JITET (Jurnal Informatika dan Teknik Elektro Terapan)
Vol. 14 No. 1, pISSN: 2303-0577 eISSN: 2830-7062 http://dx.doi.org/10.23960/jitet.v14i1.8826

SMART LOCK SYSTEM BERBASIS IOT MENGGUNAKAN ESP32 UNTUK KEAMANAN AKSES PUSAT DATA (STUDI KASUS: UPA TIK UNDIKSHA)

Made Waradiana Aryadi[1*], I Ketut Resika Arthana[2], Putu Hendra Suputra[3]

[1,2,3] Jurusan Teknik Informatika, Fakultas Teknik dan Kejuruan Universitas Pendidikan Ganesha; Jl. Udayana No. 11, Singaraja, Bali 81116; Telp/Fax (0362) 22570

Keywords:
Pusat data; *Smart lock system*; ESP32; MQTT; Pendaftaran pengguna.

Corespondent Email:
waradiana@undiksha.ac.id

Abstrak. Keamanan fisik pusat data berperan penting dalam menjamin keberlangsungan layanan teknologi informasi dari ancaman akses tidak sah dan tindakan kriminal. Pusat data UPA TIK Universitas Pendidikan Ganesha telah menerapkan sistem pengamanan dasar, namun masih menghadapi keterbatasan pada aspek pemantauan *real-time*, notifikasi otomatis, dan pengelolaan akses pengguna. Penelitian ini bertujuan merancang dan mengembangkan *smart lock system* berbasis *Internet of Things* menggunakan ESP32 guna meningkatkan keamanan akses fisik pusat data. Sistem yang dikembangkan mengintegrasikan autentikasi RFID dan sidik jari, komunikasi antar perangkat melalui protokol MQTT, sensor *magnetic door switch* untuk mendeteksi akses ilegal, serta notifikasi *real-time* melalui bot Telegram. Sistem juga dilengkapi fitur pendaftaran pengguna secara dinamis tanpa perlu pemrograman ulang perangkat. Metode penelitian yang digunakan adalah *Research and Development*. Hasil pengujian menunjukkan seluruh fungsi sistem berjalan sesuai spesifikasi dengan rata-rata *latency* sekitar 4 detik dan tingkat keberhasilan autentikasi 100%. RFID menawarkan respons yang cepat dan stabil namun memiliki risiko duplikasi dan kehilangan kartu, sedangkan sidik jari memberikan keamanan lebih tinggi meskipun *latency*-nya bervariasi. Secara keseluruhan, sistem ini mampu meningkatkan keamanan fisik pusat data secara terintegrasi dan responsif.

Abstract. *Physical security is a critical aspect in ensuring the continuity of information technology services against unauthorized access and criminal threats. The UPA TIK data center at Ganesha University of Education has implemented a basic security mechanism; however, it still lacks real-time monitoring, automatic notification, and efficient access management. This study aims to design and develop an IoT-based smart lock system using ESP32 to enhance data center access security. The proposed system integrates RFID and fingerprint authentication, MQTT-based inter-device communication, magnetic door switch sensors for illegal access detection, and real-time notifications via a Telegram bot. Additionally, a dynamic user enrollment feature is implemented, allowing user registration without device reprogramming. The research adopts the Research and Development method. Testing results indicate that all system functions operate as specified, achieving an average latency of 4 seconds and a 100% authentication success rate. RFID authentication offers faster and more stable response times but is vulnerable to card duplication and loss, whereas fingerprint authentication provides higher security due to its biometric nature despite latency variations. Overall, the system effectively enhances physical data center security in an integrated and responsive manner.*

1. PENDAHULUAN

Pusat data merupakan fasilitas penting sebagai pusat pengelolaan informasi, penyimpanan, dan distribusi data yang menampung perangkat kritis seperti server, *router*, dan *switch* yang mendukung operasi teknologi informasi. Ruangan ini harus dilengkapi pengamanan fisik maupun non-fisik, termasuk pengaturan akses pengguna dan manajemen keamanan sistem [1]. Pusat data harus menerapkan sistem keamanan ketat untuk melindungi aset dari berbagai ancaman yang berpotensi menyebabkan kehilangan atau kerusakan [2]. Kehilangan perangkat dapat menimbulkan kerugian material dan penyebab *downtime* global sebesar 25% [3], sehingga berdampak pada citra instansi, kepuasan pengguna, dan pendapatan.

Ancaman ini dapat timbul akibat penyalahgunaan kredensial atau tindak akses paksa oleh pihak tidak berwenang yang berpotensi menyebabkan perusakan, pencurian perangkat, maupun mengakses untuk merusak sistem. Kasus serupa terjadi pada PT XL Axiata Makasar pada April 2024, perangkat penting seperti *Quad Small Formfactor Pluggable* (QSFP) dicuri oleh oknum yang menyalah gunakan akses kerjanya [4].

Sejalan dengan pentingnya perlindungan pusat data di Universitas Pendidikan Ganesha (Undiksha), melalui Unit Penunjang Akademik, Teknologi dan Informasi (UPA TIK) yang bertanggung jawab atas pengembangan, pengelolaan, dan pelayanan teknologi informasi serta sistem jaringan yang menjadi fondasi berbagai layanan akademik dan operasional universitas, termasuk sistem informasi akademik, layanan kepegawaian, akses internet, dan berbagai platform teknologi yang digunakan oleh sivitas akademika [5]. Sebagai pusat penyimpanan dan pengelolaan data penting universitas, keamanan pusat data menjadi prioritas utama untuk memastikan layanan tetap optimal dan terhindar dari gangguan. Saat ini, pusat data UPA TIK telah dilengkapi sistem penguncian sidik jari dan kamera pengawas komersial sebagai sistem keamanan dasar, namun perangkat tersebut masih bersifat *stand-alone* masih memiliki keterbatasan, seperti tidak mendukung *monitoring* akses *real-time*, tidak menyediakan notifikasi otomatis, dan belum mampu mendeteksi langsung upaya pembobolan. Keterbatasan ini menimbulkan celah keamanan yang berpotensi dimanfaatkan pihak tidak berwenang, sehingga diperlukan sistem pengamanan yang lebih adaptif, terintegrasi, dan responsif dalam mendeteksi serta menangani risiko terkait akses ilegal ke pusat data.

