika.v13i2.816

Pamungkas, R., Wahiddin, D., & Mudzakir, T. (2023). Sistem presensi pegawai menggunakan face recognition dengan algoritma Local Binary Pattern Histogram (LBPH). Scientific Student Journal for Information, Technology and Science, 4(1), Article 1

Rama, G. A., Fauziah, F., & Nurhayati, N. (2020). Perancangan sistem keamanan brangkas menggunakan pengenalan wajah berbasis Android. Jurnal Media Informatika Budidarma, 4(3), Article 3. https://doi.org/10.30865/mib.v4i3.2149

Samsinar, R., Aditya, G. G., Almanda, D., Fadliondi, F., Amrulloh, F., & Ramadhan, A. I. (2023). Sistem pendeteksi kurir menggunakan smart closed circuit television (CCTV) berbasis Internet of Things (IoT) dengan media komunikasi bot Telegram (Studi Kasus: Rumah Indekost). RESISTOR (Elektronika Kendali Telekomunikasi Tenaga Listrik Komputer), 6(1), 47-54.
https://doi.org/10.24853/resistor.6.1.47-54

Santoso, A. W. (2020). Sistem keamanan pintu laboratorium berbasis sensor fingerprint dan magnetic lock. JTT (Jurnal Teknologi Terapan, 6(1), Article 1. https://doi.org/10.31884/jtt.v6i1.236

Satrio, B. (2022). Sistem keamanan rumah berbasis IoT dengan Arduino dan kamera CCTV. Jurnal Repoteknologi, 2(11)

Setiawan, A., Hutauruk, G. P. P., & Aisyah, T. (2023). Prototipe kelas pintar dengan absensi otomatis MAC address gawai berbasis IoT. INSOLOGI: Jurnal Sains dan Teknologi, 2(1), Article 1. https://doi.org/10.55123/insologi.v2i1.1400

Sufian, S., & Setiyadi, D. (2021). Sistem keamanan pada ruangan server menggunakan teknologi berbasis Internet of Things dan aplikasi Blynk. Informatics for Educators and Professionals: Journal of Informatics, 5(2), 186–195. https://doi.org/10.51211/itbi.v5i2.1543

Sunardi, S., Yudhana, A., & Talib, M. A. (2022). Perancangan sistem pengenalan wajah untuk keamanan ruangan menggunakan metode Local Binary Pattern Histogram. Jurnal Teknologi Elektro, 13(2), 123–129. https://doi.org/10.22441/jte.2022.v13i2.010

Suryansah, A., Habibi, R., Awangga, R. M., & Fatonah, R. N. S. (2020). Implementasi face recognition untuk mengakses ruangan. Jurnal MediaTIK, 25–28.

Syafutra, H., Aziz, T. M. N., Novianty, I., Irmansyah, I., Chusnu, M., & Prayoga, D. (2024). Implementasi sistem keamanan pintu otomatis berbasis face recognition di Proactive Robotic: Integrasi ESP32-Cam dan Telegram. Jurnal Riset Fisika Indonesia, 4(2), Article 2. https://doi.org/10.33019/jrfi.v4i2.5380