BULLETIN OF COMPUTER SCIENCE RESEARCH
ISSN 2774-3659 (Media Online)
Vol 6, No 4, June 2026 | Hal 1544-1551
https://hostjournals.com/bulletincsr
DOI: 10.47065/bulletincsr.v6i4.1178

Perancangan Keamanan Informasi pada Sistem Persuratan Berbasis Web Menggunakan Autentikasi dan Middleware

Panggah Widianda*, Muhammad Hafidz Amali, Adhitya Admaja, Maulana Raka Saputra

Fakultas Sains Teknologi dan Kesehatan, Program Studi Informatika, Universitas Islam Mulia Yogyakarta, Yogyakarta, Indonesia
Email: [1,*]panggah.widiandana@uim-yogya.ac.id, [2]2123032@uim-yogya.ac.id, [3]2123014@uim-yogya.ac.id, [4]2123026@uim-yogya.ac.id
Email Penulis Korespondensi: panggah.widiandana@uim-yogya.ac.id

Abstrak−Pengelolaan persuratan digital melalui sistem berbasis web telah meningkatkan efisiensi administrasi, namun di sisi lain memunculkan kerentanan baru terhadap ancaman siber. Keamanan informasi merupakan aspek penting dalam pengembangan sistem persuratan berbasis web karena sistem ini mengelola data surat masuk, surat keluar, serta dokumen resmi yang bersifat sensitif. Tanpa mekanisme pengamanan yang baik, sistem berpotensi mengalami akses tidak sah, manipulasi data, serta kebocoran informasi. Oleh karena itu, penelitian ini bertujuan untuk merancang mekanisme keamanan informasi melalui penerapan autentikasi (*auth*) dan *middleware* sebagai pengendali akses sistem secara berlapis. Metode penelitian yang digunakan adalah metode perancangan sistem (*system design*) yang mencakup analisis kebutuhan keamanan, pemodelan matriks kendali akses (*Access Control Matrix*), perancangan arsitektur pencegat rute, dan pengujian otorisasi *Black-box*. Dalam penerapannya, autentikasi digunakan untuk memastikan identitas pengguna sebelum mengakses sistem, sedangkan *middleware* berfungsi sebagai lapisan pengaman untuk membatasi akses berdasarkan peran pengguna. Hasil perancangan menunjukkan bahwa penerapan *auth* dan *middleware* mampu meningkatkan kontrol akses, menjaga kerahasiaan data, serta memperkuat keamanan informasi dalam sistem persuratan berbasis web. Kontribusi utama penelitian ini adalah penyediaan model keamanan informasi berlapis berbasis *Role-Based Access Control* (RBAC) terintegrasi yang dapat diadopsi oleh berbagai institusi untuk mencegah eskalasi hak akses (*privilege escalation*) dan manipulasi data pada sistem administrasi internal.

Kata Kunci: Keamanan Informasi; Sistem Persuratan; Autentikasi; Middleware; Web Application

Abstract−The management of digital correspondence through web-based systems has improved administrative efficiency, but on the other hand, it introduces new vulnerabilities to cyber threats. Information security is a crucial aspect in the development of web-based mailing systems because this system manages incoming mail, outgoing mail, and official documents that are highly sensitive. Without a good security mechanism, the system has the potential to experience unauthorized access, data manipulation, and information leaks. Therefore, this study aims to design an information security mechanism through the application of authentication (auth) and middleware as system access controllers. The research method used is a system design method that includes security requirement analysis, Access Control Matrix modeling, routing interceptor architecture design, and Black-box authorization testing. In its application, authentication is used to ensure user identity before accessing the system, while middleware serves as a security layer to restrict access based on user roles. The design results show that the application of auth and middleware can improve access control, maintain data confidentiality, and strengthen information security in web-based mailing systems. The main contribution of this research is the provision of an integrated Role-Based Access Control (RBAC) layered information security model that can be adopted by various institutions to prevent privilege escalation and data manipulation in internal administration systems.

Keywords: Information Security; Mailing System; Authentication; Middleware; Web Application

1. PENDAHULUAN

Perkembangan teknologi informasi mendorong berbagai macam organisasi dan institusi pendidikan untuk mengadopsi sistem berbasis web dalam pengelolaan administrasi harian, termasuk salah satunya adalah pengelolaan persuratan. Sistem persuratan berbasis web memungkinkan seluruh proses pengajuan, verifikasi, disposisi, dan pengarsipan surat dilakukan secara digital sehingga proses birokrasi menjadi jauh lebih efisien, transparan, dan terstruktur. Namun, digitalisasi masif pada sektor administrasi ini juga membawa serta peningkatan risiko terhadap keamanan informasi secara siber. Beberapa ancaman yang sering ditemui pada pengelolaan peladen web meliputi akses tidak sah oleh peretas (unauthorized access), pencurian data, serangan injeksi kode, serta manipulasi data persuratan resmi oleh pihak internal maupun eksternal yang tidak berwenang. Keamanan informasi pada dasarnya diciptakan dengan tujuan krusial untuk menjaga tiga pilar utama keamanan siber, yaitu kerahasiaan (confidentiality), keutuhan (integrity), dan ketersediaan (availability) data. Pada aplikasi pengelolaan persuratan, informasi yang lalu lalang dikelola bersifat sangat penting, legal, dan rahasia, sehingga membutuhkan mekanisme pengamanan aplikasi web yang solid, berlapis, dan sulit ditembus.