Berkaitan dengan hal tersebut, penelitian ini bertujuan untuk merancang dan membangun sistem penguncian pintar berbasis *Internet of Things* (IoT) untuk meningkatkan keamanan akses pusat data UPA TIK Undiksha. Penelitian sebelumnya menunjukkan efektivitas teknologi IoT dalam meningkatkan keamanan fisik dengan memanfaatkan ESP32 dan sensor *magnetic door switch* untuk *monitoring* pintu dengan notifikasi Telegram [6], serta pengembangan merancang sistem akses pintu menggunakan ESP32 dengan autentikasi RFID dan *keypad* dan solenoid *lock* dengan integrasi aplikasi Blynk [7]. Meskipun demikian, sistem-sistem tersebut masih terbatas pada fungsi dasar autentikasi dan *monitoring*, belum mencakup kemampuan deteksi tindak pembobolan akses.

Kondisi ini menunjukkan bahwa sistem keamanan yang ada belum memadai untuk menghadapi ancaman modern yang semakin kompleks, sehingga diperlukan solusi keamanan yang lebih adaptif dan terintegrasi. Berdasarkan permasalahan tersebut, penelitian ini bertujuan untuk merancang *smart lock system* berbasis IoT menggunakan ESP32 yang mengintegrasikan autentikasi RFID dan sidik jari dengan komunikasi *Message Queuing Telemetry Transport* (MQTT), menyediakan *monitoring* akses *real-time* serta notifikasi Telegram, dan menambahkan mekanisme deteksi pembobolan sebagai peningkatan keamanan fisik melalui sensor pintu. Dengan mengadopsi integrasi perangkat berbasis MQTT untuk komunikasi dua arah, fitur pendaftaran pengguna melalui bot Telegram.

2. TINJAUAN PUSTAKA

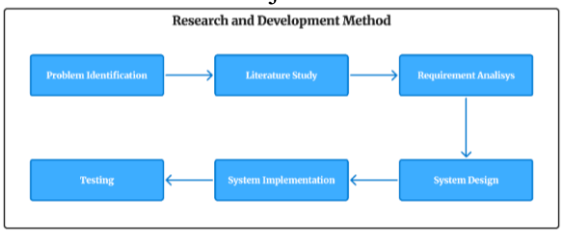
Literatur yang dipelajari dalam penelitian ini mencakup berbagai sumber yang relevan dengan perancangan dan pengujian *smart lock system* berbasis IoT. Kajian literatur meliputi standar keamanan pusat data berdasarkan ISO/IEC 27001:2022 *Annex* A 7.4 tentang *Physical Security Monitoring*, yang menekankan pentingnya penerapan sistem pemantauan fisik seperti CCTV, alarm, dan

kontrol akses untuk mencegah akses tidak sah ke area terbatas [8]. Selain itu, dipelajari pula metode pengujian *Black-box* untuk mengevaluasi fungsionalitas sistem berdasarkan spesifikasi yang telah ditetapkan tanpa memperhatikan struktur logika internal perangkat lunak [9], serta metode pengujian performa yang mencakup pengujian waktu *respon*, *throughput*, kemampuan sistem dalam menangani beban kerja tinggi, dan ketahanan sistem dalam penggunaan jangka panjang.

Kajian teknis juga mencakup pemahaman mengenai konsep IoT di mana perangkat fisik dapat terhubung dengan sensor dan perangkat lunak sehingga mampu berkomunikasi atau kontrol satu sama lain melalui internet [10], lalu cara kerja mikrokontroler ESP32 yang telah dilengkapi dengan modul WiFi sehingga mampu terhubung ke jaringan nirkabel dan berkomunikasi dengan perangkat lain [11], modul RFID MFRC-522 yang beroperasi pada frekuensi 13,56 *MHz* sesuai standar ISO/IEC 14443 A [12], serta modul sidik jari SFM V-1.7 yang menggunakan antarmuka UART sehingga mikrokontroler memiliki kendali penuh terhadap proses komunikasi data biometrik [13]. Selain itu, dipelajari pula prinsip kerja solenoid *lock* yang beroperasi dengan prinsip *Normally Closed* (NC) pada tegangan 12V, sensor *magnetic door switch* sebagai pendeteksi status pintu, serta protokol MQTT yang menerapkan arsitektur *publish/subscribe* sehingga memungkinkan server menangani banyak klien secara fleksibel dan efisien melalui komunikasi jarak jauh [14].

3. METODE PENELITIAN

Metode penelitian yang digunakan adalah *Research and Development* (R&D), seperti ditunjukkan pada Gambar 1. Penelitian diawali dengan mengidentifikasi permasalahan keamanan akses ruang server, dilanjutkan mencari tinjauan pustaka yang relevan untuk membangun sistem. Tahap analisis kebutuhan meliputi kebutuhan perangkat keras dan perangkat lunak. Selanjutnya, desain sistem mencakup perancangan perangkat keras, arsitektur MQTT, dan *flowchart* sistem. Tahap implementasi sistem meliputi implementasi MQTT Broker, pendaftaran pengguna, autentikasi pengguna, serta deteksi akses ilegal. Tahap terakhir adalah testing melalui pengujian *Black-box* dan pengujian performa untuk memastikan sistem berjalan sesuai kebutuhan.



