

Kelayakan dan Keterbatasan Prototipe Kontrol Akses *PIN* Berbasis *Arduino* untuk Pengamanan Arsip Perencanaan

Feasibility and Limitations of an Arduino-Based PIN Access Control Prototype for Securing Planning Archives

Imam Mas Ulum^{1*}, Abdi Pandu Kusuma, Sabitul Kirom

¹ Fakultas Teknik dan Informatika, Universitas Islam Balitar, Blitar, Indonesia

Article Info

Article history:

Received Agustus 7, 2026

Revised Agustus 31, 2026

Accepted Agustus 31, 2026

Published Agustus 31, 2026

Kata Kunci:

Kontrol Akses Arsip;
Autentikasi PIN;
Prototipe Arduino;
Solenoid Door Lock;
Evaluasi Kelayakan

Keywords:

Archive Access Control;
PIN Authentication;
Arduino Prototype;
Solenoid Door Lock;
Feasibility Evaluation

License: [CC BY 4.0](https://creativecommons.org/licenses/by/4.0/)



Copyright: © 2026 The Author(s)

ABSTRAK

Pengamanan arsip perencanaan membutuhkan kontrol akses yang mampu membatasi penggunaan ruang penyimpanan secara konsisten. Observasi awal di Ruang Bina Program Dinas Pertanian Kabupaten Tulungagung menunjukkan bahwa akses arsip masih mengandalkan kunci mekanis tanpa verifikasi elektronik. Penelitian ini bertujuan mengembangkan dan mengevaluasi kelayakan prototipe kontrol akses PIN berbasis Arduino untuk pengamanan arsip perencanaan. Penelitian menggunakan metode *Research and Development* dengan model ADDIE. Sistem mengintegrasikan Arduino Uno, keypad 4×4, LCD 16×2, relay, solenoid door lock, dan buzzer. Implementasi terbatas pada model pintu untuk uji prototipe, bukan instalasi permanen di ruang arsip. Evaluasi dilakukan melalui empat skenario fungsional, validasi tiga ahli, dan uji tiga pengguna menggunakan skala Likert 1–5. Keempat skenario menghasilkan respons sesuai rancangan (4/4). Validasi ahli menghasilkan 70 dari 75 (93,33%), sedangkan pengujian pengguna menghasilkan 75 dari 75 (100%); berdasarkan kategori operasional penelitian, keduanya termasuk Sangat Layak. Hasil tersebut menunjukkan kelayakan pada konteks pengujian terbatas, bukan bukti efektivitas keamanan jangka panjang. Keterbatasan utama meliputi autentikasi satu faktor, belum tersedianya *access log*, belum adanya cadangan daya, pengulangan uji yang tidak terdokumentasi, serta ukuran uji pengguna yang kecil.

ABSTRACT

Planning archives require access control capable of consistently restricting access to storage areas. Initial observation in the Program Development Division of the Tulungagung Regency Agriculture Office showed that archive access still relied on mechanical keys without electronic verification. This study aimed to develop and evaluate the feasibility of an Arduino-based PIN access-control prototype for planning archive security. The study employed a *Research and Development* method using the ADDIE model. The system integrated an Arduino Uno, a 4×4 keypad, a 16×2 LCD, a relay, a solenoid door lock, and a buzzer. Implementation was limited to a model door for prototype testing, not a permanent archive-room installation. Evaluation included four functional scenarios, validation by three experts, and testing by three users using a 1–5 Likert scale. All four scenarios produced the expected responses (4/4). Expert validation produced 70 out of 75 (93.33%), while user testing produced 75 out of 75 (100%); under the study's operational criteria, both were categorized as *Very Feasible*. These results indicate

feasibility within a limited testing context rather than long-term security effectiveness. Key limitations include single-factor authentication, the absence of an access log, no backup power supply, undocumented repeated testing, and the small user-test sample.

Corresponding Author:

Imam Mas Ulum
Fakultas Teknik dan Informatika, Universitas Islam Balitar,
Blitar, Indonesia
Email: mammasulum.diperta@gmail.com

1. PENDAHULUAN

Arsip perencanaan merupakan bagian penting dari akuntabilitas instansi karena memuat informasi yang digunakan dalam penyusunan program, anggaran, evaluasi, dan pelaporan kinerja. Undang-Undang Nomor 43 Tahun 2009 menempatkan ketersediaan arsip yang autentik, utuh, dan terpercaya sebagai bagian penting penyelenggaraan kearsipan [1]. Pedoman pemeliharaan arsip dinamis juga menekankan perlunya menjaga keutuhan, keamanan, dan keselamatan arsip, baik fisik maupun informasinya [2]. Berdasarkan observasi dan wawancara pada Ruang Bina Program Dinas Pertanian Kabupaten Tulungagung, akses ke ruang penyimpanan arsip perencanaan masih menggunakan kunci mekanis sehingga belum tersedia verifikasi elektronik untuk membatasi akses pengguna.