Beberapa tahun terakhir, beragam pendekatan teknologi telah diteliti secara masif untuk meningkatkan fungsionalitas dan keamanan sistem berbasis web di berbagai sektor. Keamanan akses dan verifikasi pengguna telah berhasil diterapkan pada sistem inventori logistik menggunakan mekanisme One Time Password (OTP) yang terbukti secara signifikan mampu meminimalisir intrusi akses ilegal [1]. Selain keamanan berbasis kata sandi dinamis yang kedaluwarsa secara berkala, pemanfaatan instrumen pelacakan optik berupa Quick Response (QR) Code telah diimplementasikan pada sistem informasi administrasi persuratan sekolah guna mempercepat validasi dokumen fisik ke format digital [2]. Di ruang lingkup pengelolaan level korporasi, standarisasi dan perencanaan strategis arsitektur terkait manajemen keamanan informasi telah mengadopsi kerangka kerja internasional seperti ISO/IEC 27001 secara masif guna memastikan perlindungan seluruh aset informasi [3]. Upaya digitalisasi layanan konsumen komersial juga menunjukkan tren positif, di mana implementasi QR Code pada sistem pemesanan makanan berbasis antarmuka web mobile sukses meningkatkan efisiensi proses pemesanan pelanggan [4].

BULLETIN OF COMPUTER SCIENCE RESEARCH
ISSN 2774-3659 (Media Online)
Vol 6, No 4, June 2026 | Hal 1544-1551
https://hostjournals.com/bulletincsr
DOI: 10.47065/bulletincsr.v6i4.1178

Sisi rekayasa perangkat lunak, perancangan fondasi web menggunakan bahasa pemrograman absolut seperti Hypertext Preprocessor (PHP) murni yang diintegrasikan dengan sistem manajemen basis data MySQL masih menjadi standar andalan dalam mengembangkan manajemen barang dagang [5]. Demi menunjang skalabilitas dan tingkat keamanan kueri yang lebih terorganisasi, framework CodeIgniter banyak diaplikasikan dalam membangun infrastruktur ujian online, terutama mengingat kemampuannya yang sangat baik dalam memisahkan logika dari visual melalui arsitektur Model-View-Controller (MVC) [6]. Selain optimalisasi kode, pendekatan dari sudut pandang interaksi manusia juga dipertimbangkan; contoh penerapannya dapat dilihat dari penggunaan metodologi Design Thinking pada rekayasa sistem informasi metrologi guna memastikan aplikasi memberikan resolusi akurat atas kendala pengguna akhir [7]. Sementara itu, bagi proyek berskala terikat, kerangka pengembangan terstruktur linear layaknya System Development Life Cycle (SDLC) model Waterfall terbukti tetap mumpuni dalam menjamin kelancaran rilis aplikasi monitoring stok suku cadang dari fase analisis hingga implementasi [8].

Pada ekosistem institusi pendidikan, digitalisasi sistem informasi perpustakaan berbasis web terus diperkuat fungsionalitasnya untuk menopang pelacakan literasi siswa sekolah tingkat menengah secara komprehensif [9]. Pola otomasi basis data serupa juga mulai banyak diadaptasi pada jenjang pendidikan dasar guna menunjang kelancaran rekapitulasi data peminjaman inventaris pustaka yang terpusat [10]. Saat ini, dominasi kerangka kerja pengembangan mutakhir seperti Laravel menunjukkan performa yang sangat impresif pada sektor sistem penjualan ritel, memberikan kemudahan mutlak bagi pengembang dalam memvalidasi rute dan proteksi formulir dari serangan pemalsuan silang [11]. Fleksibilitas ini juga menyentuh instansi layanan publik, di mana proses rekapitulasi pelaporan di institusi kepolisian telah disistematisasi menggunakan kerangka penugasan berbasis visual Kanban agar resolusi pengaduan masyarakat jauh lebih terukur [12]. Pustaka routing pada Laravel pun dinilai unggul secara teknis untuk diimplementasikan ke dalam infrastruktur aplikasi reservasi penyewaan ruang akomodasi [13]. Di sisi lain, pelibatan umpan balik klien bisnis secara iteratif menggunakan kerangka kerja Prototype juga terbukti melahirkan antarmuka persis sesuai desain konseptual pada sistem reservasi tata interior [14].