Gambar 1. Metode Penelitian

3.1. Analisis Kebutuhan

Tahap ini mencakup identifikasi kebutuhan sistem secara menyeluruh, yang meliputi analisis perangkat keras dan perangkat lunak yang diperlukan untuk mendukung operasional *smart lock system* yang dirancang agar dapat bekerja secara optimal, andal, dan terintegrasi. Dari sisi perangkat keras, sistem ini menggunakan ESP32 sebagai mikrokontroler utama yang berfungsi mengendalikan proses autentikasi pengguna serta mekanisme penguncian pintu. Antar perangkat dalam sistem saling terhubung melalui komunikasi MQTT. Proses identifikasi pengguna dilakukan dengan memanfaatkan modul MFRC-522 yang berfungsi membaca identitas unik dari kartu RFID pengguna, serta modul sensor sidik jari SFM V-1.7 yang digunakan untuk memverifikasi identitas pengguna berdasarkan data biometrik yang telah tersimpan.

Untuk memantau kondisi fisik pintu, sistem dilengkapi dengan sensor *magnetic door switch* yang memberikan informasi status pintu dalam kondisi terbuka atau tertutup, sekaligus berperan dalam mendeteksi adanya akses tidak sah. Mekanisme penguncian pintu menggunakan solenoid *lock* sebagai kunci elektromagnetik yang pengendaliannya dilakukan melalui *relay*. Selain itu, digunakan tombol tekan sebagai sarana akses keluar dari dalam ruangan. Informasi terkait status sistem, instruksi penggunaan, serta hasil autentikasi ditampilkan melalui OLED *display* berukuran 0,96 inci, sedangkan *buzzer* digunakan sebagai media notifikasi suara terhadap kondisi atau status tertentu pada sistem. Sistem catu daya terdiri dari adaptor 12 V sebagai sumber daya solenoid *lock* dan adaptor 5 V sebagai sumber daya bagi mikrokontroler serta modul pendukung lainnya.

Dari sisi perangkat lunak, analisis dilakukan untuk memastikan seluruh komponen perangkat

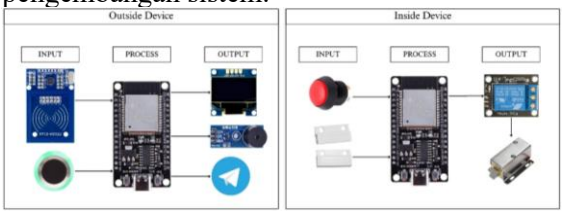
keras dapat berfungsi secara optimal dan terintegrasi dalam satu sistem. Perangkat lunak yang digunakan meliputi Arduino IDE sebagai lingkungan pengembangan dan pemrograman mikrokontroler, Mosquitto yang berperan sebagai broker MQTT untuk menangani komunikasi data secara *real-time* antar perangkat, serta Firebase yang dimanfaatkan sebagai media penyimpanan data pengguna dan riwayat akses sistem secara terpusat. Selain itu, Telegram Bot digunakan sebagai sarana pengiriman notifikasi kepada administrator serta sebagai media interaksi untuk menjalankan perintah tertentu, seperti proses pendaftaran pengguna pada sistem.

3.2. Perancangan Sistem

Perancangan sistem bertujuan sebagai dasar pengembangan yang terstruktur agar dapat direalisasikan sesuai harapan [15]. Pada tahap ini dilakukan perancangan perangkat keras, arsitektur komunikasi MQTT, serta *flowchart* sistem untuk menggambarkan alur kerja keseluruhan sistem.

3.1.1. Perancangan Perangkat Keras

Perancangan desain perangkat keras dilakukan sebagai penghubung antar modul, sensor, dan mikrokontroler untuk memastikan setiap komponen terintegrasi sesuai fungsinya serta menjadi acuan teknik dalam pengembangan sistem.



Gambar 2. Desain perangkat keras

Pada perangkat sisi luar ruangan bekerja sebagai sistem autentikasi pengguna dengan komponen penunjang saling terhubung pada ESP32 dengan konektivitas sebagai berikut:

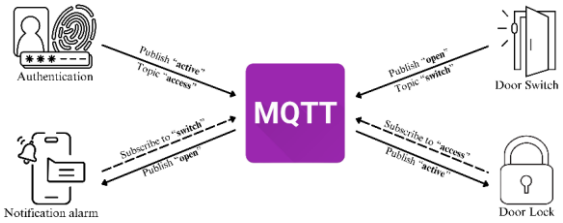
a. MFRC-522: SDA→D21; SCK→D22; MOSI→D23; MISO→D19; VCC→3.3V; GND→GND.
b. SFM-V 1.7: TX→D16; RX→D17; VCC→3.3V; GND→GND.
c. OLED display: SDA→D4; SCL→D18; VCC→3.3V; GND→GND.
d. Buzzer: pin1→D26; pin2→GND.

