Journal of Vocational Education and Information Technology
Vol. 7, No. 2, Desember 2026, 671 - 680
E-ISSN: 2722-5305
Terakreditasi **SINTA Peringkat 4**
Surat Keputusan Direktur Jenderal Pendidikan Tinggi, Riset, dan Teknologi, Nomor: 230/E/KPT/2024

Implementasi *Multi-Factor Authentication* Berbasis RFID, Biometrik, dan PIN pada Sistem Keamanan Ruang Arsip

Maulana Muzakki Bhaswara [1,*], Chrystia Aji Putra [2], Ardhon Rakhmadi [3]

[1,2,3] Program Studi Informatika; Fakultas Ilmu Komputer, Universitas Pembangunan Nasional Veteran Jawa Timur; Jalan Raya Rungkut Madya No. 1, Gunung Anyar, Surabaya, Jawa Timur; e-mail: 22081010045@student.upnjatim.ac.id , ajiputra@upnjatim.ac.id

ardhon.rakhmadi.fasilkom@upnjatim.ac.id

* Korespondensi: e-mail: 22081010045@student.upnjatim.ac.id

Diterima: 12-08-2026 ; Review: 28-10-2026; Disetujui: 21-11-2026

Abstrak: Kunci fisik tradisional memiliki banyak kelemahan sehingga dianggap sudah tidak memadai lagi untuk mengamankan dokumen-dokumen vital negara yang disimpan pada ruang arsip. Hal ini disebabkan oleh beberapa faktor seperti risiko duplikasi kunci dan minimnya rekam jejak akses otomatis. Faktor tersebut merupakan celah keamanan yang fatal. Oleh karena itu, pada penelitian ini dilakukan perancangan sistem keamanan terintegrasi berbasis *Internet of Things* (IoT) yang memperketat akses masuk ruang arsip tersebut. Pendekatan yang digunakan pada penelitian ini adalah perlindungan berlapis yang melalui *Multi Factor Authentication* (MFA). Sistem ini mengharuskan pengguna untuk melewati tahap kombinasi verifikasi mutlak: sensor sidik jari biometrik, RFID, dan *input* kode PIN. Mikrokontroler yang berfungsi sebagai pusat kendali memiliki tugas untuk mengatur seluruh proses autentikasi. Pada hasil perancangan perangkat keras (*hardware*), prototipe terbagi menjadi empat zona fungsional yaitu: eksterior, interior, plafon, dan kotak panel. Pembagian ini dapat menghasilkan rute kabel yang tersembunyi agar dapat mengurangi probabilitas sabotase fisik. Perangkat lunak yang terdapat pada sistem ini memungkinkan untuk melakukan pencatatan setiap percobaan akses secara akurat. Seluruh *data log* akan dikirimkan via protokol MQTT menuju server database MySQL. Data log ini kemudian akan disajikan sebagai fitur Jejak Audit (*Audit Trail*) yang akan ditampilkan pada *dashboard admin*. Kesimpulannya, pengujian menunjukkan arsitektur sistem ini berhasil mengeksekusi logika autentikasi dengan akurasi RFID 100% dan sidik jari 96%, serta transmisi log akses beroperasi optimal pada latensi rata-rata 145 ms untuk menjamin akuntabilitas riwayat akses.
Kata kunci: Ruang Arsip, Jejak Audit, Internet of Things. Autentikasi Multi-Faktor, Keamanan Fisik

Abstract: *Traditional physical keys have many weaknesses and are therefore no longer considered adequate for securing vital state documents stored in archives. This is due to several factors, such as the risk of key duplication and the lack of an automated access log. These factors constitute critical security vulnerabilities. Therefore, this study designed an integrated security system based on the Internet of Things (IoT) to tighten access to these archive rooms. The approach used in this study is layered protection through Multi-Factor Authentication (MFA). This system requires users to pass through a combination of mandatory verification steps: a biometric fingerprint sensor, RFID, and PIN code input. A microcontroller, functioning as the control center, is responsible for managing the entire authentication process. In the hardware design, the prototype is divided into four functional zones: exterior, interior, ceiling, and panel box. This division allows for hidden cable routing to reduce the likelihood of physical sabotage. The software in this system enables accurate logging of every access mAP@0.5:0.95 of 0.1449, an increase of 0.0542 and 0.0191 respectively over the baseline. These results indicate that*

Copyright@2026. LEMBAGA PENGEMBANGAN DAN INOVASI UNDHARI

combining several augmentation techniques is more effective at improving the model's model's attempt. All log data is transmitted via the MQTT protocol to a MySQL database server. This log data is then presented as an Audit Trail feature displayed on the admin dashboard. In conclusion, testing shows that this system architecture successfully executes authentication logic with 100% RFID and 96% fingerprint accuracy, and the access log transmission operates optimally at an average latency of 145 ms to ensure accountability for access history.
***Keywords**:Archive Room, Audit Trail, Internet of Things, Multi-Factor Authentication, Physical Security*