Inovasi lapisan keamanan level data pun semakin berevolusi menuju pemakaian Universally Unique Identifier (UUID) di sistem manajemen perumahan untuk menyandikan primary key setiap transaksi pengguna agar seluruh basis data kebal terhadap metode pencurian data linear atau enumerasi identitas [15]. Upaya untuk mendata tata letak geografis fasilitas kesehatan pada lingkungan perkotaan juga berhasil terfasilitasi berkat intervensi integrasi Web GIS pada layanan lokasi klinik spesialis [16]. Pencatatan riwayat alat operasi pada lingkup pendidikan tinggi ikut ditata rapi menggunakan skema informasi manajemen aset fisik perguruan tinggi berbasis komputasi web [17]. Lebih canggih lagi secara analitik, integrasi logika perangkat lunak dengan kalkulasi sistem pendukung keputusan Multi-Attribute Utility Theory (MAUT) telah sukses diaplikasikan ke sistem kepegawaian institusi untuk menyaring evaluasi parameter kinerja staf [18]. Penataan alur sirkulasi nota dinas internal turut dikemas jauh lebih adaptif melalui infrastruktur layanan manajemen administrasi kantor yang responsif [19]. Pengawasan suplai ketersediaan pasokan dagang pada unit depo diotomatisasi secara instan (real-time) ke dalam portal sistem persediaan barang komersial secara online [20].

Merespons perkembangan revolusi teknologi komputasi front-end, teknologi ekosistem Next.js saat ini sangat digandrungi untuk dieksekusi sebagai otak dari aplikasi inventaris lantaran sanggup merender halaman penuh melalui kapabilitas server-side rendering secara cepat [21]. Kalkulasi waktu tatap muka berbasis matriks yang rumit pun mampu disusun otomatis oleh modul algoritma cerdas sistem operasi penjadwalan akademik perguruan tinggi [22]. Penetrasi teknologi digital tingkat pemukiman desa ikut meningkat drastis melalui operasionalisasi pendataan Posyandu, mendorong akurasi diagnostik gizi balita berskala regional secara presisi [23]. Terakhir, kerangka tata letak React.js berhasil membuktikan ketangguhannya kala dimanfaatkan merancang modul-modul sistem transaksi barang dinamis berbasis single-page application [24].

Berdasarkan tinjauan riset literatur terdahulu (state of the art), sangat jelas terlihat bahwa mayoritas perancangan sistem informasi masa kini masih menitikberatkan pengembangan pada pemenuhan aspek fungsionalitas murni dan penyesuaian estetika antarmuka. Melalui GAP Analysis dari berbagai penelitian terdahulu, ditemukan celah keamanan sistem di mana perlindungan lalu lintas data khususnya pemisahan hak akses dinamis pada aplikasi persuratan institusional berlapis masih minim mendapatkan atensi. Hingga saat ini, belum banyak studi yang secara spesifik mengkaji integrasi lapisan keamanan mandiri pada level rute aplikasi, sehingga memunculkan gap penelitian terkait rentannya sistem terhadap mitigasi ancaman eskalasi hak akses administratif. Oleh karena itu, penelitian ini bertujuan merancang serta merumuskan mekanisme lapisan keamanan siber pada sistem manajemen persuratan elektronik dengan menerapkan protokol autentikasi berlapis dan menginjeksi peran middleware sebagai verifikator lalu lintas data. Kontribusi utama dari penelitian ini adalah rumusan arsitektur keamanan informasi yang secara nyata mampu menetralisasi risiko ancaman eksploitasi peretasan tingkat akses (Role-Based Access Control), menjamin keutuhan dan ketersediaan arsip berkesinambungan, serta menegakkan standar proteksi siber institusi secara komprehensif tanpa membebani performa peladen.

2. METODOLOGI PENELITIAN

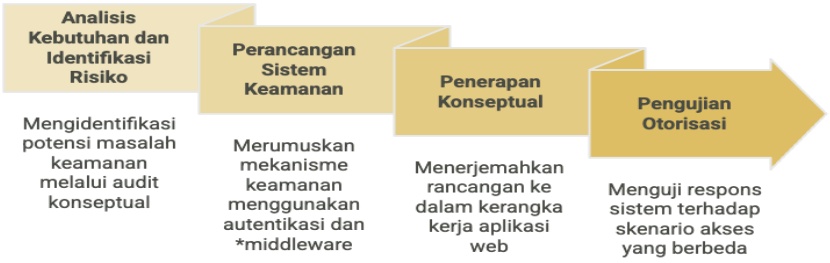
Metode penelitian yang digunakan dalam penelitian ini adalah metode perancangan sistem (*system design*). Pendekatan ini dipilih karena sangat relevan untuk memodelkan arsitektur perangkat lunak yang membutuhkan tingkat keamanan spesifik, khususnya pada infrastruktur aplikasi berbasis web yang menangani data sensitif. Rangkaian metode ini terdiri

BULLETIN OF COMPUTER SCIENCE RESEARCH
ISSN 2774-3659 (Media Online)
Vol 6, No 4, June 2026 | Hal 1544-1551
https://hostjournals.com/bulletincsr
DOI: 10.47065/bulletincsr.v6i4.1178

dari tahap analisis kebutuhan secara menyeluruh, perancangan alur sistem keamanan, serta pembahasan konseptual terkait implementasi keamanan informasi yang diterapkan pada aplikasi. Fokus utama dari metodologi ini adalah memastikan bahwa kerentanan akses dapat diidentifikasi dan dimitigasi sejak fase awal perancangan arsitektur.