Pada perangkat sisi dalam ruang menangani sistem penguncian dan deteksi akses ilegal yang terhubung dengan ESP32 dengan konektivitas sebagai berikut:

a. *Magnetic door switch*: pin1→D2; pin2→GND.
b. *Relay*: COM→D33; VCC→5V; GND→GND.
c. *Push button*: pin1→D5; pin2→GND

3.1.2. Arsitektur Komunikasi MQTT

MQTT sebagai pusat kendali komunikasi untuk menjembatani pertukaran pesan antar perangkat agar di terima dengan tepat dan aman [16]. Protokol ini dirancang dengan sederhana agar mudah di implementasikan [17]. *Publish* akan mengirim pesan ke broker melalui sebuah topik, lalu *subscribe* yang menerima pesan berupa topik secara otomatis. Sesuai dengan Gambar 3. Modul autentikasi mempublikasikan status "*active*" ke topik *access* setelah autentikasi berhasil, yang kemudian di-*subscribe* oleh *Door Lock* untuk membuka kunci pintu. Selanjutnya, *Door Switch* mempublikasikan status pintu "*open*" ke topik *switch*, yang di-*subscribe* oleh alarm notifikasi untuk mengaktifkan alarm dan mengirim notifikasi saat terdeteksi kondisi tidak normal.



Gambar 3. Arsitektur komunikasi MQTT

3.1.3. *Flowchart* Sistem

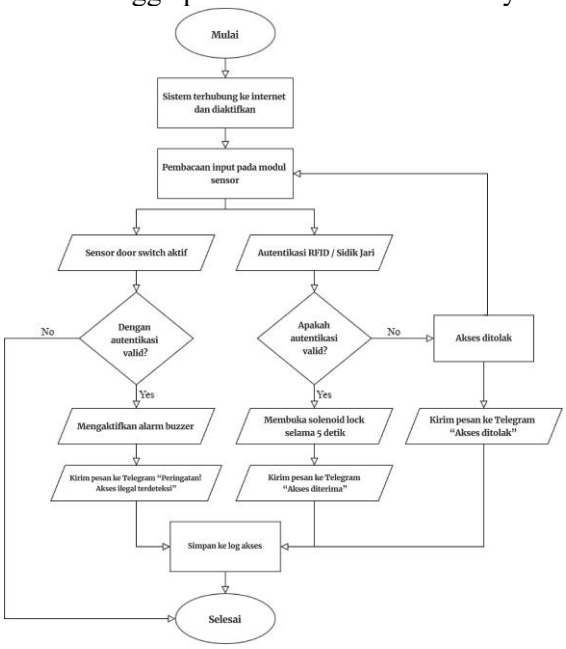
Penjelasan berikut menguraikan secara berurutan setiap tahapan yang terdapat pada Gambar 4, yang berfungsi untuk menggambarkan mekanisme kerja sistem dalam melakukan autentikasi pengguna dan deteksi akses ilegal.

a. Sistem diaktifkan dan secara otomatis terhubung ke WiFi yang telah di configurasi di dalam kode program.
b. Setelah terkoneksi, sistem melakukan pembacaan data autentikasi yang di tangkap dari modul RFID atau sidik jari. Jika data yang terbaca valid dengan data yang tersimpan, maka akses dinyatakan berhasil.
c. Ketika akses berhasil, maka sistem akan membuka penguncian pintu selama 5 detik. Setelah itu pengiriman pesan "Akses berhasil" ke Telegram, serta akan disimpan menjadi log akses di Firebase.
d. Ketika akses gagal, maka sistem akan menolak akses. Setelah itu pengiriman

pesan “Akses di tolak” ke Telegram, serta disimpan menjadi log akses di Firebase.

e. Apabila sensor pintu mendeteksi keadaan pintu terbuka tanpa melalui autentikasi yang sah, maka kondisi ini dianggap akses ilegal yang akan mengaktifkan alarm *buzzer* dan pengiriman pesan “Peringatan! Akses ilegal terdeteksi” ke Telegram.

f. Setelah semua proses terselesaikan, sistem akan kembali ke tahap awal untuk menunggu pembacaan sensor berikutnya



Gambar 4. *Flowchart* sistem

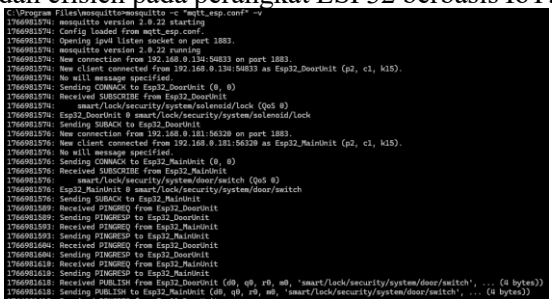
4. HASIL DAN PEMBAHASAN

4.1. Hasil Implementasi

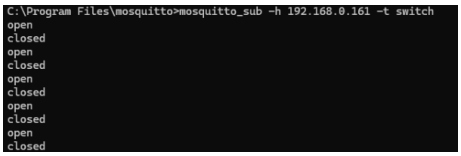
Hasil implementasi merupakan proses realisasi dari rancangan sistem yang telah disusun pada tahap sebelumnya, baik dari sisi perangkat keras maupun perangkat lunak. Implementasi difokuskan pada penerapan arsitektur komunikasi MQTT antar perangkat, integrasi autentikasi pengguna, deteksi akses ilegal, serta fitur pendaftaran pengguna secara dinamis melalui bot Telegram.

4.1.1. Hasil MQTT Broker

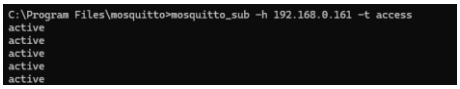
Implementasi arsitektur MQTT ditunjukkan pada Gambar 5, dengan broker Mosquitto sebagai pusat komunikasi antara perangkat penguncian dan autentikasi, serta sistem notifikasi. Perangkat autentikasi mempublikasikan status akses ke topik *access* setelah autentikasi RFID atau sidik jari berhasil, yang kemudian di-*subscribe* oleh perangkat penguncian untuk membuka solenoid *lock*. Selanjutnya, perangkat penguncian mempublikasikan status pintu ke topik *switch* berdasarkan pembacaan *magnetic door switch* untuk mendeteksi kondisi akses ilegal. Penggunaan protokol MQTT memungkinkan komunikasi data berlangsung secara *real-time* dan efisien pada perangkat ESP32 berbasis IoT.