1. Pendahuluan

Ruang Arsip memiliki peran yang sangat penting dalam suatu instansi atau perusahaan karena ruangan tersebut menyimpan berbagai dokumen-dokumen penting, berharga, serta bersifat rahasia yang memiliki nilai baik nilai hukum atau nilai historis. Hal ini diperkuat oleh Undang-Undang Republik Indonesia Nomor 43 Tahun 2009 tentang Kearsipan yang menyebutkan bahwa arsip memrupakan memori kolektif, alat pertanggungjawaban, serta identitas jati diri yang wajib dikelola dan dilindungi [9]. Mengingat penting nya aset-aset tersebut, tentunya perlindungan khusus berupa fisik sangat diperlukan guna mencegah ancaman-ancaman seperti pencurian. Kasus nyata terjadi pada pembobolan dokumen yang terjadi pada gudang arsip PT Kereta Api Indonesia (KAI) Tanjung Karang, di mana petugas yang lalai dalam pengawasan pintu akses yang mengakibatkan hilangnya dokumen penting dalam jumlah yang besar [5]. Maka dari itu, Sistem Keamanan ruang arsip dianjurkan untuk memenuhi prinsip nirsangkal (*non-repudiation*), di mana setiap identitas dari individu yang mengakses ruangan tersebut harus terverifikasi secara mutlak dan tidak dapat disangkal [11]. Akan tetapi, mayoritas sistem keamanan ruang arsip yang digunakan saat ini masih bergantung pada kunci konvensional dan kartu akses biasa. Kelemahan pada kunci konvensional tersebut menimbulkan kerentanan keamanan yang fatal, secara spesifik berupa tingginya risiko akses tidak sah akibat mudah diduplikasi serta tidak tersedianya rekam jejak akses (*audit trail*) otomatis yang aktual untuk melakukan penelusuran identitas [1]. Di sisi lain, penggunaan kartu akses biasa yang merupakan metode autentikasi tunggal (*Single Factor Authentication*) juga memiliki celah keamanan yaitu risiko untuk dipindahtangankan (*transferable*) [8]. Selain itu, kartu akses sangat rawan hilang, dicuri, atau tertinggal yang membuat kemungkinan ruangan akan diakses secara illegal menjadi lebih besar. Apabila terjadi suatu insiden keamanan, pengelola akan mengalami kesulitan untuk melakukan penelurusan pelaku akibat dari minimnya pencatatan riwayat akses (*Audit Trail*) yang aktual [4].

Guna mengatasi celah dari keamanan autentikasi tunggal tersebut, diperlukan adanya penerapan *Multi-Factor Authentication* (MFA) yang merupakan solusi yang ideal. Pengganbungan tiga faktor autentikasi yaitu Kartu RFID yang berperan sebagai faktor kepemilikan, PIN sebagai faktor pengetahuan, dan sidik jari berperan sebagai faktor inherensi (biometrik) [14]. Dengan penerapan MFA, tingkat keamanan dapat ditingkatkan secara signifikan karena masing-masing faktor mampu saling menutupi kelemahan masing-masing. Pada pemilihan faktor biometrik, penggunaan sensor sidik jari dinilai lebih optimal dibandingkan dengan metode-metode lain seperti seperti *Face Recognition* (Pengenalan Wajah) [7]. Hal ini dipengaruhi oleh beberapa faktor, seperti batasan arsitektur perangkat keras (*hardware constraints*), di mana mikrokontroler ESP32 yang memiliki keterbatasan memori dan daya komputasi untuk menangani pemrosesan wajah yang besar. Faktor selanjutnya yang memiliki pengaruh siginfikan adalah performa kamera pemindai wajah yang rentan mengalami penurunan akurasi yang drastis pada kondisi minim cahaya, sedangkan sensor sidik jari memiliki unit pemrosesan sinyal digital (DSP) madniri yang stabil dalam berbagai kondisi pencahayaan [2].

Beberapa penelitian terdahulu telah berupaya untuk mengembangkan sistem *Smart Lock* (Kunci Pintar) berbasis *Internet of Things* (IoT) [13]. Namun, sebagian besar dari riset tersebut hanya berfokus pada implementasi pada skala rumah tangga serta hanya dilakukan penerapan satu hingga dua faktor autentikasi [12]. Selain itu, mikrokontroler yang digunakan pada sistem banyak menggunakan mikrokontroler berkapasitas rendah seperti Arduino Nano atau ESP8266 *single core* yang memiliki keterbatasan seperti konektivitas internet mandiri dan kecepetan pemrosesan data yang lebih lambat [10]. Mayoritas dari sistem tersebut juga hanya menggunakan penyimpanan secara lokal pada kartu memori (SD Card) atau jaringan lokal (*local web server*) untuk menyimpan data riwayat akses [6]. Hal ini meningkatkan risiko kehilangan

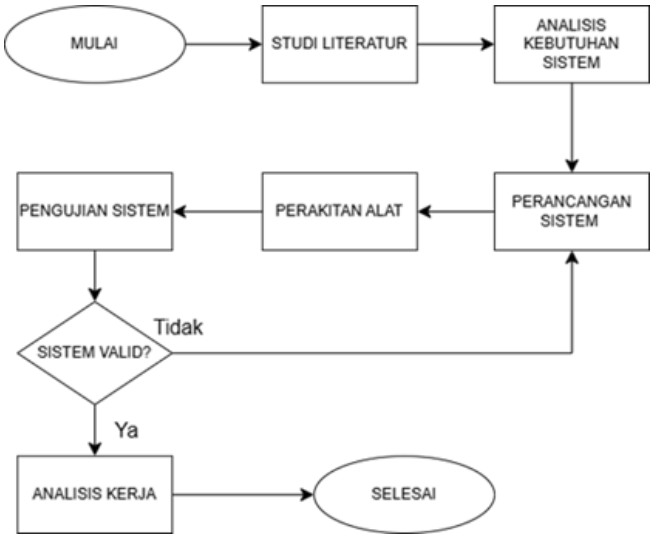
Vol.7, No. 2, Desember 2026, 671 - 680

data apabila perangkat rusak mengalami kerusakan fisik. Celah penelitian (*Research Gap*) yang ditemukan dari penelitian-penelitian sebelumnya, yaitu belum ada sistem yang mengintegrasikan MFA tiga lapis secara terpusat dengan sistem manajemen data untuk standar akuntabilitas ruang penyimpanan vital.