Pemanfaatan mikrokontroler untuk kontrol akses telah banyak dikaji. Suwartika dan Sembada mengembangkan pengamanan pintu laboratorium menggunakan Arduino Uno, *keypad*, *relay*, dan *solenoid door lock* [3]. Hermawanto dkk. menerapkan RFID dan Arduino pada laboratorium komputer untuk mengurangi keterbatasan kunci manual [4]. Sholeh dkk. mengintegrasikan Arduino Uno dengan *QR-Code* pada pintu perpustakaan dan melaporkan keberhasilan pembacaan *QR-Code* pada pengujian sistem [5], sedangkan Hazarah menggunakan *QR-Code* dan *solenoid* sebagai alternatif pengunci pintu berbasis Arduino [6]. Rangkaian penelitian tersebut menunjukkan bahwa Arduino dapat digunakan sebagai pengendali akses elektronik dengan beragam media autentikasi.

Perkembangan berikutnya mengarah pada penguatan fungsi peringatan, identifikasi pengguna, dan pencatatan akses. Al Imran dkk. mengevaluasi sistem keamanan pintu berbasis Arduino dan Android dengan aspek *functionality*, *efficiency*, *usability*, dan *portability* [7]. Rismawati dkk. memanfaatkan E-KTP sebagai identitas pengguna pada sistem Arduino [8], sedangkan Fauzi dkk. mengintegrasikan RFID dengan basis data *web* untuk merekam penggunaan ruang [9]. Nathiq juga mengembangkan *smart door lock* RFID-Arduino yang disertai pencatatan data akses [10]. Temuan-temuan tersebut menunjukkan bahwa pengembangan kontrol akses tidak hanya ditentukan oleh keberhasilan membuka atau menutup kunci, tetapi juga oleh mekanisme identifikasi, kemudahan penggunaan, dan kemampuan sistem menyediakan jejak akses.

Literatur yang ditelaah dalam penelitian ini menunjukkan dua kecenderungan utama. Pertama, sejumlah penelitian menekankan keberhasilan aktuasi pintu menggunakan Arduino dengan variasi media autentikasi [3]–[8]. Kedua, penelitian yang lebih lanjut mulai menambahkan identifikasi pengguna dan pencatatan akses berbasis RFID atau basis data [9], [10]. Berdasarkan cakupan literatur yang ditelaah dalam penelitian ini, belum tampak evaluasi yang secara eksplisit menggabungkan pengujian fungsi prototipe, penilaian kelayakan terbatas oleh ahli dan pengguna, serta identifikasi kesenjangan implementasi terhadap kebutuhan arsip yang menuntut kontrol identitas dan jejak akses. Oleh karena itu, kontribusi penelitian ini tidak diletakkan pada kebaruan autentikasi PIN, melainkan pada evaluasi berlapis terhadap prototipe kontrol akses arsip: kesesuaian fungsi perangkat, kelayakan pada konteks uji terbatas, kendala teknis catu daya dan instalasi, serta keterbatasan desain berupa autentikasi satu faktor dan ketiadaan *access log*. Berdasarkan kesenjangan tersebut, penelitian ini

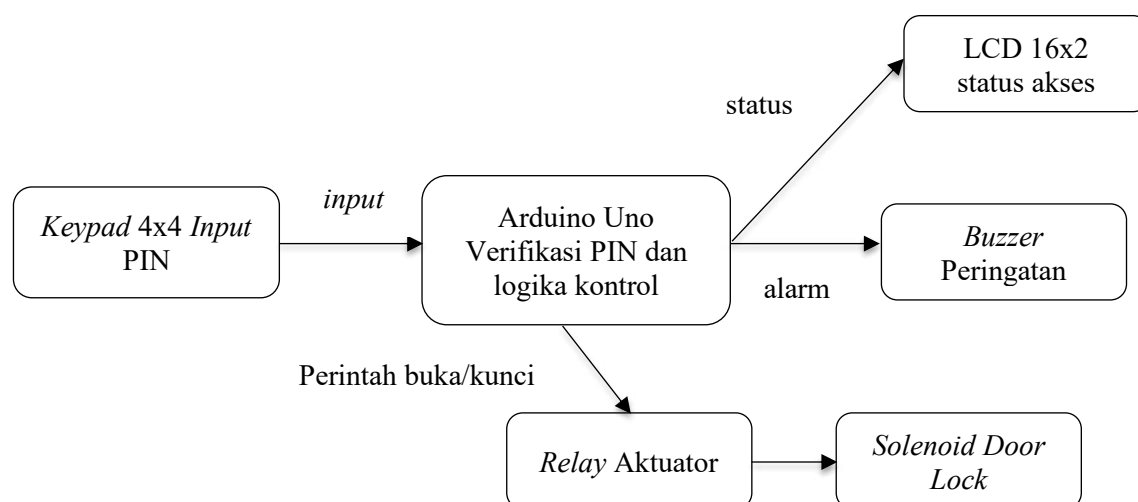
bertujuan mengembangkan dan mengevaluasi kelayakan prototipe kontrol akses PIN berbasis Arduino untuk pengamanan arsip perencanaan..

