Perancangan Arsitektur Keamanan Ruang Arsip Berbasis IoT Menggunakan Autentikasi Multi-Faktor dan Audit Trail

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

[1]Program Studi Informatika/Fakultas Ilmu Komputer
Universitas Pembangunan Nasional "Veteran" Jawa Timur
Surabaya, Indonesia
[1*]22081010045@student.upnjatim.ac.id

[2]Program Studi Informatika/Fakultas Ilmu Komputer
Universitas Pembangunan Nasional "Veteran" Jawa Timur
Surabaya, Indonesia
[2]ajiputra@upnjatim.ac.id

[3]Program Studi Informatika/Fakultas Ilmu Komputer
Universitas Pembangunan Nasional "Veteran" Jawa Timur
Surabaya, Indonesia
[3]ardhon.rakhmadi.fasilkom@upnjatim.ac.id

***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 serta memantau kondisi lingkungan 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 sekaligus membaca indikator dari sensor keselamatan (suhu, asap, dan api). 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 lunakyang 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. Desain sistem ini juga telah menerapkan mekanisme fail-safe. Yang artinya ketika sistem mendeteksi adanya potensi bahaya, maka sistem akan mengabaikan protokol keamanan dan otomatis membuka kunci pintu agar evakuasi darurat dapat lebih mudah dilakukan. Kesimpulannya, arsitektur sistem ini telah dirancang agar mampu menutup celah akses ilegal serta menjamin akuntabilitas riwayat akses dan tetap memprioritaskan keselamatan manusia apabila terjadi bencana.**
Kata kunci— Ruang Arsip, Jejak Audit, Internet of Things. Autentikasi Multi-Faktor, Keamanan Fisik

***Abstract*— Traditional physical keys have numerous vulnerabilities and are no longer considered adequate for securing vital state documents stored in archive rooms. This is due to several factors, such as the risk of key duplication and the lack of automated access tracking. These factors constitute a critical security vulnerability. Therefore, this research proposes the design of an Internet of Things (IoT)-based integrated security system that tightly restricts entry access and monitors the environmental conditions of the archive room. The approach utilized in this study layered protection through Multi-Factor Authentication (MFA). The system requires users to pass a strict combination of verifications: a biometric fingerprint sensor, RFID, and PIN code input. A microcontroller, acting as the control center, manages the entire authentication process while simultaneously reading indicators form safety sensors (temperature, smoke, and fire). In the hardware design, the prototype is divided into four functional zones: exterior, interior, ceiling, and panel box. This zoning allows for concealed cable routing, thereby reducing the probability of physical sabotage. The software integrated into this system enables accurate logging of every access 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. The system design also incorporates a fail-safe mechanism. This means that when the system detects a potential hazard, it overrides the security protocols and automatically unlocks the door to facilitate easier emergency evacuation. In conclusion, the architecture of this system is designed to eliminate unauthorized access vulnerabilities. Guarantee the accountability of access history, and prioritize human safety in the event of disaster.**
Keywords— Archive Room, Audit Trail, Internet of Things, Multi-Factor Authentication, Physical Security

I. PENDAHULUAN

Ruang arsip merupakan aset vital bagi sebuah perusahaan atau institusi. Hal ini dikarenakan ruang arsip berfungsi untuk menjaga memori kolektif data rahasia, serta dokumen yang memiliki kekuatan hukum tinggi [16]. Pengelolaan aset penting dengan benar merupakan mandat hukum yang tertera pada Undang-Undang Republik Indonesia Nomor 43 Tahun 2009, dimana negara berkewajiban melindungi dan melestarikan arsip sebagai identitas bangsa [1]. Karena dokumen arsip yang memiliki sifat tidak tergantikan, maka akses terhadap fasilitas ini menuntut penerapan prinsip nirsangkal (*non-repudiation*) yang mutlak. Identitas setiap

orang yang mengakses ruangan tersebut harus terverifikasi secara akurat demi menjamin akuntabilitas yang tidak dapat dibantah [2].

Namun, kebanyakan sistem keamanan ruang arsip saat ini bergantung pada kunci fisik tradisional atau kartu akses tunggal. Kelemahan yang dimiliki oleh kunci fisik sangat fatal. Kunci fisik sangat mudah untuk diduplikasi, dibobol, dan tidak mampu untuk merekam riwayat akses sama sekali [4]. Disisi lain, teknologi *Radio Frequency Identification* (RFID) menawarkan efisiensi digital, namun teknologi ini masih memiliki celah yaitu resiko data yang dapat ditransfer (*transferable risk*). Pada kondisi ini, kartu akses dapat dipinjamkan atau dicuri, sehingga meningkatkan kemungkinan untuk pihak yang tidak berwenang dapat mengakses ruangan tanpa terdeteksi sebagai pemilik yang sah [5]. Lemahnya sistem keamanan ruang arsip memiliki dampak yang nyata. Hal ini diperkuat dengan insiden pencurian 100 bal dokumen di gudang arsip PT KAI. Pencurian ini membuktikan bahwa betapa rentannya titik akses yang tidak diawasi dengan ketat [6]. Selain itu, terdapat ancaman lain seperti resiko terjadinya kebakaran. Kebakaran yang terjadi di Gedung Kementerian ATR/BPN pada awal 2025 [7] merupakan sebuah bukti nyata bahwa sistem keamanan dianjurkan untuk dapat melakukan integrasi aspek perlindungan fisik wajib yang selaras dengan prinsip CIA Triad: *Confidentiality* (Kerahasiaan), *Integrity* (Integritas), dan *Availability* (Ketersediaan). Kerahasiaan menjamin bahwa hanya pemilik akses yang sah yang memiliki akses pada ruangan tersebut, sementara integritas memastikan bahwa dokumen tersebut tetap utuh. Aspek ketersediaan pun memiliki peran yang sangat krusial, terutama saat terjadi situasi yang darurat di mana akses evakuasi harus terbuka cepat bagi petugas yang berwenang [13].