Berdasarkan celah penelitian yang ditemukan, artikel ini mengusulkan solusi dengan merancang dan mengimplementasikan sistem keamanan *smart lock* menggunakan logika *Multi-Factor Authentication* yang mengintegrasikan komponen RFID, Sidik Jari, dan PIN berbasis mikrokontroler ESP32. Fokus utama dari penelitian ini adalah pengebangan arsitektur perangkat keras, penyusunan *Flowchart* (diagram alir) dari algoritma verifikasi berlapis pada firmware mikrokontroler, serta analisis kinerja sistem dalam memproses antrean instruksi sensor [3]. Melalui pengujian fungsionalitas komponen (*black box testing*) dan pengukuran waktu respons (*response time*) eksekusi, penelitian ini diharapkan dapat memberikan kontribusi mengenai keandalan serta akuntabilitas infrastruktur pengamanan digital yang efisien [15].

2. Metode Penelitian

Penelitian ini menggunakan pendekatan *Research and Development* (R&D) dimana metode ini berfokus perancangan arsitektur keamanan fisik dan pembuatan prototipe sistem *smart lock* berbasis *Internet of Things* (IoT). Pendekatan R&D dipilih karena pengerjaan arsitektur *Internet of Things* (IoT) membutuhkan siklus pengembangan yang berulang, mulai dari mematangkan konsep dasar hingga memvalidasi logika alat secara sistem. Tujuan utamanya adalah mentransformasikan seluruh persyaratan keamanan ruang arsip yang bersifat teoritis menjadi sebuah integrasi fungsional antara perangkat keras dan lunak. Untuk memberikan gambaran yang sistematis mengenai proses dari *Research and Development* (R&D) yang dilakukan, alur penelitian telah divisualisasikan melalui diagram alir pada Gambar 1.



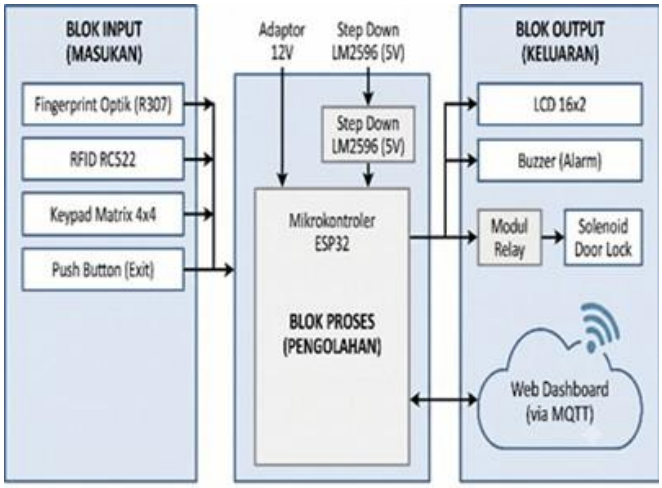
Gambar 1. Diagram Alir Tahapan Penelitian R&D

Berdasarkan diagram alir pada gambar 1, berikut merupakan penjelasan dari setiap tahapan dari penelitian yang dilakukan. Pada tahap pertama dilakukan Studi Literatur. Pada fase ini berfokus pada pengkajian literatur dan penelitian terdahulu yang relevan dengan sistem *smart lock*, teknologi IoT, dan protokol komunikasi. Tahapan ini bertujuan untuk menemukan *research gap* pada sistem-sistem konvensional sebagai dasar dari perumusan kebaruan (*novelty*) penelitian, yaitu penerapan MFA. Setelah menemukan *research gap* pada masing-masing penelitian terdahulu, dilakukan tahap analisis kebutuhan sistem. Pada tahap ini dilakukan pendefinisian batasan operasional dan spesifikasi teknis. Analisis dilakukan terhadap batas daya, kapasitas komputasi, dan limitasi memori dari mikrokontroler agar mampu mengakomodasi integrasi pembacaan sidik jari (R307), kartu RFID (RC522) tanpa menyebabkan antrean data. Pada tahap selanjutnya, dilakukan pengembangan *Work Breakdown Structure* (WBS) dilakukan

untuk membagi sistem menjadi subsistem yang lebih spesifik. Pada sisi *hardware*, dilakukan perancangan *layout* (tata letak) purwarupa yang terdapat beberapa zona fungsional. Pada sisi *software*, dirancang topologi transmisi MQTT serta relasi basis data MySQL untuk kebutuhan *Audit Trail*. Pada tahap eksekusi dari desain yang telah dirancang. Proses ini mencakup wiring komponen elektronika. Secara paralel, penulisan kode program C++ diimplementasikan melalui kerangka kerja Arduino IDE dan diunggah ke mikrokontroler. Pengujian dilakukan secara empiris untuk memastikan sistem berjalan sesuai dengan skenario yang diharapkan. Tahap evaluasi keandalan sistem pada penelitian ini menggunakan tiga metode utama:

1) Pengujian fungsional, menggunakan metode *black-box testing* untuk memvalidasi respons aktuator terhadap berbagai skenario kombinasi masukan sensor.
2) Pengujian autentikasi, guna menguji algoritma *Multi-Factor Authentication* (MFA) yang mewajibkan pengguna melewati verifikasi lapisan inherensi (sidik jari), kepemilikan (RFID), dan pengetahuan (PIN) secara berurutan.
3) Pengukuran latensi MQTT, untuk mengukur waktu tunda (*delay*) transmisi pengiriman paket data log menuju server database MySQL menggunakan pendekatan *Round-Trip Time*.