2. METODE

Penelitian menggunakan metode *Research and Development* (R&D) dengan model ADDIE yang meliputi *Analysis*, *Design*, *Development*, *Implementation*, dan *Evaluation* [16]. Model ADDIE dipilih sebagai kerangka pengembangan bertahap untuk menghubungkan identifikasi kebutuhan, perancangan perangkat, pengembangan prototipe, uji penggunaan terbatas, dan evaluasi. Dalam penelitian ini, ADDIE digunakan sebagai kerangka proses R&D dan tidak diposisikan sebagai standar verifikasi rekayasa perangkat keras. Tahap *Analysis* dilakukan melalui observasi kondisi ruang arsip dan wawancara dengan petugas untuk mengidentifikasi kelemahan akses mekanis dan kebutuhan pengguna. Dokumentasi yang tersedia tidak memuat jumlah informan maupun waktu observasi dan wawancara secara rinci, sehingga keterlacakan tahap analisis kebutuhan menjadi salah satu keterbatasan metodologis. Tahap *Design* menghasilkan rancangan perangkat keras dan logika autentikasi. Tahap *Development* mencakup perakitan, pemrograman, dan pengujian awal. Pada dokumentasi penelitian, tahap *Implementation* dilakukan melalui uji prototipe pada model pintu yang merepresentasikan mekanisme akses ruang arsip; tahap ini tidak diperlakukan sebagai bukti instalasi operasional permanen pada pintu ruang arsip. Tahap *Evaluation* digunakan untuk menilai fungsi, kelayakan teknis, kemudahan penggunaan, dan kendala yang muncul selama uji prototipe.

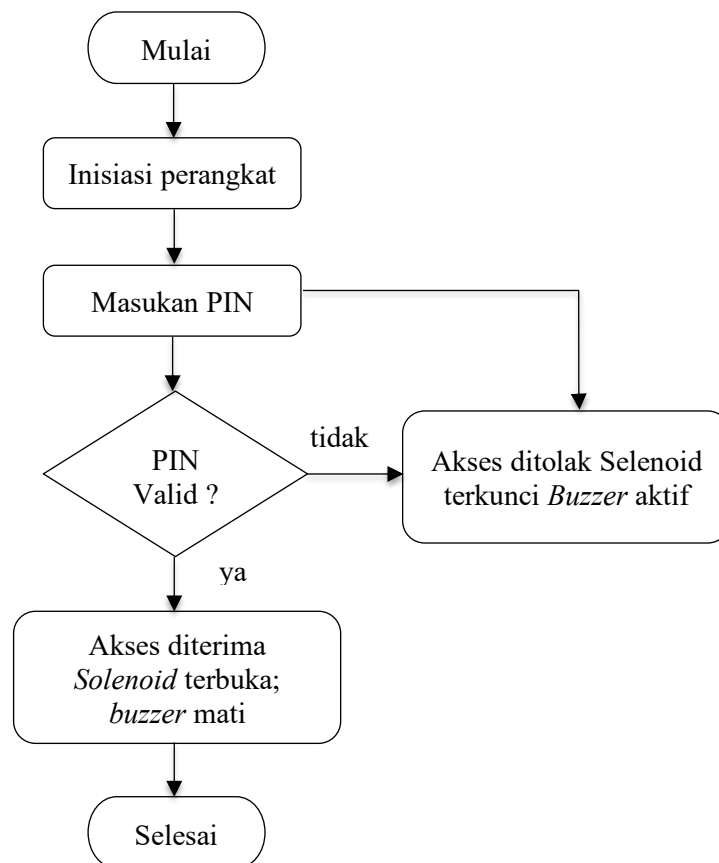
2.1 Perancangan Sistem

Sistem terdiri atas Arduino Uno sebagai pengendali utama, *keypad* 4×4 sebagai *input* PIN, LCD 16×2 sebagai antarmuka informasi, *relay* sebagai pengendali aktuatur, *solenoid door lock* sebagai mekanisme pengunci, dan *buzzer* sebagai indikator peringatan. PIN yang dimasukkan melalui *keypad* dibandingkan dengan PIN yang tersimpan pada program Arduino. Dokumentasi penelitian tidak memuat mekanisme perubahan PIN melalui antarmuka pengguna atau penyimpanan kredensial terpisah. Karena itu, penyimpanan PIN pada program diperlakukan sebagai keterbatasan desain, terutama dari sisi kemudahan pengelolaan kredensial dan perubahan PIN. Jika PIN valid, Arduino mengaktifkan *relay* untuk membuka *solenoid*, LCD menampilkan status akses diterima, dan *buzzer* tidak berbunyi. Jika PIN tidak valid, *relay* tidak diaktifkan, *solenoid* tetap terkunci, LCD menampilkan penolakan akses, dan *buzzer* berbunyi. Arsitektur hubungan antarkomponen ditunjukkan pada Gambar 1.