Implementasi sistem berbasis IoT menjawab tantangan ini dengan menyediakan kontrol akses sekaligus pemantauan ancaman lingkungan secara aktif dan reaktif. Beberapa penelitian terdahulu telah mencoba melakukan penerapan teknologi *smart lock* dengan biometrik canggih seperti pengenalan wajah. Namun, metode ini terbatasi oleh kendala teknis yang apabila dijalankan pada mikrokontroler ESP32 yang memiliki keterbatasan memori dan daya komputasi [9]. Selain itu, akurasi kamera sangat bergantung pada pencahayaan ruang tersebut, di sisi lain, area ruang arsip seringkali ditemui memiliki cahaya yang minim [12]. Sebagai alternatif yang lebih optimal, sensor sidik jari menawarkan stabilitas yang tinggi pada berbagai kondisi cahaya serta memiliki unit pemrosesan mandiri yang tidak membebani memori utama mikrokontroler [8].

Keandalan sistem IoT juga sangat bergantung pada protokol komunikasi. Protokol *Message Queuing Telemetry Transport* (MQTT) terbukti sangat efisien untuk mikrokontroler karena arsitekturnya yang ringan [11].Apabila diba- -ndingkan dengan permintaan HTTP tradisional yang memakan banyak *bandwidth* dan daya, MQTT mampu menjaga koneksi persisten dengan latensi yang rendah [14].Hal ini memastikan bahwa setiap notifikasi dapat terkirim ke dasbor pemantauan dalam hitungan detik [15].

Agar standar keamanan *zero-trust* dapat terwujud, penelitian ini mengusulkan penerapan *Multi-Factor Authentication* (MFA) yang menggabungkan tiga pilar utama: faktor bawaan (sidik jari), faktor kepemilikan (kartu RFID), dan faktor pengetahuan (kode PIN) [10]. Arsitektur ini dijalankan oleh mikrokontroler ESP32 untuk meminimalisir adanya satu titik kegagalan (*single point of failure*) [19]. Sebagai lapisan akhir, sistem ini dilengkapi dengan Jejak Audit digital. Berbeda dengan log manual yang rentan terhadap manipulasi fisik [17], log digital yang tersimpan dalam basis data MySQL akan mencatat seluruh interaksi secara permanen dan transparan.

II. TINJAUAN PUSTAKA

A. *Penelitian Terdahulu*

Guna memposisikan penelitian ini di antara studi dan penelitian yang telah ada, dilakukan tinjauan terhadap beberapa literatur terkait sistem *smart lock*. Tabel 1 menguraikan perbandingan antara

penelitian terdahulu dengan arsitektur yang diusulkan pada penelitian ini

Tabel 1. Perbandingan Penelitian Terdahulu

Peneliti & Tahun	Fokus Penelitian	Metode/ Komponen Utama	Keterbatasan dan Kebaruan Sistem
Rismawati et al. (2024) [3]	Keamanan pintu otomatis menggunakan E-KTP.	Arduino Uno, RFID RC522 (E-KTP).	Hanya bergantung pada satu faktor autentikasi fisik, sehingga memiliki celah keamanan *transferable risk* (kartu dapat dicuri/dipinjamkan).
Aryadi et al. (2026) [13]	*Smart lock system* berbasis IoT untuk pusat data.	Mikrokontroler ESP32.	Berfokus pada kontrol akses jarak jauh, namun belum menerapkan autentikasi berlapis dan ketiadaan fitur mitigasi keselamatan.
Mangata et al. (2022) [9]	Studi komparasi antara sistem pengenalan wajah dengan sidik jari.	Sensor sidik jari dan modul pengenalan wajah.	Penelitian ini hanya merupakan evalusai dari performa biometrik dan belum diimplementaskan k edalam arsitektur ruang arsip terintegrasi.
Penelitian ini (2026)	Arsiektur keamanan ruang arsip berbasis IoT MFA & Audit Trail.	ESP32. R307 (Sidik Jari), RFID, PIN, Sensor Lingkungan (MQ-2, DHT22, Flame Sensor), MQTT, MySQL.	Menerapkan Autentikasi Multi Faktor mutlak, rekam jejak adigital yang tidak dapat disangkal (*non-repudiation*), serta mekanisme *fail-safe* otomatis untuk evakuasi bencana.

Berdasarkan tabel 1, kekurangan utama dari sistem-sistem yang telah dirancang sebelumnya tereletak pada ketergantungan terhadap lapisan autentikasi tunggal dan kurangnya integrasi dengan aspek keselamatan lingkungan. Penelitian ini menutupi celah-celah tersebut dengan membawa kebaruan (*novelty*) berupa implementasi *Multi-Factor Authentication* (MFA) yang menggabungkan faktor bawaan (sidik jari), kepemilikan (RFID), serta pengetahuan (PIN) yang dieksekusi pada mikrokontroler ESP32. Selain itu, arsitektur yang dirancang memiliki keunggulan tambahan berupa mekanisme *fail-safe* untuk mitigasi kebakaran dan pencatatan Jejak Audit (*Audit Trail*) secara *real-time* melalui protokol MQTT menuju basis data MySQL, guna menjamin prinsip *non-repudiation* pada pengarsipan dokumen.