Tahap ini juga mencakup evaluasi iteratif, apabila ditemukan error atau ketidaksesuaian output atau latensi yang terlalu tinggi, maka proses akan dikembalikan ke tahap Perancangan Sistem untuk perbaikan *hardware* atau evaluasi algoritma. Sebaliknya, apabila sistem telah merespons seluruh parameter MFA dan *fail-safe* dengan benar, maka purwarupa dinyatakan valid dan penelitian dilanjutkan ke tahap analisis. Pada tahap Analisis Kerja yang merupakan tahap finalisasi di mana data mentah hasil pengujian diolah menjadi informasi kuantitatif. Hasil analisis ini digunakan untuk menarik kesimpulan mengenai tingkat keandalan, keamanan, dan akuntabilitas arsitektur sistem keamanan yang dibangun. Mikrokontroler ESP32 difungsikan sebagai unit pemrosesan pusat (otak) yang mengelola seluruh antarmuka input dan output. Blok input dikonfigurasi secara spesifik untuk memfasilitasi algoritma *Multi-Factor Authentication* (MFA) yang terdiri dari modul RFID RC522 sebagai pembaca token kepemilikan, *Keypad Matrix* 4x4 sebagai modul masukan lapisan pengetahuan (PIN), dan sensor biometrik optikal R307 sebagai pemindai lapisan inherensi. Pada blok output, mikrokontroler dihubungkan dengan aktuator *Solenoid Door Lock* 12V untuk mengunci pintu, *buzzer* sebagai alarm peringatan, dan layar LCD 16x2 sebagai antarmuka informasi yang interaktif bagi pengguna. Seluruh distribusi daya kelistrikan dari adaptor 12V diturunkan secara presisi menggunakan modul *step-down* LM2596 untuk menyuplai tegangan 5V yang stabil pada mikrokontroler dan sensor sebagaimana diilustrasikan pada Gambar 2.



Gambar 2. Blok Diagram Sistem Keamanan Multi-Factor Authentication

Pengembangan perangkat lunak (*software*) dilakukan menggunakan bahasa pemrograman C++ yang dikompilasi menggunakan platform Arduino IDE. Algoritma pada

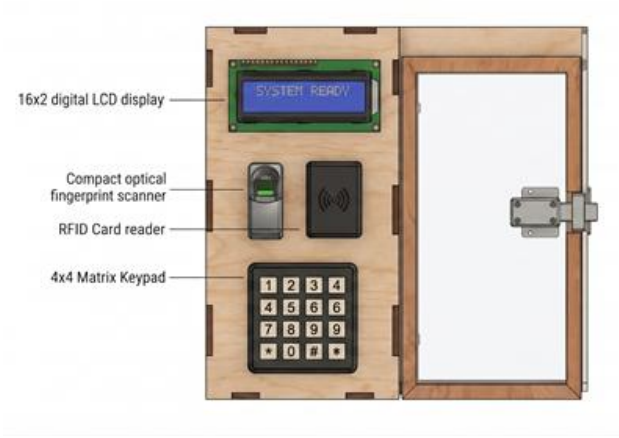
firmware ESP32 dirancang dengan logika autentikasi silang yang fleksibel, di mana pengakses wajib untuk melewati ketiga faktor yang tersedia. Pada kondisi *standby*, sistem akan menunggu input pertama dari sensor sidik jari. Apabila input sidik jari berhasil terverifikasi valid di dalam basis data mikrokontroler, maka layar LCD akan memberikan instruksi agar pengguna melakukan input selanjutnya berupa kartu RFID. Apabila input RFID telah terverifikasi dan dinyatakan valid, maka layar LCD akan menginstruksikan pengguna untuk memberikan input berupa PIN. Apabila ketiga input berhasil dinyatakan valid, sistem akan memutus arus pada modul *relay*, sehingga tuas solenoid ditarik mundur dan pintu terbuka selama 5 detik sebelum mengunci kembali secara otomatis. Sebaliknya, apabila terjadi kegagalan validasi pada salah satu tahap atau pengguna memberikan input yang tidak terdaftar pada basis data, sistem akan langsung menolak akses membunyikan buzzer peringatan, dan me-reset siklus autentikasi ke kondisi awal. Selain mengeksekusi logika verifikasi akses, software dari sistem ini juga diprogram untuk mengelola Jejak Audit (*Audit Trail*). Mikrokontroler memanfaatkan modul Wi-Fi bawaan agar dapat terhubung dengan protokol *Message Queuing Telemetry Transport* (MQTT). Setiap input yang terjadi baik itu akses yang berhasil diotorisasi atau percobaan yang gagal akan langsung dikirimkan oleh mikrokontroler sebagai pesan terenkripsi kepada server broker MQTT. Pesan tersebut kemudian akan diteruskan secara *real-time* menuju Web Dashboard SI-PAKAR dan disimpan secara permanen di dalam pangkalan data MySQL. Integrasi perangkat lunak ini memastikan setiap riwayat akses memiliki catatan waktu (*timestamp*) dan identitas pengguna yang tidak dapat dimanipulasi secara lokal.