Gambar 1. Arsitektur prototipe kontrol akses arsip berbasis Arduino

Alur pada Gambar 2 dimulai dari inisialisasi perangkat dan *input* PIN. Sistem kemudian memverifikasi PIN terhadap nilai yang tersimpan. PIN valid mengaktifkan *relay* dan membuka *solenoid*, sedangkan PIN tidak valid mempertahankan *solenoid* dalam keadaan terkunci serta mengaktifkan peringatan; setelah penolakan, pengguna dapat mengulangi *input* PIN. Alur ini digunakan sebagai dasar penyusunan skenario pengujian fungsi utama sistem.



Gambar 2. Alur autentikasi PIN pada prototipe

2.2 Prosedur Pengujian dan Analisis Kelayakan

Pengujian fungsional disusun dalam empat skenario terdokumentasi, yaitu: (1) pengunggahan program dan komunikasi Arduino dengan komponen, (2) pembacaan *keypad* serta tampilan status pada LCD, (3) respons terhadap PIN valid, dan (4) respons terhadap PIN tidak valid. Kesesuaian dinilai dengan membandingkan respons teramati terhadap respons yang dirancang. Dokumen pengujian tidak memuat jumlah pengulangan setiap skenario, sehingga hasil fungsional dilaporkan sebagai cakupan skenario yang sesuai (4/4), bukan sebagai *success rate* atau ukuran reliabilitas berulang. Pengujian kondisi batas seperti PIN salah berturut-turut, *input* kosong atau kurang digit, *restart* perangkat, serta kondisi listrik mati dan hidup kembali juga tidak terdokumentasi, sehingga ketahanan sistem terhadap kondisi tersebut belum dapat dinilai. Setelah fungsi dasar dinyatakan berjalan, kelayakan sistem dinilai secara terbatas oleh tiga validator dengan kompetensi di bidang teknologi informasi/sistem komputer dan oleh tiga petugas yang berinteraksi dengan ruang arsip. Instrumen validator terdiri atas lima pernyataan yang mencakup desain perangkat keras, pembacaan PIN melalui *keypad*, proses autentikasi oleh Arduino, kinerja *solenoid door lock*, serta aspek keamanan dan kelayakan penggunaan. Instrumen pengguna juga terdiri atas lima pernyataan yang menilai kemudahan penggunaan, kemudahan *input* PIN, kejelasan informasi LCD, persepsi peningkatan keamanan dibandingkan kunci konvensional, dan kelayakan sistem secara keseluruhan. Seluruh butir menggunakan skala Likert 1–5. Rincian masa

pengalaman validator serta hasil uji validitas dan reliabilitas instrumen secara terpisah tidak tersedia pada dokumentasi penelitian; karena itu, hasil validasi diposisikan sebagai evaluasi prototipe terbatas. Persentase kelayakan dihitung menggunakan $P = (\text{jumlah skor diperoleh} / \text{jumlah skor maksimum}) \times 100\%$. Untuk interpretasi deskriptif, penelitian menggunakan interval sama 20 poin: 81–100% = Sangat Layak, 61–80% = Layak, 41–60% = Cukup Layak, 21–40% = Kurang Layak, dan 0–20% = Tidak Layak. Kategori ini merupakan kriteria operasional penelitian dan tidak dimaksudkan sebagai generalisasi terhadap populasi pengguna yang lebih luas.

3. HASIL DAN PEMBAHASAN

3.1 Hasil Pengembangan dan Pengujian Fungsional

Prototipe mengintegrasikan Arduino Uno, *keypad*, LCD, *relay*, *solenoid door lock*, dan *buzzer* dalam satu rangkaian kontrol akses. Pengujian dilakukan setelah program diunggah ke Arduino dan koneksi perangkat diperiksa. Empat skenario fungsional yang terdokumentasi seluruhnya menghasilkan respons sesuai rancangan (4/4). Angka 4/4 menunjukkan keterpenuhan skenario yang diuji, bukan reliabilitas sistem dalam pengujian berulang. Ringkasan respons teramati disajikan pada Tabel 1.