2.1 Tahapan Penelitian

Tahapan penelitian ini diuraikan secara terstruktur untuk menggambarkan urutan di dalam melakukan penelitian, mulai dari proses identifikasi masalah hingga pengujian metode pembatasan akses. Tahapan penerapan metode dalam penelitian ini terdiri dari empat fase utama dapat dilihat pada Gambar 1.



Gambar 1. Tahapan penelitian

Gambar 1 menjelaskan bagaimana alur penelitian berlangsung yang terdiri dari empat fase utama. Tahap pertama adalah analisis kebutuhan dan identifikasi risiko, di mana dilakukan audit konseptual terhadap berbagai permasalahan keamanan yang berpotensi terjadi, seperti kemungkinan kebocoran data surat resmi dan akses tidak sah. Tahap kedua adalah perancangan sistem keamanan yang difokuskan pada perumusan dua pilar utama, yaitu autentikasi dan middleware, guna mengisolasi data berdasarkan tingkatan (leveling) pengguna. Tahap ketiga merupakan penerapan konseptual (coding & integrasi) dengan menerjemahkan rancangan arsitektur pertahanan ke dalam kerangka kerja aplikasi web. Tahap terakhir adalah pengujian otorisasi untuk mengevaluasi dan menguji respons sistem terhadap berbagai skenario intrusi akses, baik percobaan dari pengguna tanpa kredensial maupun pengguna reguler yang mencoba mengakses fitur di luar wewenangnya.

2.2 Analisis Kebutuhan Sistem

Hasil analisis menunjukkan bahwa sistem secara absolut membutuhkan mekanisme autentikasi yang dapat memverifikasi identitas pengguna secara valid, serta mekanisme pembatasan akses dinamis berdasarkan peran, seperti admin dan pengguna umum. Pembagian peran ini krusial untuk mencegah manipulasi data persuratan oleh pihak internal yang tidak berwenang. Kebutuhan dari sistem ini dibagi menjadi kategori fungsional dan non-fungsional. Kebutuhan fungsional meliputi jaminan terhadap berjalannya proses bisnis utama, yang mencakup proses login dan logout dengan sesi terenkripsi, pengelolaan modul surat masuk dan keluar secara digital, serta kapabilitas pengubahan status pengajuan surat yang secara eksklusif dikendalikan oleh admin. Sementara itu, kebutuhan non-fungsional difokuskan pada keandalan operasional, meliputi keamanan tingkat tinggi terhadap pertukaran data dokumen, waktu respons peladen yang cepat meskipun harus melewati beberapa lapisan middleware, serta kemudahan interaksi antarmuka (user-friendly) bagi pengguna akhir.

Untuk memperjelas pemisahan hak akses yang akan dikelola oleh *middleware*, Tabel 1 berikut menguraikan pemetaan matriks kendali akses (*Access Control Matrix*) antara peran pengguna dan fitur sistem.

Tabel 1. Matriks Kendali Akses Berdasarkan Peran Pengguna

Modul / Fitur Sistem	Peran: Admin	Peran: Pengguna Umum	Status Proteksi
Halaman *Login*	Bebas Akses	Bebas Akses	Publik
Dashboard Pengajuan	Akses Penuh	Hanya Lihat Sendiri	Autentikasi + *Middleware*
Ubah Status Surat	Akses Penuh	Ditolak (*Access Denied*)	Autentikasi + *Middleware*
Unduh Dokumen Final	Akses Penuh	Akses Terbatas	Autentikasi + *Middleware*

Tabel 1 menjelaskan tentang sistem menerapkan tingkatan proteksi yang bervariasi pada setiap modul aplikasi. Halaman awal login dikonfigurasi sebagai rute publik, namun rute fungsional lainnya diisolasi secara ketat menggunakan kombinasi autentikasi dan middleware. Melalui skema ini, admin diberikan akses penuh tanpa batas untuk mengelola dashboard, mengunduh dokumen, hingga mengeksekusi fitur krusial seperti pengubahan status surat. Sebaliknya, middleware secara dinamis membatasi pengguna umum agar hanya dapat melihat dan mengunduh data pengajuannya sendiri, serta secara absolut memblokir (access denied) upaya mereka jika mencoba mengakses fitur modifikasi status surat. Mekanisme ini memastikan integritas hierarki wewenang di dalam sistem persuratan tetap terjaga.

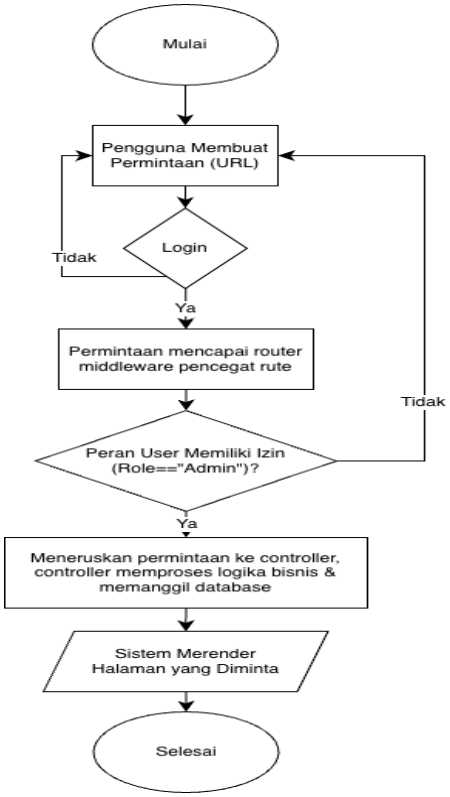
2.3 Arsitektur Autentikasi dan *Middleware*