Tahapan akhir dari penelitian ini adalah pengujian fungsionalitas dan kinerja sistem. Pengujian fungsionalitas dilakukan menggunakan metode Black Box Testing untuk memvalidasi apakah respons output dari *hardware* sudah berjalan sesuai dengan skenario kombinasi input MFA yang dirancang. Sementara itu, pengujian kinerja kuantitatif dilakukan dengan mengukur response time eksekusi algoritma pemrosesan pada mikrokontroler dan mengukur tingkat tingkat latensi jaringan saat mentransmisikan paket *log data* menuju *dashboard* pemantauan jarak jauh.

3. Hasil dan Pembahasan

3.1 Hasil Perancangan Arsitektur

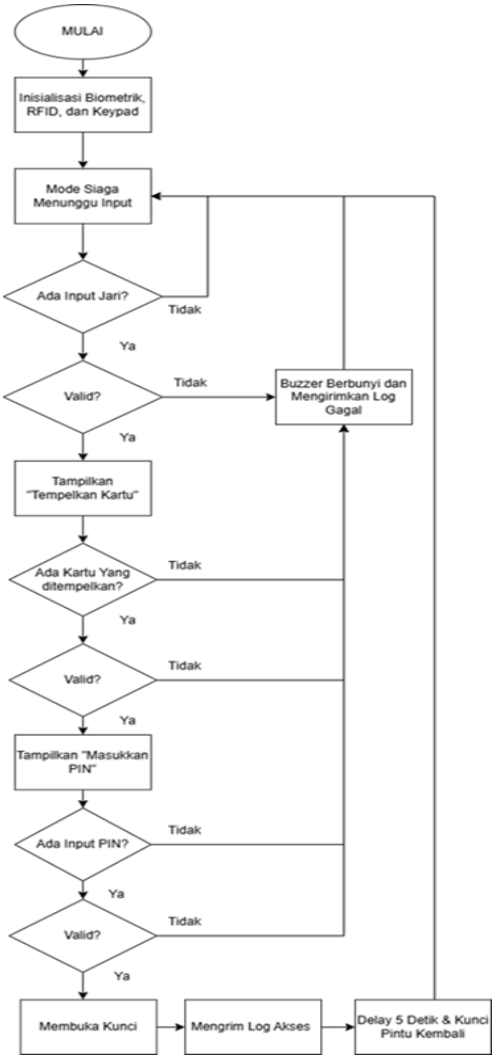
Hasil dari desain arsitektur adalah tata letak perangkat keras dan alur perangkat lunak yang disesuaikan dengan persyaratan keamanan arsip vital [9]. ESP32 adalah pusat komando yang mengelola semua saluran komunikasi tanpa tabrakan data. Pembaca RFID RC522 ditugaskan ke bus SPI, pemindai sidik jari R307 ke bus serial UART, dan antarmuka *keypad* ke pin digital GPIO. disusun dan dipetakan langsung ke pin analog. Sistem kelistrikan dilindungi dengan modul penurunan tegangan untuk menstabilkan tegangan menuju sensor biometrik dan juga untuk melindungi dari lonjakan arus yang dihasilkan oleh tarikan tuas pengunci solenoid 12V. Gambaran dari tata letak purwarupa tersebut ditunjukkan pada Gambar 3.



Gambar 3. Tata Letak Purwarupa Maket Ruang Arsip

Untuk perancangan sisi perangkat lunak, alur eksekusi ini diprioritaskan dan dikhususkan untuk pengelolaan keamanan berlapis melalui sistem *Multi-Factor Authentication* (MFA), dimana alur logika yang mengontrol aksesnya divisualisasikan secara utuh dalam format *flowchart* pada Gambar 4. Implementasi dari sistem ini adalah, sistem akan disetting membuat

siaga penuh (*standby mode*) hingga modul sensor menangkap adanya bentuk interaksi fisik awal dari pengguna. Akses ke dalam ruang arsip tersebut akan diizinkan sepenuhnya untuk bilamana pengguna dapat memvalidasi identitasnya dengan pemindaian sidik jari dan melalui pindaian sidik jari biometrik yang telah tersimpan pada basis data untuk kemudian diikuti dengan proses memasukan kombinasi angka PIN ke dalam *keypad*. Jika semua rangkaian protokol autentikasi tersebut sudah dipastikan valid, maka mikrokontroler akan langsung mengeksekusi untuk menarik tuas pada kunci solenoid, sekaligus mengirimkan *data log* akses keberhasilan secara langsung (*real-time*) melalui protokol transmisi MQTT, kemudian dalam waktu seketika mengunci ulang pintu pengaman tersebut secara otomatis setelah melewati masa jeda selama 5 detik. Jika terjadi kegagalan dalam salah satu tahap dari verifikasi maka hal tersebut akan memicu aktuator *buzzer* untuk membunyikan alarm, dan pada saat yang bersamaan *log* riwayat dari gagal akses tersebut juga akan terkirim dan terekam dalam *server* utama.