Gambar 5. Log MQTT Broker



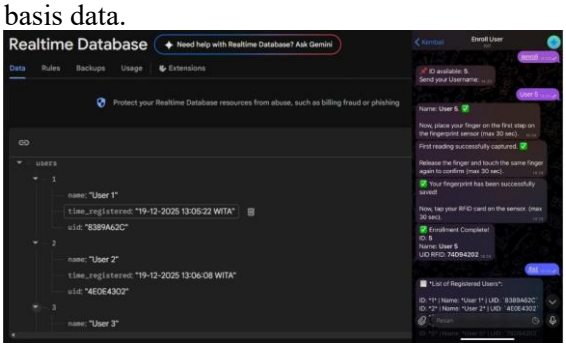
Gambar 6. Hasil *subscribe topic switch*



Gambar 7. Hasil *subscribe topic access*

4.1.2. Hasil Pendaftaran Pengguna

Implementasi fitur pendaftaran pengguna ditunjukkan pada Gambar 8. Proses pendaftaran pengguna dilakukan melalui bot Telegram oleh administrator sistem. Ketika perintah pendaftaran dikirimkan, sistem masuk ke mode pendaftaran pengguna dan menunggu proses pemindaian RFID dan sidik jari secara berurutan. Data autentikasi yang berhasil direkam akan disimpan ke *database* Firebase sebagai data pengguna resmi. Apabila salah satu tahapan pendaftaran gagal, sistem akan membatalkan proses dan tidak menyimpan data, sehingga menjaga konsistensi dan keamanan basis data.



Gambar 8. Hasil pendaftaran pengguna

4.1.3. Hasil Autentikasi Penggunassss

Berdasarkan hasil perancangan dan implementasi yang telah dilakukan, *smart lock system* berbasis IoT menggunakan ESP32 berhasil dikembangkan dan diuji melalui pembuatan prototipe yang menyerupai lingkungan pusat data UPA TIK Undiksha. Sistem ini mengintegrasikan autentikasi RFID dan sidik jari, komunikasi MQTT, notifikasi Telegram, serta log akses yang tersimpan pada Firebase.

Gambar 9. Hasil autentikasi pengguna dan notifikasi Telegram

4.1.4. Hasil Deteksi Akses Ilegal

Sensor *magnetic door switch* digunakan sebagai mekanisme untuk mendeteksi akses ilegal. Ketika pintu dibuka tanpa melalui proses autentikasi yang sah, sistem secara otomatis mengidentifikasi kondisi tersebut sebagai akses ilegal. Selanjutnya, *buzzer* diaktifkan sebagai alarm lokal, LED indikator berkedip sebagai peringatan visual, dan notifikasi peringatan dikirimkan ke Telegram secara *real-time*. Fitur ini menjadi pembeda utama dibandingkan sistem *smart lock* komersial yang umumnya hanya autentikasi akses tanpa mekanisme deteksi pembobolan secara langsung. Dengan adanya fitur ini, sistem mampu memberikan perlindungan tambahan terhadap potensi ancaman fisik pada pusat data.

Gambar 10. Hasil deteksi akses ilegal dan notifikasi Telegram

4.2. Tabel Pengujian

4.2.1. Pengujian *Black-box*

Pengujian s*mart lock system* berbasis IoT pada penelitian ini dilakukan menggunakan metode Black Box testing dengan teknik *Decision Table* untuk menguji sistem sesuai spesifikasi yang telah dirancang.

Tabel 1. Hasil pengujian *Black-box* pada OLED *display*

Skenario	Output	Hasil
Sistem diaktifkan	Sistem siap, Pindai di sini	Sukses
Pindai autentikasi yang telah di daftarkan	Akses berhasil, Welcome <*username*>	Sukses
Pindai autentikasi yang tidak di daftarkan	Akses ditolak	Sukses
Tekan tombol akses keluar ruangan	Akses keluar berhasil	Sukses
Pintu terbuka tanpa autentikasi	Peringatan! Akses ilegal terdeteksi	Sukses

Tabel 2. Hasil pengujian *Black-box* pada indikator LED

Skenario	Output	Hasil
Sistem diaktifkan	LED biru aktif mode *standby*	Sukses
Pindai autentikasi yang telah di daftarkan	LED hijau aktif selama 3 detik	Sukses
Pindai autentikasi yang tidak di daftarkan	LED merah berkedip 3x	Sukses
Pintu terbuka tanpa autentikasi	LED merah berkedip 10x	Sukses

Tabel 3. Hasil pengujian *Black-box* pada solenoid *lock*

Skenario	Output	Hasil
Pindai autentikasi yang telah di daftarkan	Membuka penguncian selama 5 detik	Sukses
Pindai autentikasi yang tidak di daftarkan	Tetap dalam kondisi tertutup	Sukses
Tekan tombol akses keluar ruangan	Membuka penguncian selama 5 detik	Sukses

Tabel 4. Hasil pengujian *Black-box* pada alarm *buzzer*

Skenario	Output	Hasil
Pindai autentikasi yang tidak di daftarkan	*Buzzer* aktif selama 3x	Sukses
Pintu terbuka tanpa autentikasi	*Buzzer* aktif selama 10x	Sukses

Tabel 5. Hasil pengujian *Black-box* pada pesan Bot Telegram.