B. Landasan Teori

1. Keamanan Ruang Arsip dan Prinsip Nirsangkal

Ruang arsip bukan sekadar tempat menaruh kertas, melainkan fasilitas yang menyimpan dokumen-dokumen yang menuntut perlindungan mutlak. Dalam kacamata keamanan informasi, setiap orang yang masuk ke area sensitif harus memenuhi prinsip nirsangkal (*non-repudiation*). Artinya, identitas mereka wajib terverifikasi secara pasti dan tercatat dalam sebuah basis data yang tidak bisa diubah-ubah[2]. Sayangnya, banyak solusi kunci pintar di pasaran lebih mementingkan kemudahan pengguna rumahan dan melupakan fitur pencatatan log yang lengkap. Padahal, institusi kearsipan sangat membutuhkan Jejak Audit (*Audit Trail*) digital untuk memenuhi standar akuntabilitas dan audit modern.

2. Multi-Factor Authentication

Tren sistem kontrol akses kini mulai meninggalkan *keypad* angka atau kartu tunggal dan beralih ke sistem keamanan berlapis. Ketergantungan pada satu faktor seperti kartu akses atau PIN memiliki celah keamanan yang disebut sebagai *transferable risk*, di mana token fisik tersebut sangat mudah hilang, dicuri, atau dipnjamkan kepada pihak yang tidak berwenang [5].

Multi-Factor Authentication merupakan solusi yang hadir dengan mengharuskan pengguna untuk melewati kombinasi verfikasi mutlak. Prinsip kerja MFA didasarkan pada tiga pilar utama keamanan:

A. Faktor Bawaan: Unsur biometrik unik yang melekat pada tubuh pengguna, seperti sidik jari.
B. Faktor Kepemilikan: Objek fisik yang dimiliki oleh pengguna, seperti kartu RFID.
C. Faktor Pengetahuan: Informasi rahasia yang hanya dapat dimiliki dan diingat oleh pengguna, seperti kode PIN.

Menggabungkan ketiga faktor ini terbukti mampu menciptakan tembok pertahanan kontrol akses yang sangat

kuat [10].

3. *Internet of Things (IoT dan Protokol MQTT*

Pemanfaatan *Internet of Things* (IoT) membuat sistem keamanan tradisional naik kelas karena status pintu yang bisa dipantau dari jauh secara *real-time* [13]. Dalam merancang sistem IoT yang diotaki mikrokontroler, faktor pemilihan protokol komunikasi sangat menentukan kelancaran data. Kurnianto et al. [11] dan Kristiyanti et al. [14] sudah membuktikan keandalan protokol *Message Queuing Telemetry Transport* (MQTT) untuk mengirim data telemetri sensor. Arsitektur MQTT ini sangat ringan dan tidak rakus daya seperti model permintaan HTTP biasa. Protokol ini sanggup menahan koneksi agar tetap menyala dengan tingkat latensi yang rendah. Alhasil, notifikasi log pintu maupun peringatan bahaya dari sensor bisa langsung muncul di *dashboard server* dalam hitungan detik.

4. *Mekanisme Fail-Safe dan Mitigasi Bencana*

Mengamankan area vital tidak boleh hanya berfokus pada cara mencegah penyusup, tapi juga harus memikirkan keselamatan nyawa personel. Desainer sistem keamanan selalu dihadapkan pada titik keseimbangan antara menjaga Kerahasiaan (*Confidentially*), Ketersediaan akses (*Availability*). Pintu elektronik yang dikunci terlalu kuat justru berpotensi berubah menjadi jebakan maut ketika terjadi kebakaran [7]. Maka dari itu, sistem keamanan cerdas wajib memiliki alat pemantauan lingkungan (seperti sensor pendeteksi asap dan api) yang diikat dengan mekanisme *fail-safe*. Lewat mekanisme ini, sistem bisa langsung mengambil alih kendali dan membuka tuas pintu pengaman secara otomatis agar petugas di dalam ruangan bisa segera melakukan evakuasi darurat.

5. *Komponen Mikrokontroler dan Sensor*

Agar arsitektur konseptual ini bisa beroperasi dengan stabil, pemilihan spesifikasi perangkat keras menjadi pondasi utama yang tidak bisa ditawar [19].

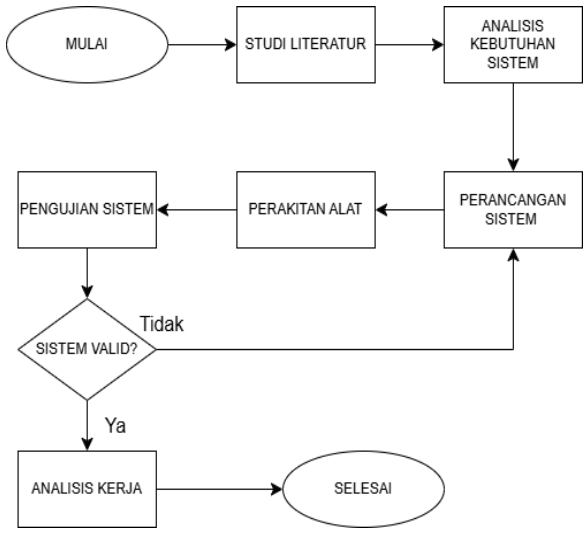
A. Mikrokontroler ESP32: Bertindak sebagai jantung pemrosesan. Modul Wi-Fi yang menyertai *chip* ini juga memiliki kelebihan untuk dapat mengeksekusi skema autentikasi yang rumit sambil mengirim *data log* MQTT ke internet secara *real-time.* [20].
B. Sensor Biometrik R307 dan Modul RFID RC522: R307 adalah pemindai sidikjari optikal yang melakukan pencocokan pola identitas sidik jari dalam modul itu sendiri, beban kerja pada ESP32 pun menjadi jauh lebih ringan [8]. Sementara itu, RC522 juga memancarkan frekuensi 13,56 MHz untuk membaca token *Radio Frequency Identification* (RFID) [21]. Keduanya adalah penjaga gerbang pertama pada lapisan validasi fisik.
C. Sensor Lingkungan (DHT22, MQ-2, dan Flame Sensor): Komponen ketiga ini sebagai nyawa utama dalam pekerjaan mitigasi bencana. Sensor DHT22 Mengukur Dalam Memeriksa Perubahan Suhu dan Kelembaban Ekstrim Secara Digital [23]. Sensor MQ-2 disiapkan untuk mendeteksi gas mudah terbakar yang meningkatkan atau sekawanan asap [24]. Sebagai validasi terakhir untuk ancaman kebakaran, Flame Sensor akan mendeteksi gelombang inframerah yang dihasilkan oleh asap [25].