Gambar 4. Flowchart Logika Sistem Keamanan MFA

3.2 Pengujian Performa Sistem

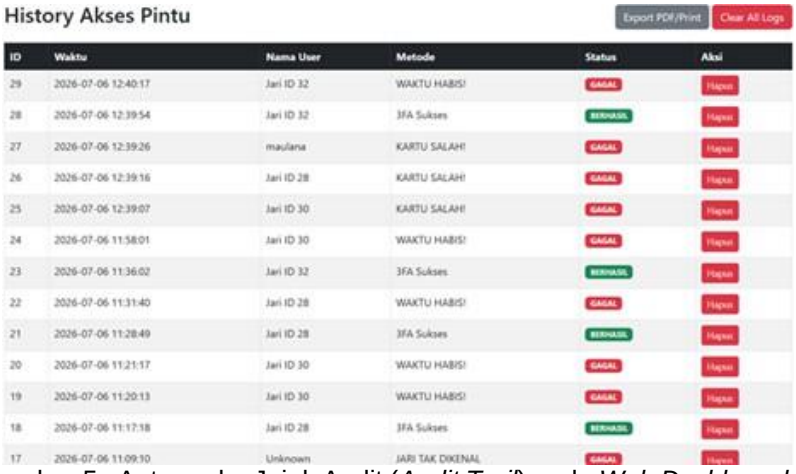
Pengujian pada sistem ini dilakukan menggunakan metode *Black Box Testing* untuk memvalidasi fungsionalitas dari perangkat keras dan algoritma perangkat lunak. Fokus utama dari pengujian ini diarahkan kepada kinerja logika *Multi-Factor Authentication* (MFA) yang diterapkan pada mikrokontroler ESP32. Untuk memenuhi standar dari keamanan ruang arsip, sistem ini dirancang dengan aturan *zero-trust* yang ketat, di mana pengakses diwajibkan untuk

melewati ketiga lapisan keamanan secara berurutan, yakni Faktor Inherensi (Sidik Jari), Faktor Kepemilikan (RFID), dan Faktor Pengetahuan (PIN), dan diakhiri dengan percobaan kegagalan pada salah setiap tahapan guna menguji pembatalan secara langsung proses autentikasi dan sistem akan menolak akses. Pendekatan ini memastikan jaminan keamanan mutlak dari risiko pemindahtanganan maupun pencurian kredensial. Hasil pengujian dari berbagai skenario autentikasi berlapis tersebut dipaparkan secara rinci pada Tabel 1.

Tabel 1. Hasil Pengujian Multi-Factor Authentication (MFA)

Skenario Pengujian	Kombinasi Autentikasi	Respons
Skenario 1	Sidik Jari Valid +Kartu RFID Valid + PIN Valid	Berhasil (Solenoid Terbuka)
Skenario 2	Sidik Jari Valid + Kartu RFID Valid + PIN Salah	Gagal (Akses Ditolak)
Skenario 3	Sidik Jari Valid + Kartu RFID Tidak Valid	Gagal (Akses Ditolak)
Skenario 4	Sidik Jari Tidak Terdaftar	Gagal (Akses Ditolak)
Skenario 5	Sidik Jari Valid (Ditempel Tanpa Kartu/PIN)	Diabaikan

Berdasarkan Tabel 1, mikrokontroler berhasil mengeksekusi instruksi keamanan secara sekuensial sesuai dengan rancangan algoritma. Apabila pengguna berhasil memvalidasi ketiga faktor secara berurutan, ESP32 memutus arus pada *relay*, menarik tuas aktuator solenoid, dan menampilkan pesan keberhasilan pada layar LCD. Sebaliknya, apabila pengguna gagal pada salah satu lapisan, sistem seketika akan menolak akses dan kembali ke mode siaga. Setelah tahapan verifikasi akses di perangkat keras selesai, pengujian dilanjutkan pada keandalan arsitektur jaringan komunikasi menggunakan protokol *Message Queuing Telemetry Transport* (MQTT). Hasil pemantauan menunjukkan bahwa mikrokontroler ESP32 mampu berfungsi sebagai *publisher* yang mentransmisikan paket *data log* secara *real-time* menuju *Web Dashboard* SI-PAKAR tanpa mengalami penundaan yang mengganggu pemrosesan antrean sensor. Setiap aktivitas interaksi di pintu terekam secara persisten di dalam pangkalan data MySQL dan ditampilkan dalam bentuk tabel *Audit Trail*. Pengelola ruang arsip dapat melihat dengan jelas identitas pengguna, metode autentikasi yang digunakan, waktu kejadian (*timestamp*), serta status keberhasilan akses, seperti yang diilustrasikan pada Gambar 2. Hal ini membuktikan bahwa integrasi antara komponen fisik dan perangkat lunak *dashboard* berjalan sinkron dalam memenuhi prinsip nirsangkal dan akuntabilitas fasilitas.



Gambar 5. Antarmuka Jejak Audit (*Audit Trail*) pada *Web Dashboard*

Untuk membuktikan keandalan prototipe, evaluasi sistem tidak hanya sebatas pengujian fungsionalitas, namun juga mencakup analisis performa secara kuantitatif. Pengujian ini difokuskan pada dua metrik utama, yaitu tingkat akurasi pembacaan identitas pada modul *Multi-Factor Authentication* (MFA) dan latensi waktu respons pengiriman data log melalui protokol MQTT.

Pertama, Pengujian akurasi dilakukan pada sensor sidik jari (R307) dan modul RFID (RC522) untuk mengukur tingkat keberhasilan sistem dalam mengenali identitas yang terdaftar, serta kemampuannya dalam menolak identitas asing. Metrik evaluasi yang digunakan meliputi *False Rejection Rate* (FRR) atau penolakan keliru terhadap pengguna yang sah, dan *False*

Acceptance Rate (FAR) atau penerimaan keliru terhadap pihak asing. Pengujian dilakukan sebanyak 50 kali percobaan utnuk masing-masing modul.