Skenario	Output	Hasil
Pindai autentikasi yang telah di daftarkan	Akses berhasil, <*id*>, <*username*>, <*times*>	Sukses
Pindai autentikasi yang tidak di daftarkan	Akses ditolak, Percobaan akses tidak sah <*times*>	Sukses
Pintu terbuka tanpa autentikasi	Peringatan! Akses ilegal terdeteksi	Sukses
Mengirimkan perintah */enroll*	Melakukan proses pendaftaran pengguna baru	Sukses
Mengirimkan perintah */list*	Menampilkan *list* pengguna yang telah terdaftar	Sukses
Mengirimkan perintah */delete*	Melakukan penghapusan data pengguna berdasarkan id	Sukses
Mengirimkan perintah */log*	Menampilkan log riwayat akses yang telah terjadi	Sukses

4.2.2. Pengujian Performa

Pengujian kinerja adalah jenis pengujian yang bertujuan untuk mengevaluasi kualitas sistem dalam hal kecepatan, stabilitas, dan efisiensi saat digunakan dalam berbagai kondisi. Evaluasi dilakukan dengan menghitung rata-rata waktu tunda dan persentase kegagalan autentikasi menggunakan rumus berikut:

$$Average\ latency = \frac{Total\ times}{Total\ tests} \quad (1)$$

$$Success\ rate = \frac{Number\ successful}{Total\ tests} \times 100\% \quad (2)$$

Tabel 6. Hasil pengujian performa autentikasi dengan sidik jari yang terdaftar

No.	Hasil	Username	Waktu Mulai	Solenoid Terbuka	Firebase	Notifikasi Telegram	Waktu Total
1.	Diterima	User 1	14:38:53	14:38:55	14:38:55	14:38:57	0:00:04
2.	Diterima	User 2	14:40:19	14:40:20	14:40:20	14:40:22	0:00:03
3.	Diterima	User 3	14:40:32	14:40:32	14:40:33	14:40:35	0:00:03
4.	Diterima	User 4	14:40:42	14:40:43	14:40:43	14:40:46	0:00:04
5.	Diterima	User 5	14:40:50	14:40:50	14:40:51	14:40:52	0:00:02
...							
20.	Diterima	User 5	14:48:48	14:48:50	14:48:50	14:48:52	0:00:04
Rata-rata *latency*							**0:00:05**

$$Success\ rate = \frac{20}{20} \times 100\% = 100\%$$

Tabel 7. Hasil pengujian performa autentikasi dengan RFID yang terdaftar

No.	Hasil	Username	Waktu Mulai	Solenoid Terbuka	Firebase	Notifikasi Telegram	Waktu Total
1.	Diterima	User 1	15:28:09	15:28:12	15:28:12	15:28:14	0:00:05
2.	Diterima	User 2	15:28:29	15:28:32	15:28:32	15:28:34	0:00:05
3.	Diterima	User 3	15:28:42	15:28:44	15:28:44	15:28:46	0:00:04
4.	Diterima	User 4	15:28:54	15:28:56	15:28:56	15:28:58	0:00:04
5.	Diterima	User 5	15:29:10	15:29:13	15:29:13	15:29:15	0:00:05

No.	Hasil	Username	Waktu Mulai	Solenoid Terbuka	Firebase	Notifikasi Telegram	Waktu Total
…							
20.	Diterima	User 5	15:31:29	15:32:31	15:32:31	15:32:33	0:00:04
Rata-rata *latency*							**0:00:04**

$$Success\ rate = \frac{20}{20} \times 100\% = 100\%$$

Tabel 8. Hasil pengujian performa dengan autentikasi yang tidak terdaftar

No.	Hasil	Waktu Mulai	Buzzer Aktif	Solenoid Terbuka	Firebase	Notifikasi Telegram	Waktu Total
1.	Ditolak	16:14:18	16:14:18	-	16:14:20	16:14:22	0:00:04
2.	Ditolak	16:14:26	16:14:26	-	16:14:28	16:14:29	0:00:03
3.	Ditolak	16:14:33	16:14:33	-	16:14:35	16:14:37	0:00:04
4.	Ditolak	16:14:40	16:14:40	-	16:14:42	16:14:44	0:00:04
5.	Ditolak	16:14:47	16:14:47	-	16:14:50	16:14:51	0:00:04
…							
20.	Ditolak	16:18:51	16:18:51	-	16:18:53	16:18:55	0:00:04
Rata-rata *latency*							**0:00:04**

$$Success\ rate = \frac{20}{20} \times 100\% = 100\%$$

4.3. Pembahasan

Berdasarkan hasil implementasi sistem, *smart lock system* berbasis IoT yang dikembangkan berhasil mengintegrasikan autentikasi RFID dan sidik jari, komunikasi antar perangkat menggunakan protokol MQTT, serta sistem notifikasi dan *monitoring real-time* melalui bot Telegram. Implementasi arsitektur MQTT memungkinkan pertukaran data antar perangkat autentikasi, perangkat penguncian, dan sistem notifikasi berlangsung secara efisien dan *real-time*, sehingga perintah pembukaan kunci, status pintu, serta peringatan keamanan dapat diproses lebih responsif untuk mengatasi nilai *latency* yang signifikan. Selain itu, fitur pendaftaran pengguna melalui bot Telegram memberikan fleksibilitas dalam pengelolaan pengguna karena pendaftaran dapat dilakukan secara dinamis tanpa pemrograman ulang perangkat, sekaligus menjaga konsistensi data melalui penyimpanan terpusat di Firebase.