III. METODOLOGI PENELITIAN

Pengerjaan riset ini mengadopsi pendekatan *Research and Development* (R&D) yang secara khusus difokuskan pada tahap perancangan arsitektur dan pembuatan purwarupa sistem [26]. 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:

1. Studi Literatur

   Fase ini berfokus pada pengkajian literaratur 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 dan mekanisme *fail-safe.*

2. 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), serta sensor lingkungan tanpa menyebabkan antrean data

3. Perancangan Sistem

   Pada tahap ini 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, alur logika mekanisme *fail-safe*, serta relasi basis data MySQL untuk kebutuhan *Audit Trail*.

4. Perakitan Alat

   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.

5. Pengujian dan Validasi Sistem

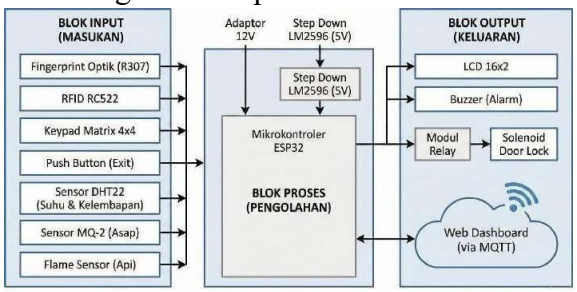
   Pengujian dilakukan secara empiris untuk memastikan sistem berjalan sesuai dengan skenario yang diharapkan. Metode pengujian mencakup *Black-Box testing* untuk memvalidasi fungsi *input-output* sensor, simulasi pemicuan bahaya kebakaran (asap dan api), serta pengujian kecepatan pengiriman paket data log akses ke basis data. Tahap ini juga memcakup evaluasi iteratif, apabila ditemukan *error* atau ketidaksesuaian *output* atau latensi yang terlalu tinggi, maka proses akan dikembalikan ke tahap Perancangan Sistem untuk perbaikan *hardwar*e 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.

6. Analisis Kerja

   Tahap ini 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.

Sebagai penjabaran lebih lanjut dari tahap Perancangan dan Perakitan Sistem, arsitektur

integrasi perangkat keras divisualisasikan melalui diagram blok pada Gambar 2.



Gambar 2. Diagram Blok Sistem Keamanan Terintegrasi

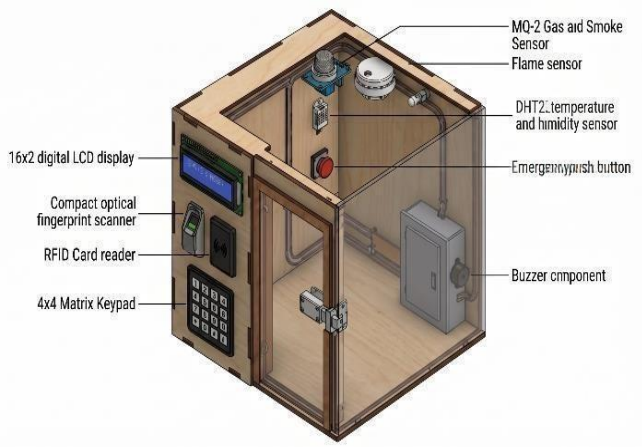
Secara fungsional, penulis telah merancang pondasi perangkat lunak dengan menyematkan mekanisme keamanan yang berupa interupsi yang memprioritaskan penyelamatan nyawa. Jika sensor mendeteksi tanda-tanda kebakaran seperti asap tebal atau panas ekstrem, ESP32 diprogram untuk memutus sirkuit solenoid dan membuka pintu secara otomatis (*auto-unlock*). Sambil memastikan akuntabilitas akses, protokol MQTT digunakan sebagai jalur transmisi untuk mengirim semua *log* aktivitas ke *server* basis data MySQL secara *real-time.*