Tabel 1. Hasil Pengujian *Multi-Factor Authentication* (MFA)

Komponen Pengujian	Skenario Percobaan	Jumlah Percobaan	Berhasil	False Rejection	False Acceptance
Skenario 1	Sidik Jari Valid +Kartu RFID Valid + PIN Valid	25	24	1	0
Skenario 2	Sidik Jari Valid + Kartu RFID Valid + PIN Salah	25	25	0	0
Skenario 3	Sidik Jari Valid + Kartu RFID Tidak Valid	25	25	0	0
Skenario 4	Sidik Jari Tidak Terdaftar	25	25	0	0
Skenario 5	Sidik Jari Valid (Ditempel Tanpa Kartu/PIN)	25	25	0	0

Berdasarkan tabel 2, tingkat akurasi dari modul RFID mencapai 100% pada rentang jarak baca optimal. Sedangkan sensor sidik jari mencatat tingkat *True Acceptance* sebesar 96% dengan 1 kali penolakan keliru (FRR) yang disebabkan oleh posisi penempatan jari yang kurang tepat pada penampang prisma sensor. Sistem terbukti sangat aman dengan mencatatkan angka 0% untuk *False Acceptance Rate* (FAR), yang berarti tidak ada satupun identitas asing atau tidak terdaftar yang berhasil menembus lapisan validasi fisik

Kedua, Pengujian latensi komunikasi dilakukan untuk memvalidasi klaim efisiensi pengiriman data pencatatan akses menuju server Jejak Audit (*Audit Trail*). Pengukuran waktu tunda (*delay*) menggunakan pendekatan *Round-Trip Time* (RTT) yang diukur mulai dari saat mikrokontroler ESP32 mengeksekusi perintah pengiriman (*publish*) hingga menerima balasan konfirmasi (*acknowledgement*) dari server MySQL. Pengujian dilakukan sebanyak 30 kali percobaan pada kondisi jaringan Wi-Fi standar dengan bandwidth rata-rata 20 MBPS. Hasil rekapitulasi perhitungan waktu latensi disajikan pada Tabel 3.

Tabel 3. Hasil Pengukuran Latensi Pengiriman Data Log MQTT

Parameter Pengukuran	Nilai Waktu (ms)	Keterangan
Jumlah Percobaan (n)	30 Kali	Gabungan pengiriman log akses normal dan darurat
Latensi Minimum (Tercepat)	118ms	Waktu tempuh terbaik
Latensi Maksimum (Terlama)	210ms	Waktu tempuh saat terjadi jeda koneksi.
Rata-Rata Latensi $\bar{x}$	145ms	Dihitung dari formula aritmatika $\frac{\sum Latensi}{n}$
Packet Deliver Ratio	100%	Seluruh 30 paket data berhasil diterima dan tersimpan di MySQL

Berdasarkan Tabel 2, sistem memperoleh nilai rata-rata latensi sebesar 145 ms dengan tingkat keberhasilan pengiriman paket (*Packet Delivery Ratio*) mencapai 100%. Menurut standar telekomunikasi ITU-T G.114 mengenai kualitas layanan jaringan, latensi di bawah 150 ms dikategorikan sebagai sangat baik (*excellent*) dan berada jauh di bawah ambang batas toleransi sistem pemantauan *real-time* yaitu 1000 ms (1 detik). Hasil ini membuktikan secara kuantitatif bahwa protokol MQTT sangat ringan dan stabil dijalankan pada arsitektur ESP32 tanpa menyebabkan overhead memori ataupun kegagalan transmisi *data log* ke basis data MySQL

3.3 Pembahasan

Sebagai hasil evaluasi keseluruhan, sistem keamanan MFA berbasis IoT ini memiliki beberapa kelebihan dan kelemahan. Kelebihan utama dari sistem ini terletak pada arsitektur

Vol.7, No. 2, Desember 2026, 671 - 680

keamanan wajib tiga lapis yang memberikan jaminan perlindungan *zero-trust* tingkat tertinggi, sehingga fasilitas benar-benar terisolasi dari berbagai vektor ancaman duplikasi akses. Pengalihan beban pemrosesan pencocokan pola (*template matching*) pada modul R307 mandiri juga menjaga performa ESP32 tetap responsif saat mengeksekusi algoritma sekuensial. Di sisi lain, sistem ini memiliki kelemahan pada aspek kenyamanan pengguna (*usability*) dan ketergantungan perangkat keras. Proses pembukaan pintu membutuhkan waktu interaksi yang sedikit lebih lama dibandingkan sistem konvensional. Selain itu, karena algoritma mewajibkan ketiga parameter bernilai valid, kerusakan fisik pada salah satu antarmuka masukan, seperti layar pemindai jari yang kotor atau sensor RFID yang tergores, akan mengakibatkan pintu tidak dapat diakses sama sekali secara reguler, kecuali menggunakan mekanisme tombol darurat dari dalam ruangan.

4. Kesimpulan

Berdasarkan hasil perancangan dan pengujian yang telah dilakukan, dapat disimpulkan bahwa sistem keamanan ruang arsip berbasis *Internet of Things* (IoT) menggunakan mikrokontroler ESP32 telah berhasil diimplementasikan dengan menerapkan logika *Multi-Factor Authentication* (MFA) secara sekuensial. Penerapan aturan *zero-trust* yang mewajibkan pengguna untuk memvalidasi tiga lapisan keamanan secara berurutan, yaitu pemindaian sidik jari, kartu RFID, dan PIN, terbukti mampu meningkatkan standar keamanan secara absolut dan memenuhi prinsip nirsangkal (*non-repudiation*). Berdasarkan pengujian, sistem berhasil menjalankan logika autentikasi tiga lapis (MFA) ini secara sekuensial untuk mengeliminasi pencurian kredensial, dengan tingkat akurasi pembacaan RFID mencapai 100% dan sensor sidik jari sebesar 96%. Selain itu, sistem pelaporan Jejak Audit (*Audit Trail*) juga beroperasi dengan optimal melalui transmisi protokol MQTT. Pelaporan rekam jejak akses beroperasi secara *real-time* dengan rata-rata latensi pengiriman 145 ms dan rasio keberhasilan 100% tanpa membebani pemrosesan mikrokontroler. Keunggulan utama dari sistem ini adalah terciptanya lapisan pertahanan ganda (*defense in depth*) yang sepenuhnya mengeliminasi risiko pemindahtanganan kredensial. Namun demikian, perlindungan berlapis ini membuat durasi pembukaan pintu menjadi lebih lama dan memiliki risiko kegagalan akses total apabila salah satu sensor antarmuka mengalami kerusakan fisik.