Pengujian fungsional sistem dilakukan menggunakan metode Pengujian *Black-box* dengan teknik *Decision Table*, di mana skenario pengujian disusun berdasarkan kombinasi *input* dan keluaran yang diharapkan dalam bentuk tabel [18]. Pendekatan ini bertujuan untuk memastikan bahwa setiap fungsi sistem bekerja sesuai dengan spesifikasi yang telah dirancang. Hasil pengujian pada Tabel 1 – Tabel 5. menunjukkan bahwa seluruh komponen sistem, seperti OLED *display*, LED indikator, *buzzer*, solenoid *lock*, sensor *magnetic door switch*, serta Telegram bot, berfungsi dengan baik pada setiap skenario pengujian. Sistem secara konsisten hanya membuka penguncian ketika autentikasi dinyatakan valid dan menolak autentikasi tidak sah, sekaligus mengaktifkan peringatan pada kondisi akses ilegal.

Selain pengujian fungsional, dilakukan pengujian performa untuk mengevaluasi kualitas sistem dari aspek waktu respons dan tingkat keberhasilan autentikasi. Performance testing bertujuan untuk menilai kinerja sistem serta dampaknya terhadap pengguna melalui evaluasi dan analisis mendalam [19]. Berdasarkan hasil pengujian pada Tabel 6 – Tabel 8, mendapatkan rata-rata *lacenty* sistem berada pada kisaran 4 detik untuk seluruh skenario pengujian, dengan rincian bahwa autentikasi RFID menunjukkan *lacenty* yang relatif stabil pada rentang 4 – 5 detik, sedangkan autentikasi sidik jari memiliki variasi *latency* yang lebih besar, yaitu antara 2 – 8 detik.

Perbedaan karakteristik autentikasi RFID dan sidik jari menunjukkan adanya *trade-off* antara performa dan keamanan sistem. RFID unggul dalam kecepatan dan kestabilan waktu respons karena proses pembacaan kartu yang sederhana dan tidak dipengaruhi kondisi

pengguna, namun masih memiliki kelemahan dari sisi keamanan akibat potensi duplikasi ID, risiko kehilangan kartu, serta kebutuhan biaya tambahan untuk ketersediaan kartu. Sebaliknya, autentikasi sidik jari menawarkan tingkat keamanan yang lebih tinggi karena berbasis biometrik yang unik dan tidak memerlukan media fisik, meskipun performanya cenderung bervariasi akibat pengaruh kondisi jari saat proses verifikasi. Oleh karena itu, integrasi kedua metode autentikasi ini mampu menyeimbangkan aspek kecepatan, stabilitas, dan keamanan, sehingga *smart lock system* menjadi lebih adaptif dan andal untuk diterapkan pada lingkungan pusat data dengan kebutuhan keamanan tinggi dan *monitoring real-time.*

5. KESIMPULAN

Berdasarkan hasil perancangan, implementasi, dan pengujian yang telah dilakukan, dapat disimpulkan bahwa *smart lock system* berbasis IoT menggunakan ESP32 berhasil dikembangkan sebagai solusi peningkatan keamanan akses fisik pusat data UPA TIK Universitas Pendidikan Ganesha. Sistem ini mampu mengintegrasikan autentikasi RFID dan sidik jari, komunikasi antar perangkat menggunakan protokol MQTT, deteksi akses ilegal melalui sensor *magnetic door switch*, serta notifikasi dan *monitoring real-time* melalui bot Telegram.

Hasil pengujian fungsional menunjukkan bahwa seluruh fitur sistem berjalan sesuai dengan spesifikasi perancangan, sedangkan hasil pengujian performa menunjukkan sistem memiliki rata-rata *latency* sebesar 4 detik dengan tingkat keberhasilan autentikasi yang terdaftar dan penolakan autentikasi yang tidak terdaftar mencapai 100%. Selain itu, fitur pendaftaran pengguna memberikan kemudahan dalam pengelolaan akses pengguna secara dinamis tanpa pemrograman ulang perangkat. Dengan demikian, *smart lock system* berbasis IoT yang dikembangkan mampu meningkatkan keamanan fisik pusat data secara terintegrasi, responsif, dan lebih adaptif dibandingkan sistem penguncian di pasaran.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada UPA TIK Universitas Pendidikan Ganesha atas dukungan dan fasilitas yang diberikan selama pelaksanaan penelitian ini. Apresiasi juga disampaikan kepada seluruh pihak yang telah memberikan kontribusi dan masukan sehingga penelitian ini dapat diselesaikan dengan baik.

DAFTAR PUSTAKA

[1] A. R. Dwiyanto, Nurfiyah, D. Yusuf, Z. T. Rony, and B. Karsono, “Kebijakan Keamanan Informasi (Information Security Policy),” Bekasi, Oct. 2023.

[2] A. D. L. Sugianto, F. Samopa, and H. M. Astuti, “Penilaian Dan Kontrol Risiko Terhadap Infrastruktur Dan Keamanan Informasi Berdasarkan Standar ISO/IEC 27001:2013 (Studi Kasus: Institut Teknologi Sepuluh Nopember),” *Sebatik*, vol. 24, no. 1, pp. 96–101, Jun. 2020, doi: 10.46984/sebatik.v24i1.910.

[3] M. A. Bakri, M. Farhan, A. Sujatmiko, and A. Firasanti, “Pemantauan Suhu dan Deteksi Gerak Obyek Berbasis IoT pada Ruang Server Menggunakan Thinger.IO,” *TELKA: Jurnal Telekomunikasi, Elektronika, Komputasi, dan Kontrol*, vol. 8, no. 1, pp. 74–81, May 2022, doi: 10.15575/telka.v8n1.74-81.