Tabel 1. Ringkasan pengujian fungsional sistem

No	Objek/Skenario	Respons Teramati	Status
1	Arduino Uno	Program dapat diunggah dan komunikasi dengan komponen berjalan	Sesuai
2	<i>Keypad</i> dan LCD	<i>Input</i> tombol terbaca dan status akses ditampilkan	Sesuai
3	PIN valid	<i>Relay</i> aktif, <i>solenoid</i> terbuka, LCD menampilkan akses diterima, <i>buzzer</i> tidak berbunyi	Sesuai
4	PIN tidak valid	<i>Relay</i> tidak aktif, <i>solenoid</i> tetap terkunci, LCD menampilkan akses ditolak, <i>buzzer</i> berbunyi	Sesuai

Pada uji prototipe ditemukan dua kendala teknis. *Solenoid* tidak dapat menarik mekanisme pengunci secara optimal ketika catu daya awal belum memenuhi kebutuhan arus. Setelah sumber daya diganti dengan adaptor 12 V 2 A, *solenoid* dapat membuka dan mengunci sesuai perintah Arduino. Kendala lain terjadi pada tampilan LCD akibat koneksi yang kurang stabil; setelah jalur kabel dan konfigurasi diperiksa, LCD kembali menampilkan informasi dengan benar. Temuan ini menunjukkan bahwa keberhasilan logika program perlu dibaca bersama dengan kecukupan catu daya dan kualitas instalasi perangkat keras. Dokumentasi penelitian tidak memuat spesifikasi arus nominal *solenoid*, detail proteksi rangkaian, maupun konfigurasi pemisahan beban *relay* dari Arduino secara rinci. Karena itu, hasil pengujian ini menunjukkan fungsi operasional pada prototipe, tetapi belum dapat digunakan untuk menyimpulkan kecukupan desain kelistrikan atau keselamatan elektris secara menyeluruh. Pengulangan pengujian juga tidak terdokumentasi, sehingga tingkat keandalan jangka panjang belum dapat ditentukan.



Gambar 3. Prototipe sistem pada model pintu pengujian

3.2 Hasil Validasi Ahli dan Pengujian Pengguna

Validasi ahli menilai desain perangkat keras, pembacaan PIN melalui *keypad*, proses autentikasi oleh Arduino, kinerja *solenoid door lock*, serta aspek keamanan dan kelayakan penggunaan. Validasi ini bersifat terbatas karena hanya melibatkan tiga validator dan tidak dimaksudkan sebagai generalisasi terhadap komunitas ahli yang lebih luas. Skor tiga validator disajikan pada Tabel 2.

Tabel 2. Hasil validasi ahli

No	Penilai	Skor	Persentase	Kategori
1	Validator 1	23/25	92,00%	Sangat Layak
2	Validator 2	23/25	92,00%	Sangat Layak
3	Validator 3	24/25	96,00%	Sangat Layak
	Rata-rata	70/75	93,33%	Sangat Layak

Total skor validasi ahli adalah 70 dari skor maksimum 75 atau 93,33%, sehingga berdasarkan kriteria operasional penelitian prototipe berada pada kategori Sangat Layak. Nilai tersebut menunjukkan kesesuaian rancangan terhadap indikator yang dinilai oleh tiga validator pada konteks uji terbatas, bukan kelayakan umum untuk seluruh kondisi penggunaan. Dokumentasi yang tersedia hanya memuat skor total masing-masing validator dan belum menyajikan skor per butir atau komentar rinci setiap validator. Karena itu, aspek yang memperoleh penilaian paling rendah dan masukan perbaikan spesifik belum dapat diidentifikasi dari data yang tersedia. Hasil ini juga tidak secara langsung membuktikan ketahanan keamanan atau keandalan jangka panjang karena pengujian masih berfokus pada fungsi prototipe dan penilaian kelayakan awal.

Pengujian pengguna dilakukan kepada tiga petugas yang berinteraksi dengan ruang arsip. Instrumen menilai kemudahan penggunaan sistem, kemudahan *input* PIN, kejelasan informasi LCD,

persepsi peningkatan keamanan dibandingkan kunci konvensional, dan kelayakan sistem secara keseluruhan. Seluruh pengguna memberikan skor 25 dari 25 sebagaimana dirangkum pada Tabel 3. Karena ukuran pengguna sangat kecil, hasil ini diposisikan sebagai uji penerimaan prototipe secara terbatas.