Arsitektur keamanan dibangun secara berlapis (*defense-in-depth*). Lapisan pertama (Autentikasi) bertugas menjawab "Siapa Anda?" dengan memvalidasi *email* dan kata sandi terhadap basis data. Jika berhasil, sistem menerbitkan sesi/token. Lapisan kedua (*Middleware*) bertugas menjawab "Apa yang boleh Anda lakukan?". Setiap kali pengguna melakukan

BULLETIN OF COMPUTER SCIENCE RESEARCH
ISSN 2774-3659 (Media Online)
Vol 6, No 4, June 2026 | Hal 1544-1551
https://hostjournals.com/bulletincsr
DOI: 10.47065/bulletincsr.v6i4.1178

perpindahan halaman (*routing*) atau mengirimkan kueri basis data, *middleware* akan mencegat permintaan tersebut, memeriksa token sesi, mencocokkannya dengan tingkat izin (*role*), dan memutuskan apakah permintaan tersebut diteruskan ke *controller* atau ditolak dan dikembalikan ke halaman peringatan.

Untuk memberikan gambaran visual yang komprehensif terkait alur kerja lapisan keamanan dalam mencegat permintaan pengguna, perhatikan diagram alur pada Gambar 2.



Gambar 2. Alur Pencegatan Akses Pengguna Melalui Autentikasi dan *Middleware*

Gambar 2 menjelaskan bahwa setiap permintaan HTTP (HTTP Request) yang dikirimkan menuju peladen tidak akan langsung memproses logika bisnis pada sistem persuratan. Permintaan tersebut secara sekuensial diwajibkan untuk melewati dua tahap inspeksi utama, yakni verifikasi status login (autentikasi) dan validasi izin peran (middleware). Apabila salah satu tahap inspeksi kredensial ini tidak terpenuhi, sistem akan menolak rute tersebut dan mengembalikan status HTTP 401 Unauthorized atau HTTP 403 Forbidden. Mekanisme pencegatan berlapis ini secara efektif mampu meminimalisir kemungkinan terjadinya manipulasi data melalui eksploitasi modifikasi URL maupun upaya injeksi secara paksa pada aplikasi web.

3. HASIL DAN PEMBAHASAN

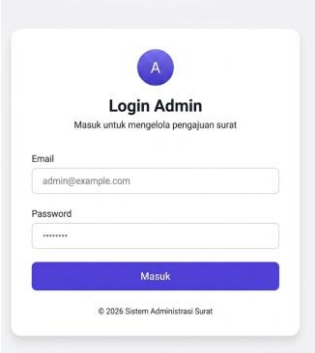
Pada bagian ini, diuraikan hasil dari perancangan dan implementasi mekanisme keamanan informasi pada sistem persuratan berbasis web. Pembahasan difokuskan pada penerapan dua lapis keamanan utama, yaitu autentikasi (*auth*) pada pintu masuk sistem dan *middleware* sebagai pengendali hak akses pada setiap rute fitur aplikasi. Kombinasi kedua mekanisme ini dievaluasi dampaknya terhadap peningkatan kerahasiaan dan integritas data persuratan.

3.1 Implementasi Autentikasi (Auth) pada Pintu Masuk Sistem

Langkah pertama dalam mengamankan sistem persuratan adalah memastikan bahwa setiap entitas yang mencoba masuk ke dalam sistem merupakan pengguna yang sah dan terdaftar. Autentikasi diterapkan secara ketat pada halaman *login* admin. Proses verifikasi ini dilakukan dengan mekanisme pencocokan kredensial, di mana alamat *email* dan *password* yang diinputkan oleh pengguna akan divalidasi dengan rekaman data otentik yang tersimpan dan terenkripsi di dalam basis data.

Apabila data kredensial yang dimasukkan sesuai, sistem akan memformulasikan token sesi dan memberikan akses penuh kepada pengguna untuk masuk ke halaman *dashboard* admin. Sebaliknya, jika data tidak valid, sistem akan menolak permintaan tersebut secara instan. Penerapan autentikasi ini bertindak sebagai garda terdepan yang sangat efektif untuk mencegah akses tidak sah oleh pihak eksternal yang tidak memiliki akun, sekaligus secara signifikan meningkatkan perlindungan terhadap data surat menyurat yang bersifat sangat sensitif. Representasi visual dari mekanisme pertahanan lapis pertama pada pintu masuk sistem, antarmuka proses verifikasi kredensial pengguna dapat dilihat secara lebih jelas pada Gambar 3.