IV. HASIL DAN PEMBAHASAN

A. Hasil Perancangan Arsitektur

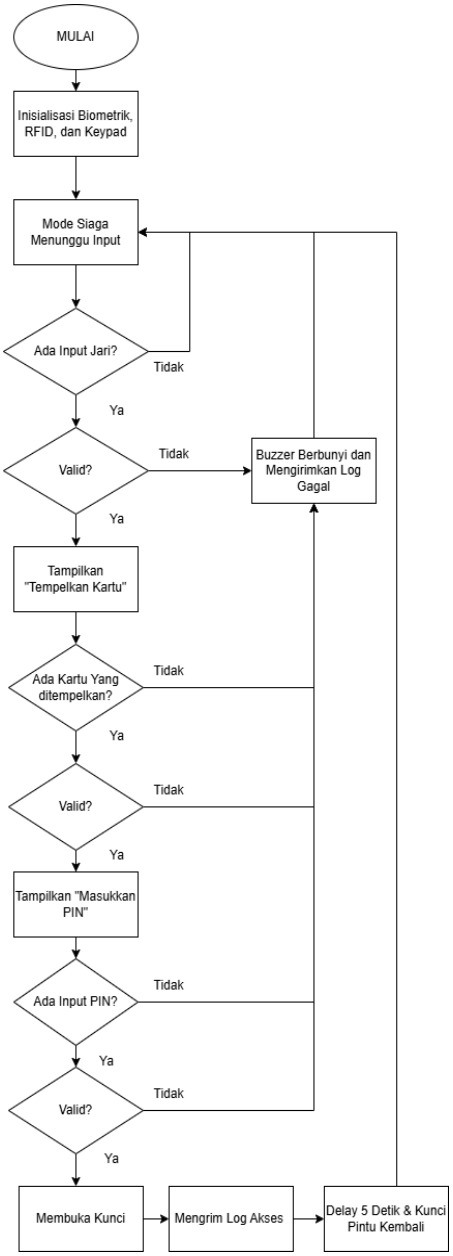
Hasil dari desain arsitektur adalah tata letak perangkat keras dan alur perangkat lunak yang disesuaikan dengan persyaratan keamanan arsip vital [31]. ESP32 adalah pusat komando yang mengelola semua saluran komunikasi tanpa tabrakan data. Pembaca RFID RC522 ditugaskan ke bus SPI, pemindai sidik jari R307 ke bus serial UART, dan antarmuka *keypad* ke pin digital GPIO. Sensor suhu DHT22 [23], detektor asap MQ-2 [24], dan sensor kebakaran [25] 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. Secara fisik, arsitektur ini diimplementasikan dalam desain profil (*mockup*) ruang arsip yang dipisahkan menjadi empat area fungsional (eksterior, interior, langit-langit, dan panel tertutup) yang dirancang untuk mengurangi risiko sabotase fisik. [28]. Gambaran dari tata letak purwarupa tersebut ditunjukkan pada Gambar 2.

Gambar 3. Gambaran Tata Letak Purwarupa Maket Ruang Arsip



Untuk perancangan sisi perangkat lunak, pada arsitektur dari algoritma dibagi secara terstruktur ke dalam dua bagian alur eksekusi utama untuk melakukan *workload distribution* pada mikrokontroler. Pertama, dua 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 3. Salah satu 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 kartu RFID 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

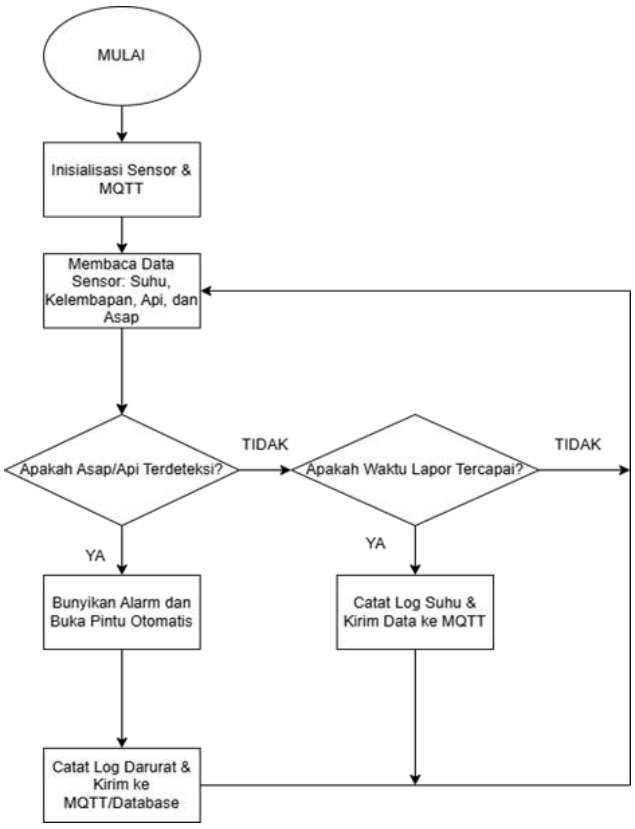
Alur eksekusi kedua dikhususkan untuk operasi keamanan dan merupakan proses paralel seperti yang ditunjukkan pada Gambar 4. Mikrokontroler melakukan perulangan konstan untuk membaca data sensor suhu, kelembaban, asap, dan api. Jika lingkungan normal, sistem hanya akan mengirimkan data telemetri secara berkala ke MQTT. Tetapi jika mendeteksi asap tebal atau percikan api, sistem akan langsung membunyikan alarm dan membuka pintu secara paksa (*auto-unlock*) tanpa menunggu verifikasi kunci MFA. Catatan darurat ini juga segera dikirim ke basis data untuk investigasi kedepannya.

Gambar 5. Flowchart Logika Pemantauan Lingkungan dan Fail Safe

B. Pengujian Performa Sistem

Untuk membuktikan keandalan *prototype*, 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 Authenticatiion* (MFA) dan latensi waktu respons pengiriman data log melalui protokol MQTT.

1. Analisis Akurasi Sensor Autentikasi
   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 2. Hasil Pengujian Akurasi Sensor Autentikasi

Komponen Pengujian	Skenario Percobaan	Jumlah Percobaan	Berhasil	False Rejection	False Acceptance
Sidik Jari (R307)	Jari Terdaftar	25	24	1	0
	Jari Tidak Terdaftar	25	25	0	0
RFID (RC522)	Kartu Terdaftar	25	25	0	0
	Kartu Tidak Terdaftar	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.

2. Analisis Latensi Transmisi MQTT

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 2.