Berdasarkan kelemahan dan temuan selama penelitian, terdapat beberapa saran untuk pengembangan sistem pengamanan di masa mendatang. Penelitian selanjutnya disarankan untuk mengintegrasikan sistem catu daya cadangan mandiri, seperti *Uninterruptible Power Supply* (UPS), agar modul keamanan pintu dan konektivitas jaringan tetap beroperasi optimal saat terjadi pemadaman listrik terpusat. Selain itu, pengembangan fitur autentikasi sekunder berbasis perangkat lunak, seperti pengiriman *One-Time Password* (OTP) melalui aplikasi pesan terenkripsi, sangat direkomendasikan untuk ditambahkan. Fitur tersebut dapat berfungsi sebagai jalur akses darurat (*backup bypass*) untuk pengelola ruang arsip apabila salah satu sensor fisik pemindai mengalami malfungsi, tanpa harus mengorbankan standar akuntabilitas pelaporan dari sistem utama.

Ucapan Terima Kasih (Opsional)

Penulis menyampaikan ucapan terima kasih kepada Program Studi Informatika, Fakultas Ilmu Komputer, Universitas Pembangunan Nasional "Veteran" Jawa Timur atas dukungan fasilitas dan lingkungan akademik yang kondusif sehingga penelitian mengenai arsitektur keamanan ruang arsip berbasis IoT ini dapat diselesaikan dengan baik. Terima kasih juga diucapkan kepada rekan-rekan mahasiswa yang telah memberikan bantuan teknis dan masukan selama proses perancangan prototipe

Referensi

[1] D. Adidrana, H. Suryoprago, and A. R. Hakim, “Perancangan Sistem Smart Door Lock Menggunakan Internet of Things,” *IJCT*, 2023.

[2] M. W. Aryadi, L. K. R. Arthana, and P. H. Suputra, “Smart Lock System Berbasis IoT Menggunakan ESP32 untuk Keamanan Akses Pusat Data,” *Jurnal Informatika dan Teknik Elektro Terapan*, vol. 14, no. 1, 2026.

[3] M. A. Aziz, T. Sutikno, H. Yuliansyah, A. I. Dewi, Y. E. Rohmadi, and D. Setiawati, “Vulnerability Analysis of Smart Lock Using NIST SP 800-115 Method,” *Jurnal Penelitian*

Pendidikan IPA, vol. 11, no. 8, pp. 264–272, 2025.
[4] I. Joshua and D. W. Chandra, “Analisis Logging dan Auditing Akses Database SQL Melalui Koneksi Remote Menggunakan Anydesk,” 2023.
[5] Kompas, “Kejar Ayam Sampai Masuk Ruang Arsip PT KAI 2 Pengemis Curi 100 Bal Dokumen Senilai Rp 30 Juta,” *Kompas.com*, 2023.
[6] A. Kurnianto, J. D. Irawan, and F. X. Ariwibisono, “Penerapan IoT untuk Controlling Lampu Menggunakan Protokol MQTT Berbasis Web,” *JATI*, 2023.
[7] B. B. Mangata, D. I. N'kashama, P. B. Christian, and D. K. Muamba, “Comparative Studies Between a Facial Recognition System and a Fingerprint Recognition System for Access Control,” *IJISCS*, 2022.
[8] A. Ometov et al., “Multi-Factor Authentication: A Survey,” *Cryptography*, 2018.
[9] UU, “Undang-Undang Republik Indonesia,” UU No. 43 Tahun 2009 Tentang Kearsipan. Republik Indonesia, 2009.
[10] Rismawati, S. Paembonan, and R. Suppa, “Rancang Bangun Keamanan Pintu Otomatis Menggunakan E-KTP Berbasis Arduino Uno,” *JITET*, vol. 12, no. 3, pp. 2352–2364, 2024.
[11] E. Schiavone, A. Ceccarelli, and A. Bondavalli, “Continuous Biometric Verification for Non-Repudiation of Remote Services,” in *Proceeding 12th International Conference on Availability, Reliability and Security*, 2017.
[12] D. Setiawan, B. Rahmat, and W. S. Saputra, “IoT Pengendalian Keamanan Pintu Rumah Otomatis Menggunakan E-KTP Berbasis Mikrokontroler ESP32,” *JITEK*, 2023.
[13] J. S. Sonamoni et al., “IoT-Based Smart Remote Door Lock and Monitoring System Using an Android Application,” *Eng. Proc.*, vol. 76, no. 1, p. 85, 2024.
[14] A. A. Zainuddin et al., “Innovative IoT Smart Lock System: Enhancing Security with Fingerprint and RFID Technology,” *Malays. J. Sci. Adv. Technol.*, 2024.
[15] M. Zen, Irwan, Hafni, and M. D. P. Ananda, “Implementasi dan Pengujian Menggunakan Metode BlackBox Testing pada Sistem Informasi Tracer Study,” *Bull. Comput. Sci. Res.*, 2024.