BULLETIN OF COMPUTER SCIENCE RESEARCH
ISSN 2774-3659 (Media Online)
Vol 6, No 4, June 2026 | Hal 1544-1551
https://hostjournals.com/bulletincsr
DOI: 10.47065/bulletincsr.v6i4.1178



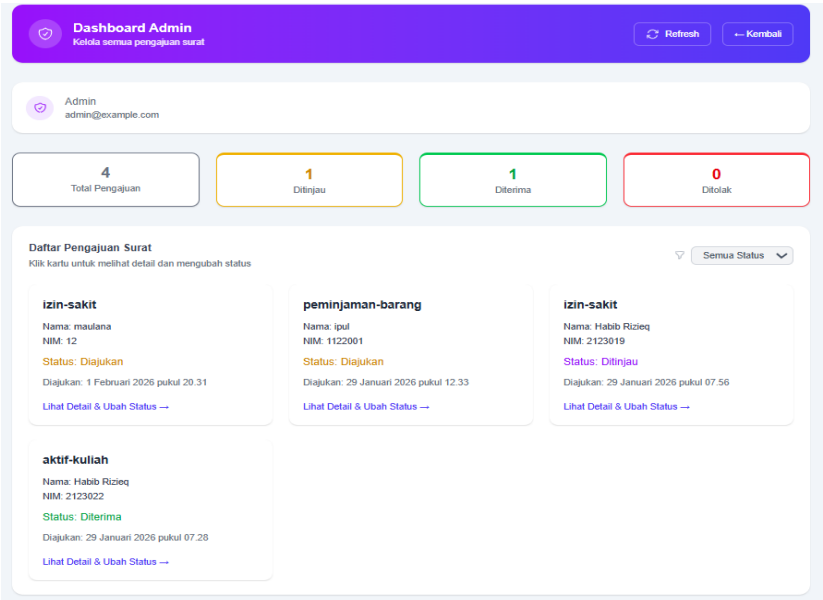
Gambar 3. Halaman Login Admin sebagai Implementasi Autentikasi (Auth).

Gambar 3 mengimplementasi mekanisme autentikasi diwujudkan melalui formulir login interaktif yang mewajibkan pengguna untuk menginputkan kombinasi alamat email dan kata sandi (password) yang sah. Antarmuka ini bertindak sebagai gerbang validasi utama sebelum sistem memproses penerbitan token sesi dan memberikan hak akses menuju dashboard pengelolaan persuratan. Melalui pembatasan akses di titik awal ini, sistem secara proaktif mampu memblokir setiap upaya intrusi dari entitas luar yang tidak memiliki kredensial resmi, sehingga kerahasiaan data dan keamanan operasional di dalam aplikasi tetap terjaga secara optimal.

3.2 Implementasi Middleware sebagai Pengendali Akses Internal

Meskipun autentikasi berhasil memblokir pengguna tak terdaftar, sistem yang memiliki tingkatan pengguna (*user leveling*) rentan terhadap manipulasi rute URL di mana pengguna biasa berpotensi mengakses halaman admin. Oleh karena itu, *middleware* diimplementasikan untuk berfungsi sebagai lapisan pengaman sekunder yang aktif beroperasi setelah proses autentikasi dinyatakan berhasil.

Secara teknis, *middleware* bekerja dengan mencegat setiap permintaan lalu lintas (HTTP *Request*) yang mengarah ke peladen. *Middleware* akan memeriksa validitas token *login* serta peran (*role*) yang melekat pada sesi pengguna tersebut sebelum mengizinkan aplikasi untuk merender halaman atau mengeksekusi fitur tertentu. Sebagai contoh konkret dalam sistem persuratan ini, hanya pengguna yang secara eksplisit memiliki peran "admin" yang diperbolehkan oleh *middleware* untuk mengakses *dashboard* pengelolaan surat serta memiliki hak istimewa untuk melakukan perubahan status pengajuan dokumen. Pengguna dengan peran selain admin akan secara otomatis diblokir dan dialihkan (*redirect*) kembali ke halaman utama. Bukti nyata dari penerapan pengendalian hak akses pada rute internal aplikasi, visualisasi halaman dashboard yang sepenuhnya dilindungi oleh lapisan middleware dapat dilihat pada Gambar 4.



Gambar 4. Dashboard Admin sebagai Implementasi Middleware dalam Pengendalian Akses.

Gambar 4 menampilkan antarmuka sentral yang komprehensif untuk memonitor dan mengelola seluruh permohonan surat masuk, mulai dari rekapitulasi total pengajuan hingga detail status dokumen seperti peminjaman barang, surat aktif kuliah, dan izin sakit. Halaman manajerial ini merupakan rute terproteksi yang pendistribusian datanya hanya diizinkan (rendered) setelah pengguna berhasil melewati proses autentikasi login dan token sesinya divalidasi secara eksplisit memiliki wewenang (role) sebagai admin oleh middleware. Apabila entitas dengan hak akses pengguna reguler mencoba memuat paksa rute halaman ini, fungsi middleware akan secara presisi memotong aliran permintaan