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 Delivery 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. Analisis Respons Sensor Lingkungan dan Mekanisme *Fail-Safe*

Untuk memvalidasi aspek Ketersediaan (*Availability*) dan keselamatan manusia pada situasi darurat, dilakukan pengujian fungsionalitas dan waktu respons terhadap rangkaian sensor lingkungan. Pengujian dilakukan dengan melakukan simulasi peningkatan suhu, paparan asap (menggunakan asap pembakaran kertas terukur), serta paparan sumber api langsung pada jarak tertentu di dalam maket purwarupa. Tujuan utama pengujian ini adalah membuktikan bahwa fungsi interupsi (*override*) pada mikrokontroler ESP32 mampu

menjalankan mekanisme fail-safe (*auto-unlock* pintu) saat parameter lingkungan melewati ambang batas bahaya (*threshold*). Hasil pengujian disajikan pada Tabel 3.

Tabel 4. Hasil Pengujian Respons Sensor Lingkungan

Komponen Sensor	Skenario Pengujian	Ambang Batas (Threshold)	Respons Sistem	Waktu Eksekusi	Hasil Pengujian
Suhu (DHT22)	Kondisi Ruangan Normal	Suhu <35	Stattus Pintuu Normal, Mengirim data secara berkala	-	VALID
	Simulasi Suhu Ekstrem	Suhu <45	Mengirim peringatan suhu tinggi ke Dashboard &Database	<1 detik	VALID
Asap/ Gas (MQ-2)	Udara Bersih	Kadar <300 PPM	Status Normal		VALID
	Paparan Asap Tebal	Kadar >300 PPm	Buzzer Berbunyi, Solenoid Terbuka, Mengirim Log Darurat	1 detik	VALID
Api (Flame Senso)	Tidak Ada Gelombang IR	Nilai Analog Normal	Stattus Normal	-	VALID
	Paparan APi (Jarak , <20cm	Deteksi Gelombang IR	Buzeer Berbunyi, Solenoid Terbuka, Mengirim Log Darurat	1 detik	VALID

Berdasarkan Tabel 3, seluruh sensor lingkungan terbukti mampu merespons perubahan kondisi fisik ruangan dengan keakuratan 100%. Yang paling krusial, ketika sensor MQ-2 mendeteksi kepekatan asap di atas 300 PPM atau ketika *Flame Sensor* menangkap paparan gelombang inframerah dari percikan api, mikrokontroler ESP32 langsung mengeksekusi protokol *fail-safe*.
Sistem secara otomatis memutus arus pada *solenoid door lock* sehingga pintu terbuka secara otomatis (*auto-unlock*) dengan waktu respons eksekusi sangat cepat, yaitu 0,5 hingga 1,2 detik. Dalam kondisi darurat ini, sistem terbukti mengabaikan (*override*) seluruh persyaratan validasi kunci MFA, membuktikan komitmen desain arsitektur yang menempatkan keselamatan nyawa manusia sebagai prioritas mutlak melampaui kerahasiaan dokumen arsip.

C. Pembahasan

Berdasarkan hasil rancangan logika dari perangkat lunak yang penjelasan lengkapnya dapat dilihat pada Gambar 3 dan Gambar 4, dengan arsitektur sistem ini adalah solusi perlindungan yang menyeluruh dibandingkan dengan pengamanan pada ruang arsip tradisional.

Pertama, suatu penerapan berlapis dari proses *sequence* MFA (Gambar 3) dapat menutupi kelemahan sebagian besar komponen terkait. Jika pembobol berhasil mencuri kartu RFID korban (*transferable risk*), pintu tidak akan terbuka juga karena sistem akan meminta pengguna untuk melakukan verifikasi biometrik. Penambahan fitur delay 5 detik untuk penguncian otomatis juga sangat efektif untuk menghilangkan potensi kesalahan pengamanan yang disebabkan human error, seperti pengguna yang lupa untuk mengunci pintu lagi setelah masuk.

Kedua, pemisahan *flow control fail-safe* (Gambar 4) paralel (*multitasking*) ini membuktikan keseimbangan antara memastikan keamanan dokumen dan keselamatan manusia. Mikrokontroler tidak perlu menunggu pengguna berada di depan pintu untuk mendeteksi atau menyadar adanya bahaya. Ketika tingkatan kadar api dan asap telah mencapai ambang batas yang ditentukan, protokol keamanan level tertinggi akan diabaikan. Karena pintu ruang arsip dapat terbuka otomatis (*auto-unlock*), maka ruang arsip yang terkunci rapat tak akan menjadi perangkap maut bagi petugas ketika insiden darurat terjadi [7].

Ketiga, arsitektur ini mengatasi kelemahan utama dari sistem pengamanan tradisional yaitu ketiadaan rekam jejak aktivitas. Seluruh interaksi fisik pada pintu dan perubahan status lingkungan ditransmisikan secara seketika (*real-time*) melalui protokol MQTT dengan rata-rata latensi sangat rendah, yaitu 145 ms (Tabel 2). Pengiriman data ini berujung pada penyimpanan log di server basis data

MySQL, yang mengukuhkan penerapan prinsip nirsangkal (*non-repudiation*) pada setiap aktivitas di ruang arsip. Sebagai pembuktian empiris dari fitur Jejak Audit (*Audit Trail*), rekam jejak aktivitas yang tersimpan di dalam database MySQL disajikan pada Tabel 5.