Tabel 3. Hasil pengujian pengguna

No	Pengguna	Skor	Persentase	Kategori
1	Pengguna 1	25/25	100,00%	Sangat Layak
2	Pengguna 2	25/25	100,00%	Sangat Layak
3	Pengguna 3	25/25	100,00%	Sangat Layak
	Rata-rata	75/75	100,00%	Sangat Layak

Skor pengguna mencapai 75/75 atau 100%, yang menunjukkan penerimaan sangat tinggi pada tiga pengguna dan lima butir instrumen yang digunakan. Karena masing-masing pengguna memperoleh 25/25 pada instrumen lima butir dengan skor maksimum 5 per butir, seluruh butir secara aritmetis memperoleh nilai maksimum dari setiap pengguna. Kondisi ini memperlihatkan *ceiling effect* yang kuat dan tidak menghasilkan variasi penilaian antar pengguna maupun antar butir. Oleh karena itu, nilai 100% tidak dapat ditafsirkan sebagai bukti bahwa risiko akses tidak sah berkurang 100% atau sebagai ukuran *usability* yang dapat digeneralisasi. Pengujian lanjutan memerlukan jumlah pengguna yang lebih besar, variasi karakteristik pengguna, serta instrumen yang mampu membedakan pengalaman penggunaan secara lebih sensitif.

3.3 Pembahasan

Keberhasilan empat skenario autentikasi pada penelitian ini konsisten dengan Suwartika dan Sembada yang mengintegrasikan *keypad*, *Arduino Uno*, *relay*, dan *solenoid* untuk pengamanan pintu laboratorium [3], serta dengan Hermawanto dkk. yang menunjukkan bahwa mikrokontroler dapat mengendalikan pengunci elektronik berdasarkan identitas yang diverifikasi [4]. Secara konseptual, kontrol akses tidak hanya mencakup keputusan membuka atau menutup pintu, tetapi juga fungsi *Access Control*, *Identification and Authentication*, serta *Audit and Accountability* sebagaimana dikelompokkan dalam NIST SP 800-53 [17]. Rujukan NIST pada penelitian ini digunakan sebagai kerangka konseptual untuk membaca kesenjangan fungsi keamanan, bukan sebagai klaim bahwa prototipe telah memenuhi atau tersertifikasi sesuai NIST SP 800-53. Dalam prototipe ini, PIN berfungsi sebagai mekanisme autentikasi untuk keputusan akses biner. Apabila satu PIN digunakan bersama, mekanisme tersebut lebih tepat dipahami sebagai verifikasi kredensial kelompok daripada identifikasi pengguna individual, karena sistem belum dapat mengaitkan setiap kejadian akses dengan identitas orang tertentu. Prototipe juga belum menyediakan *audit trail*. Dengan demikian, keberhasilan fungsi aktuasi membuktikan kesesuaian logika kontrol dasar, bukan kelengkapan kontrol keamanan.

Keterbatasan autentikasi PIN tunggal muncul karena kredensial dapat diketahui atau dibagikan kepada orang lain, sehingga sistem sulit memastikan bahwa orang yang memasukkan PIN adalah pengguna yang secara individual dapat dipertanggungjawabkan. Jodi dkk. menggabungkan *Tag Card* dan PIN sebagai dua mekanisme akses [11], Rismawati dkk. memanfaatkan identitas E-KTP [8], sedangkan Daulay dan Alamsyah menggabungkan RFID, *fingerprint*, dan basis data [13]. Perbandingan tersebut menunjukkan bahwa autentikasi multi-faktor atau identitas unik lebih sesuai apabila tujuan pengamanan memerlukan keterikatan akses dengan individu tertentu.

Keterbatasan berikutnya adalah belum tersedianya riwayat akses. Sistem berbasis RFID dan *web* yang dikembangkan Syukuryansyah dkk. memungkinkan pemantauan aktivitas melalui *website* [12], sistem Utami dkk. menyimpan data akses ke basis data [14], sedangkan Fauzi dkk. dan Nathiq menunjukkan fungsi pencatatan penggunaan ruang pada sistem berbasis RFID [9], [10]. Dalam

perspektif *accountability*, *access log* diperlukan agar kejadian akses dapat ditelusuri kembali ketika terjadi insiden atau kebutuhan audit. Oleh karena itu, ketiadaan log bukan sekadar kekurangan fitur, tetapi membatasi kemampuan prototipe untuk mendukung akuntabilitas akses arsip.

Hasil evaluasi teknis juga memperlihatkan bahwa keandalan aktuator dipengaruhi oleh kecukupan catu daya dan kualitas instalasi rangkaian. Sistem Arduino dengan kombinasi metode akses dan alarm telah dilaporkan berfungsi baik pada pengujian prototipe [7], [15], tetapi temuan penelitian ini menegaskan bahwa keberhasilan logika program tidak otomatis menjamin kontinuitas operasi. Ketergantungan pada satu sumber listrik tanpa catu daya cadangan merupakan risiko operasional karena kehilangan daya dapat mengganggu fungsi aktuator dan mekanisme akses. Dokumentasi penelitian juga belum menjelaskan perilaku pengunci ketika listrik padam, apakah sistem mempertahankan kondisi terkunci (*fail-secure*) atau membuka untuk kebutuhan keselamatan (*fail-safe*). Aspek ini perlu ditetapkan berdasarkan kebutuhan keamanan arsip dan prosedur keselamatan ruang sebelum implementasi operasional. Pengembangan berikutnya perlu mengintegrasikan *backup power*, *access log*, autentikasi yang lebih kuat, serta pengujian kondisi kehilangan daya, kemudian diuji melalui pengulangan terkontrol dan periode operasional yang lebih panjang.