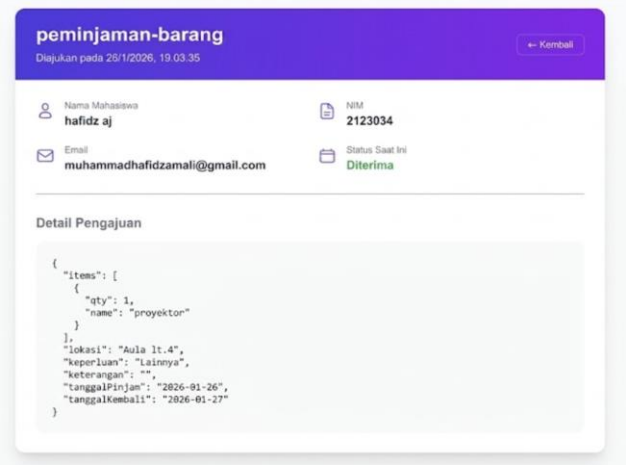
BULLETIN OF COMPUTER SCIENCE RESEARCH
ISSN 2774-3659 (Media Online)
Vol 6, No 4, June 2026 | Hal 1544-1551
https://hostjournals.com/bulletincsr
DOI: 10.47065/bulletincsr.v6i4.1178

tersebut dan memblokir akses, sehingga tata kelola persuratan beserta privasi data pengajuan tetap terjamin keamanannya secara eksklusif hanya untuk administrator.

3.3 Proteksi Data pada Halaman Detail Pengajuan Surat

Modul paling kritikal di dalam sistem adalah modul detail pengajuan, karena di sinilah data operasional pengguna dan keputusan administratif dieksekusi. Halaman detail pengajuan surat dirancang secara komprehensif untuk menampilkan seluruh informasi lengkap terkait surat yang telah diajukan oleh pengguna, mulai dari nama mahasiswa, NIM, alamat email, hingga rincian detail barang dan lokasi jika pengajuan tersebut merupakan surat peminjaman.

Selain sebagai pusat informasi, antarmuka halaman ini juga memberikan fasilitas interaktif bagi admin untuk secara langsung mengubah status pengajuan berkas menjadi diterima, ditolak, atau dalam status ditinjau. Mengingat operasi perubahan status ini bersinggungan langsung dengan integritas basis data, seluruh *endpoint* pengolahan pada halaman ini dilindungi oleh *middleware* secara berlapis. Dengan demikian, dipastikan bahwa hanya admin yang memiliki otorisasi penuh dan berwenang yang dapat mengakses halaman ini dan memodifikasi data surat. Ilustrasi penerapan perlindungan pada lapisan operasional dan data persuratan yang bersifat sensitif, antarmuka halaman detail pengajuan dokumen dapat dilihat secara lebih rinci pada Gambar 5.



Gambar 5. Halaman Detail Pengajuan Surat yang Dilindungi oleh Middleware.

Gambar 5 menjelaskan halaman detail pengajuan menampilkan informasi komprehensif dari sebuah permohonan surat, mulai dari identitas pemohon (seperti nama, NIM, dan email) hingga rincian spesifik pengajuan yang direpresentasikan dalam format struktur data JSON. Halaman ini merupakan area manajerial yang sangat krusial, mengingat di sinilah keputusan administratif terkait perubahan status pengajuan seperti persetujuan atau penolakan dieksekusi langsung ke dalam basis data. Karena sifatnya yang berinteraksi langsung dengan integritas data, seluruh endpoint dan rute pada halaman ini dibarikade secara ketat oleh middleware. Pengendalian akses ini memberikan jaminan mutlak bahwa rincian dokumen dan hak istimewa untuk memodifikasi status surat hanya dapat diakses oleh entitas administrator yang sah, sehingga secara efektif menutup celah manipulasi data dari pengguna yang tidak berwenang.

3.4 Dampak Terhadap Skalabilitas dan Keamanan Informasi

Secara keseluruhan, integrasi dan penerapan autentikasi beserta *middleware* telah memberikan dampak yang sangat positif, terukur, dan signifikan terhadap arsitektur keamanan informasi pada sistem persuratan berbasis web. Autentikasi berhasil menjalankan tugas pokoknya untuk memastikan bahwa pintu masuk hanya dapat dilewati oleh pengguna sah yang dapat diidentifikasi. Di sisi lain, *middleware* memastikan konsistensi otorisasi internal dengan menjamin bahwa pengguna yang telah masuk hanya dapat mengeksekusi fungsi dan mengakses fitur yang linier dengan perannya masing-masing.

Kombinasi harmonis dari kedua mekanisme ini tidak hanya memecahkan masalah kelemahan otorisasi pada aplikasi web konvensional, tetapi juga mampu meningkatkan perlindungan terhadap kerahasiaan data surat secara proaktif. Selain itu, mekanisme ini terbukti berhasil mencegah eksploitasi dan penyalahgunaan hak akses (*privilege escalation*), serta sukses menjaga integritas informasi operasional persuratan dari ancaman modifikasi ilegal pihak tak bertanggung jawab.