Tabel 5. Sampel Data Jejak Audit (*Audit Trail*) pada Server MySQL

ID	Waktu	ID USER	Metode	Status Akses	Status Ruangan
1	2026-07-06 12:40:17	32	WAKTU HABIS	GAGAL	AMAN
2	2026-07-06 12:39:54	32	3FA SUKSES	BERHASIL	AMAN
3	2026-07-06 12:39:26	28	KARTU SALAH	GAGAL	AMAN
4	2026-07-06 12:29:16	20	KARTU SALAH	GAGAL	AMAN
5	2026-07-06 12:39:07	32	3FA SUKSES	BERHASIL	AMAN
6	2026-07-06 11:58:01	28	3FA SUKSES	BERHASIL	AMAN
7	2026-07-06 11:36:02	28	KARTU SALAH	GAGAL	AMAN
8	2026-07-06 11:31:40	30	3FA SUKSES	BERHASIL	AMAN
9	2026-07-06 11:28:49	32	3FA SUKSES	BERHASIL	AMAN
10	2026-07-06 11:21:17	-	OVERRIDE	-	FIRE_DETECTED

Tabel 4 mendemonstrasikan bukti nyata bahwa sistem berhasil merekam variabel audit yang krusial secara permanen tanpa mengalami kehilangan paket data (*Packet Delivery Ratio* 100%). Baris log dengan ID 2,5,6,8,9 menunjukkan pencatatan akses normal oleh personel yang sah, sedangkan baris log ID 1,3,4,7 membuktikan akuntabilitas sistem dalam mendeteksi dan mencatat setiap upaya yang gagal dikarenakan jarak waktu yang terlalu lama atau identias yang digunakan tidak sesuai dengan basis data. Selanjutnya, baris log ID 10 mendokumentasikan jejak sistemik yang merekam waktu pasti kapan fungsi *fail-safe* mengambil alih pembukaan pintu akibat terdeteksinya bahaya kebakaran. Keberadaan riwayat digital pada MySQL yang bersifat permanen dan tidak dapat dimodifikasi secara sepihak (*immutable*) ini memberikan instrumen forensik yang sangat valid bagi institusi kearsipan untuk memenuhi standar audit keamanan berkala maupun investigasi insiden.

Keempat, efektivitas proteksi berlapis dari sisi perangkat lunak dan arsitektur jaringan tersebut ditopang sepenuhnya oleh pembagian desain fisik purwarupa ke dalam empat zona terisolasi (Gambar 3). Dengan menempatkan pusat komando (mikrokontroler ESP32), modul relay, serta sumber daya listrik utama di dalam zona kotak panel tertutup, dan mengalirkan jalur pengkabelan tersembunyi melalui zona plafon, arsitektur ini berhasil meminimalkan titik kerentanan fisik. Desain tata letak ini menekan probabilitas pihak eksternal untuk melakukan sabotase perangkat keras, pemotongan kabel sensor, ataupun pemutusan sumber daya listrik secara paksa dari area luar pintu

Kesimpulannya, integrasi harmonis antara ketatnya validasi fisik MFA, kecepatan respons *fail-safe* untuk keselamatan manusia, ketahanan mekanik 4 zona, serta akuntabilitas Jejak Audit digital anti-sangkal telah menjadikan arsitektur sistem keamanan ruang arsip berbasis IoT ini sebagai solusi proteksi aset vital negara yang handal, transparan, dan teruji secara kuantitatif.

V. KESIMPULAN

Desain arsitektur sistem keamanan ruang arsip pada penelitian ini berhasil memberikan solusi yang lebih baik daripada sistem kunci konvensional.Implementasi *Multi-Factor Authentication (MFA)* berdasarkan kombinasi/segemntasi pemindaian sidik jari, token RFID dan kode PIN mampu

membangun sistem *smart lock* dengan konsep *zero-trust*. Sistem ini menghilangkan risiko yang terkait dengan kartu yang hilang atau dicuri. Secara fisik, strategi memecah prototipe maket ke dalam keempat zona fungsional dapat melindungi elemen-elemen vital secara maksimal.

Selain untuk memperketat akses, arsitektur ini juga memastikan transparansi riwayat penggunaan ruangan. Penggunaan mikrokontroler ESP32 dan protokol MQTT memungkinkan untuk setiap interaksi di terhadap pintu dikirim secara langsung ke *server* MySQL. *Audit Trail* mengukuhkan prinsip nirsangkal sehingga tidak ada satu aktivitas keluar masuk yang tidak tercatat. Sementara itu, integrasi sensor lingkungan (asap, api, dan suhu) yang dikaitkan dengan mekanisme *fail-safe* memastikan bawa ruangan akan secara otomatis terbuka apabila terjadi keadaan darurat, sehingga keselamatan petugas akan selalu menjadi prioritas tertinggi yang melebihi kerahasiaan dokumen.

Adapun untuk pengembangan penelitian di masa yang akan datang, arsitektur konseptual ini sangat dianjurkan untuk diimplementasikan dalam bentuk *hardware* penuh. Pengujian lapangan secara empiris diperlukan untuk mengukur tingkat latensi dari pengiriman data berbasis MQTT pada berbagai macam kondisi jaringan internet dan juga digunakan untuk menguji ketahanan mekanik komponen solenoid yang dipakai selama penggunaan jangka panjang.

UCAPAN TERIMA KASIH

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] Republik Indonesia, Undang-Undang Republik Indonesia Nomor 43 Tahun 2009 tentang Kearsipan. Jakarta, 2009.

[2] E. Schiavone, A. Ceccarelli, dan A. Bondavalli, "Continuous biometric verification for non-repudiation of remote services", *Proc. 12th Int. Conf. on Availability, Reliability and Security*, 2017.

[3] Rismawati, S. Paembonan, dan R. Suppa, "Rancang bangun keamanan pintu otomatis menggunakan E-KTP berbasis Arduino Uno," *JITET (Jurnal Informatika dan Teknik Elektro Terapan), vol. 12, no. 3, pp. 2352-2364,* 2024.