4. KESIMPULAN

Prototipe kontrol akses PIN berbasis Arduino berhasil menjalankan empat skenario fungsi yang terdokumentasi (4/4): komunikasi perangkat, pembacaan *keypad* dan LCD, respons terhadap PIN valid, serta respons terhadap PIN tidak valid. Validasi terbatas oleh tiga ahli menghasilkan 70/75 (93,33%) dan uji terbatas oleh tiga pengguna menghasilkan 75/75 (100%), sehingga berdasarkan kriteria operasional penelitian prototipe berada pada kategori Sangat Layak pada konteks pengujian terbatas. Temuan tersebut belum membuktikan efektivitas keamanan atau keandalan jangka panjang karena jumlah validator dan pengguna kecil, pengulangan uji fungsional tidak terdokumentasi, dan seluruh pengguna memberi skor maksimum. Secara teknis, prototipe masih menggunakan autentikasi satu faktor, menyimpan PIN pada program, belum menyediakan *access log*, dan bergantung pada sumber listrik tanpa catu daya cadangan; perilaku pengunci ketika listrik padam juga belum terdokumentasi. Dengan demikian, hasil penelitian ini hanya berlaku pada prototipe, tiga validator, dan tiga pengguna dalam konteks pengujian yang dilakukan, serta belum cukup untuk menyatakan kesiapan implementasi operasional permanen. Pengembangan berikutnya perlu menambahkan autentikasi multi-faktor atau identitas unik, pencatatan akses, pengelolaan kredensial yang lebih aman, *backup power*, pengujian kondisi kehilangan daya, pengujian berulang, dan evaluasi operasional dengan jumlah pengguna yang lebih representatif.

PERNYATAAN PENGGUNAAN AI

Para penulis menyatakan bahwa dalam penelitian ini tidak menggunakan AI

KONTRIBUSI PENULIS

Konseptualisasi: Febri Yalda Sulistia, Karina Nurfebria, Nurbeti Sinulingga, Nuzul Aini Ramadhani

Metodologi: Karina Nurfebria

Pengembangan perangkat lunak/sistem: -

Pengumpulan data: Nurbeti Sinulingga

Analisis data: Nurbeti Sinulingga, Nuzul Aini Ramadhani

Validasi: Nuzul Aini Ramadhani

Visualisasi: Nuzul Aini Ramadhani, Nurbeti Sinulingga

Penelusuran literatur: Karina Nurfebria

Penulisan draf awal: Febri Yalda Sulistia

Penelaahan dan penyuntingan: Khairul
Supervisi: -
Administrasi penelitian: Karina Nurfebria

PERNYATAAN PENDANAAN

Penelitian ini dilakukan secara mandiri oleh penulis dan tidak mendapatkan dukungan pendanaan dari institusi kampus, pihak eksternal, maupun program hibah penelitian mana pun.

KONFLIK KEPENTINGAN

Para penulis menyatakan tidak terdapat konflik kepentingan dalam penelitian dan publikasi artikel ini.