[4] PT XL Axiata Tbk, “Polrestabes Makassar Tangkap Pelaku Pencurian Perangkat di Data Center XL Axiata.” Accessed: Feb. 05, 2025. [Online]. Available: https://www.xlaxiata.co.id/id/berita/polrestabes-makassar-tangkap-pelaku-pencurian-perangkat-di-data-center-xl-axiata

[5] I. W. Anugrahana, “ANALISIS PRAKTIK PROBLEM MANAGEMENT DI UPA TIK UNIVERSITAS PENDIDIKAN GANESHA MENGGUNAKAN FRAMEWORK ITIL V4,” Universitas Pendidikan Ganesha, Singaraja, 2025. Available: http://repo.undiksha.ac.id/id/eprint/25870

[6] M. Nizam, H. Yuana, and Z. Wulansari, “Mikrokontroler ESP32 Sebagai Alat Monitoring Pintu Berbasis Web,” *JATI (Jurnal Mahasiswa Teknik Informatika)*, vol. 6, no. 2, pp. 767–772, Sep. 2022, doi: https://doi.org/10.36040/jati.v6i2.5713.

[7] A. Fakhruddin, “Rancang Bangun Sistem Keamanan Pintu Rumah Berbasis Internet Of Things Dengan ESP32 Dan Aplikasi Blynk,” *Jurnal Teknik Elektro dan Informatika*, vol. 19, no. 2, pp. 53–59, May 2024, doi: http://dx.doi.org/10.30587/e-link.v19i1.7600.

[8] M. Edwards, “ISO 27001:2022 Annex A 7.4 – Physical Security Monitoring,” © 2025 Alliantist Ltd.

[9] A. N. Fathoni and U. Y. Oktiawati, “Blackbox Testing terhadap Prototipe Sistem Monitoring Kualitas Air Berbasis IoT,” *Jurnal Nasional*

Teknik Elektro dan Teknologi Informasi, vol. 10, no. 4, pp. 362–368, Nov. 2021, doi: 10.22146/jnteti.v10i4.2095.

[10] C. Dewi, R. Arthana, and K. Setemen, "RANCANG BANGUN ALAT PAKAN KUCING DENGAN MENGGUNAKAN MIKROKONTROLER BERBASIS INTERNET OF THINGS (IOT)," *Kumpulan Artikel Mahasiswa Pendidikan Teknik Informatika (KARMAPATI)*, vol. 12, no. 3, pp. 177–199, Dec. 2023, doi: 10.23887/karmapati.v12i3.70010.

[11] S. KAYA, E. AŞKAR AYYILDIZ, and M. AYYILDIZ, "Smart Door Lock Design With Internet Of Things," *International Journal of 3D Printing Technologies and Digital Industry*, vol. 6, no. 2, pp. 201–206, Aug. 2022, doi: 10.46519/ij3dptdi.1074468.

[12] Z. Achmad, "Rancang Bangun Smart Gate Pada Perpustakaan ITS Menggunakan Smart Card ITS (ITS Smart)," Undergraduate thesis, Institut Teknologi Sepuluh Nopember, 2020. Accessed: Mar. 25, 2025. Available: http://repository.its.ac.id/id/eprint/79396

[13] Matrikschung, "SFM-V1.7," ARDUINO.CC. Accessed: Mar. 30, 2025. [Online]. Available: https://docs.arduino.cc/libraries/sfm-v1.7/

[14] D. B. Prasetyo, *Protokol Jaringan Dalam Internet of Things*. Penerbit LPPM UPN "Veteran" Yogyakarta, 2020. Accessed: Apr. 30, 2025. [Online]. Available: http://eprints.upnyk.ac.id/id/eprint/27440

[15] D. Aulia Ramadini and Hastuti, "SISTEM KUNCI ELEKTRONIK PINTU KOS MENGGUNAKAN IOT BERBASIS E-KTP," *Jurnal Informatika dan Teknik Elektro Terapan*, vol. 13, no. 1, pp. 2830–7062, Jan. 2025, doi: 10.23960/jitet.v13i1.6177.

[16] F. Imansyah, R. Ratiandi, J. Marpaung, D. Suryadi, and F. Hizballah, "Perancangan Sistem Pengujian Throughput Publishing Data pada Modul ESP8266 dengan Protokol MQTT," *Jurnal Sistem dan Teknologi Informasi (JustIN)*, vol. 11, no. 3, pp. 419–424, Jul. 2023, doi: 10.26418/justin.v11i3.64820.

[17] M. Oktiana *et al.*, "Analisis Kualitas Message Queue Telemetry Transport (MQTT) Pada Rancangan Sistem Smart Door View Berbasis IoT," *KITEKTRO: Jurnal Komputer, Informasi Teknologi, dan Elektro* , vol. 9, no. 3, pp. 154–161, 2024, doi: https://doi.org/10.24815/kitektro.v9i3.43982.

[18] G. I. Marthasari, A. T. Wahyuningsih, M. R. Aviansyah, M. A. Ramadhani, and Z. Rahmatullah, "Pengujian Website Infotech Menggunakan Teknik Black-Box Decision Table," *Jurnal Informatika Universitas Pamulang*, vol. 7, no. 1, pp. 115–119, Mar. 2022.

[19] M. Hadi, N. Rahaningsih, and R. Danar, "ANALISA PERFORMA SISTEM SMART HOME BERBASIS IOT MENGGUNAKAN TELEGRAM MESSENGER BOT DAN NODEMCU ESP 32," 2024.