[4] K. Gupta, M. A. Mohammed, N. Jiwani, N. Afreen, dan M. H. U. Sharif, "Smart door locking system using IoT," dalam *2022 International Conference on Advances in Computing, Communication and Materials (ICACCM)*, IEEE, 2022.

[5] M. A. Aziz, T. Sutikno, H. Yuliansyah, A. I. Dewi, Y. E. Rohmadi, dan 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.

[6] "Kejar ayam sampai masuk ruang arsip PT KAI, 2 pengemis curi 100 bal dokumen senilai Rp 30 juta," *Kompas.com*, 14 Jul.2023. https://regional.kompas.com/read/2023/07/14/110054478/kejar-ayam-sampai-masuk-ruang-arsip-pt-kai-2-pengemis-curi-100-bal-dokumen (diakses pada 7 Jun. 2026).

[7] "Ruangan biro humas ATR/BPN terbakar, Menteri Nusron: Api sudah berhasil dipadamkan dengan cepat," *Wartakita.org*, 10 Feb. 2025. https://www.wartakita.org/ruangan-biro-humas-atr-bpn-terbakar-menteri-nusron-api-sudah-berhasil-dipadamkan-dengan-cepat/ (diakses pada 7 Jun. 2026).

[8] H. Ilmi, K. Khairuman, dan R. B. Ginting, "Perancangan sistem absensi berbasis Internet of Things (IoT) dengan fitur keamanan sidik jari," *RIGGS: Journal of Artificial Intelligence and Digital Business*, vol. 5, no. 1, pp. 154-170, 2026.

[9] B. B. Mangata, D. I. N'kashama, P. B. Christian, dan D. K. Muamba, "Comparative studies between a facial recognition system and a fingerprint recognition system for access control," *IJISCS*, 2022.

[10] A. Ometov et al., "Multi-factor authentication: A survey," *Cryptography*, 2018.

[11] A. Kurnianto, J. D. Irawan, dan F. X. Ariwibisono, "Penerapan IoT untuk controlling lampu menggunakan protokol MQTT berbasis web," *JATI*, 2023

[12] D. Setiawan, B. Rahmat, dan W. S. Saputra, "IoT pengendalian keamanan pintu rumah otomatis menggunakan E-KTP berbasis mikrokontroler ESP32," *JITEK*, 2023.

[13] M. W. Aryadi, I. K. R. Arthana, dan 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.

[14] D. R. Kristiyanti, A. Wijayanto, dan A. Aziz, "Sistem monitoring suhu dan kelembaban pada budidaya jamur tiram berbasis IoT menggunakan MQTT dan Telegram BOT," *ATASI*, 2022.

[15] A. A. Zainuddin et al., "Innovative IoT smart lock system: Enhancing security with fingerprint and RFID technology," *Malays. J. Sci. Adv. Technol.*, 2024.

[16] D. Mardhani dan A. J. S. Runturambi, "Keamanan dan pertahanan dalam studi ketahanan nasional guna mewujudkan sistem keamanan nasional," *Jurnal Inovasi Penelitian*, 2020.

[17] Syahfitri, "Internet of Things (IoT), sejarah, teknologi, dan penerapannya," *Uranus*, 2025.

[18] D. Adidrana, H. Suryoprago, dan A. R. Hakim, "Perancangan sistem smart door lock menggunakan Internet of Things," *IJCT*, 2023.

[19] B. S. Surani, A. Dharmawan, dan C. A. Bakti, "Implementasi mikrokontroler ESP32 untuk kontrol berbasis pengenalan suara dan cahaya dalam sistem smart home," *J. Inf. Technol. Comput. Sci,* 2025.

[20] M. T. K. Ballagi, M. A. Yasin, dan Z. Razilu, "Implementasi sistem absensi biometrik mahasiswa menggunakan mikrokontroler ESP32," 2026.

[21] M. B. Ahmad dan F. A. Nababa, "The need of using a radio frequency identification (RFID) system," *Int. J. New Comput. Archit. Their Appl.*, 2021.

[22] J. Singh et al., "Digital keypad security system based on Arduino with GSM module, alarm, dan temperature sensor," *SSRN Electron. J.*, 2022.
[23] Y. K. Yonatan, A. T. Mukti, dan R. N. Firmansyah, "Analisa penerapan sensor suhu menggunakan Arduino Uno: Sensor DHT22", 2025.
[24] A. Kurniawan, A. Frisca, dan R. Y. Pratama, "Rancang bangun sistem deteksi asap menggunakan sensor MQ-2 untuk keamanan lingkungan,"2025.
[25] A. Fahriyansyah, K. Hidayat, M. I. R. Ismail, dan N. Nugraha, "Sistem deteksi api pada warehouse berbasis Internet of Things dengan platform Blynk IoT", 2025
[26] M. A. Juniawan dan A. H. Rismayana, "Prototipe smart door lock berbasis Internet of Things," Politeknik TEDC, 2024.
[27] S. P. Santosa dan R. M. W. Nugroho, "Rancang bangun alat pintu geser otomatis menggunakan motor DC 24 V," 2021.
[28] S. A. Panjaitan, P. Gunoto, dan M. Algusri, "Rancang bangun sistem kendali dan monitoring penggunaan pembatasan arus listrik berbasis IoT," SIGMA Tek., 2024.
[29] I. Joshua dan D. W. Chandra, "Analisis logging dan auditing akses database SQL melalui koneksi remote menggunakan Anydesk," 2023
[30] M. Zen, Irwan, Hafni, dan M. D. P. Ananda, "Implementasi dan pengujian menggunakan metode BlackBox testing pada sistem informasi tracer study," Bull. Comput. Sci. Res., 2024.
[31] J. S. Sonamoni et al., “IoT-based smart remote door lock and monitoring system using an Android application,” Eng. Proc., 2024.