DAFTAR PUSTAKA

- [1] Republik Indonesia, *Undang-Undang Republik Indonesia Nomor 43 Tahun 2009 tentang Kearsipan*, Lembaran Negara Republik Indonesia Tahun 2009 Nomor 152, Tambahan Lembaran Negara Republik Indonesia Nomor 5071, Oct. 23, 2009.
- [2] Arsip Nasional Republik Indonesia, *Peraturan Arsip Nasional Republik Indonesia Nomor 9 Tahun 2018 tentang Pedoman Pemeliharaan Arsip Dinamis*, Berita Negara Republik Indonesia Tahun 2018 Nomor 818, Jun. 28, 2018.
- [3] R. Suwartika and G. Sembada, "Perancangan Sistem Keamanan Menggunakan Solenoid Door Lock Berbasis Arduino Uno pada Pintu Laboratorium di PT. XYZ," *Jurnal E-Komtek*, vol. 4, no. 1, pp. 62–74, 2020, doi: 10.37339/e-komtek.v4i1.217.
- [4] F. Hermawanto, H. J. Habibi, and N. C. Hasyim, "Rancang Bangun Sistem Pengunci Pintu Berbasis RFID dan Arduino pada Laboratorium Komputer Jurusan Teknik Informatika," *Jurnal Pengelolaan Laboratorium Pendidikan*, vol. 4, no. 1, pp. 26–35, 2022, doi: 10.14710/jplp.4.1.26-35.
- [5] M. B. Sholeh, A. Herlina, and F. Hasan, "Design of Automatic Door Lock Control System Library Nurul Jadid University Based On Arduino Uno R3 and QR-Code," *Buletin Ilmiah Sarjana Teknik Elektro*, vol. 2, no. 2, pp. 91–102, 2020, doi: 10.12928/biste.v2i2.2741.
- [6] A. Hazarah, "Rancang Bangun Smart Door Lock Menggunakan QR-Code dan Solenoid," *Jurnal Teknologi Informasi dan Terapan*, vol. 4, no. 1, pp. 5–10, 2017, doi: 10.25047/jtit.v4i1.14.
- [7] A. Imran, Fathahillah, V. A. Tandirerung, and Y. R. Mahendra, "Pengembangan Sistem Keamanan Pintu Rumah Dengan Peringatan Alarm Menggunakan Arduino Berbasis Android," *Jurnal MediaTIK*, vol. 5, no. 2, pp. 56–65, 2024, doi: 10.59562/mediatik.v5i2.2980.
- [8] Rismawati, S. Paembonan, and R. Suppa, "Rancang Bangun Keamanan Pintu Otomatis Menggunakan E-KTP Berbasis Arduino Uno," *Jurnal Informatika dan Teknik Elektro Terapan*, vol. 12, no. 3, pp. 2352–2364, 2024, doi: 10.23960/jitet.v12i3.4745.
- [9] M. I. Fauzi, Minarto, and M. I. Sulistyo S., "Rancang Bangun Sistem Monitoring Proses Belajar Mengajar (PBM) dengan RFID Menggunakan Arduino Nano Berbasis Web," *Jurnal Informatika dan Teknik Elektro Terapan*, vol. 11, no. 3, pp. 746–756, 2023, doi: 10.23960/jitet.v11i3.3323.
- [10] T. A. Nathiq, "Rancang Bangun Smart Doorlock Kamar Mesin dan Anjungan Berbasis RFID dan Arduino," *Venus: Jurnal Publikasi Rumpun Ilmu Teknik*, vol. 2, no. 4, pp. 14–40, 2024, doi: 10.61132/venus.v2i4.376.
- [11] S. Jodi, M. Siregar, Asmira, and N. Kusumawati, "Prototype Sistem Keamanan Pintu Rumah Menggunakan Tag Card dan PIN Berbasis Arduino Uno," *Jurnal Sistem Informasi dan Sistem Komputer*, vol. 7, no. 2, pp. 82–91, 2022, doi: 10.51717/simkom.v7i2.83.
- [12] R. Syukuryansyah, D. Setiyadi, and S. Rofiah, "Penerapan Radio Frequency Identification dalam Membangun Sistem Keamanan dan Monitoring Smart Lock Door Berbasis

- Website,” *Infotech: Journal of Technology Information*, vol. 6, no. 2, pp. 83–90, 2020, doi: 10.37365/jti.v6i2.91.
- [13] N. K. Daulay and M. N. Alamsyah, “Monitoring Sistem Keamanan Pintu Menggunakan RFID dan Fingerprint Berbasis Web dan Database,” *JUSIKOM: Jurnal Sistem Komputer Musirawas*, vol. 4, no. 2, pp. 85–92, 2019, doi: 10.32767/jusikom.v4i2.632.
- [14] D. K. Utami, A. S. M. Huda, A. Qur’ania, and R. Pratama, “Sistem Access Control Ruangan Laboratorium dan Perkuliahan Menggunakan Radio Frequency Identification,” *Jurnal Teknoinfo*, vol. 16, no. 2, pp. 258–266, 2022, doi: 10.33365/jti.v16i2.1897.
- [15] F. F. R. Rohim, “Penerapan Sistem Keamanan Pintu Rumah Menggunakan Tag Card dan PIN Berbasis Arduino Uno di Saif Fotocopy,” *JTINFO: Jurnal Teknik Informatika*, vol. 4, no. 2, pp. 294–298, 2025, doi: 10.02220/jtinfo.v4i2.1506.
- [16] R. M. Branch, *Instructional Design: The ADDIE Approach*. New York, NY, USA: Springer, 2009, doi: 10.1007/978-0-387-09506-6.
- [17] Joint Task Force, *Security and Privacy Controls for Information Systems and Organizations*, NIST Special Publication 800-53 Rev. 5. Gaithersburg, MD, USA: National Institute of Standards and Technology, 2020, doi: 10.6028/NIST.SP.800-53r5.