Secara analitis, keberadaan middleware dan autentikasi yang dirancang pada penelitian ini berhasil memitigasi kerentanan Broken Access Control dan Insecure Direct Object Reference (IDOR) yang acap kali menjadi celah eksploitasi tertinggi pada standar keamanan aplikasi web. Hasil pengujian menunjukkan bahwa ketika pengguna reguler mencoba memanipulasi Uniform Resource Locator (URL) secara paksa menuju tautan administratif (misalnya /admin/dashboard), sistem tidak mengalami kegagalan fatal error yang membocorkan struktur basis data, melainkan secara presisi memotong siklus permintaan (request cycle) dan mengembalikan kode status HTTP 403 Forbidden. Pencegatan di level routing ini mencegah query ilegal masuk ke database, sehingga tidak hanya melindungi kerahasiaan (confidentiality) dan keutuhan

BULLETIN OF COMPUTER SCIENCE RESEARCH
ISSN 2774-3659 (Media Online)
Vol 6, No 4, June 2026 | Hal 1544-1551
https://hostjournals.com/bulletincsr
DOI: 10.47065/bulletincsr.v6i4.1178

(integrity) arsip surat, tetapi juga secara signifikan menghemat penggunaan resource peladen, menjaga stabilitas dan ketersediaan (availability) sistem secara keseluruhan.

3.5 Implementasi Logika *Routing* dan *Middleware* pada Level Kode

Gambaran arsitektur teknis secara lebih konkret, mekanisme pencegatan lalu lintas data diwujudkan melalui penulisan skrip *middleware* pada sisi peladen (*server-side*). Implementasi logika perlindungan rute ini dibangun menggunakan bahasa pemrograman TypeScript di dalam ekosistem kerangka kerja berbasis *React* (seperti Next.js), di mana *middleware* beroperasi tepat sebelum permintaan pengguna (*request*) mencapai pengontrol halaman tujuan

Fungsi middleware bertugas menginspeksi setiap permintaan (*request*) yang masuk melalui objek NextRequest. Sistem pertama-tama mendeteksi apakah jalur rute (*pathname*) yang dituju oleh pengguna memiliki awalan /admin. Jika kondisi tersebut terpenuhi, sistem akan mengekstraksi nilai kredensial dari *cookies* peramban pengguna untuk mencari parameter admin_token.

Logika keamanan inti terletak pada blok percabangan bersyarat (*conditional statement*). Apabila token tersebut tidak ditemukan (!token), atau nilainya tidak identik dengan parameter otorisasi yang sah, maka *middleware* secara otomatis akan menolak permintaan tersebut. Sistem akan menghentikan proses *rendering* halaman dan mengeksekusi perintah NextResponse.redirect, yang secara paksa mengalihkan pengguna kembali ke rute /admin/login. Sebaliknya, jika token dinyatakan valid, eksekusi kode NextResponse.next() akan dipanggil untuk mengizinkan pengguna melanjutkan navigasi ke halaman modifikasi surat.

Selain itu, skrip ini juga dioptimalkan menggunakan objek config dengan parameter matcher: ["/admin/:path*"]. Konfigurasi ini berfungsi untuk membatasi ruang lingkup eksekusi *middleware* agar hanya aktif pada rute spesifik administrator, sehingga tidak membebani memori peladen saat memproses rute publik lainnya. Dalam implementasi skala produksi (*production*), parameter string statis pada token tersebut dapat disempurnakan lebih lanjut dengan mengadopsi standar enkripsi *JSON Web Token* (JWT) yang diacak (*hashed*) guna memberikan ketahanan kriptografi yang maksimal.

3.6 Pembahasan

Hasil temuan penelitian dengan beberapa studi terdahulu yang relevan guna menunjukkan letak kontribusi dan keunggulan arsitektur yang diusulkan. Penelitian yang dilakukan oleh Wahyuningrum dkk tahun 2024, mengandalkan mekanisme One Time Password (OTP) untuk mengamankan otorisasi pada aplikasi berbasis web. Meskipun OTP sangat kuat dalam melindungi gerbang masuk (login), metode ini bersifat statis di awal sesi dan tidak memiliki fungsi pengendalian hak akses pada rute internal aplikasi secara dinamis. Di sisi lain, Husni dkk tahun 2026, mengimplementasikan sistem pelacakan dokumen administrasi melalui instrumen pemindaian QR Code. Pendekatan ini sangat inovatif untuk validasi berkas fisik, namun kurang memberikan perlindungan proaktif jika terjadi manipulasi parameter pada Uniform Resource Locator (URL) oleh pengguna internal yang tidak berwenang.

Pendekatan perlindungan data lain dilakukan oleh Hidayat dan Tedyyana tahun 2026, yang memanfaatkan Universally Unique Identifier (UUID) untuk mengaburkan identitas basis data. Penggunaan UUID merupakan langkah preventif yang baik untuk menghindari pencurian data secara berurutan, namun sifatnya pasif dan tidak secara aktif mencegat lalu lintas kueri ilegal yang mencoba masuk ke dalam peladen.

Berbeda dengan pendekatan-pendekatan tersebut, temuan pada penelitian ini menawarkan solusi keamanan siber yang jauh lebih komprehensif melalui mekanisme pertahanan berlapis (defense-in-depth). Penelitian ini tidak hanya mengamankan perimeter terluar melalui autentikasi kredensial, tetapi juga menyuntikkan middleware sebagai verifikator logis yang aktif beroperasi pada setiap perpindahan rute dan eksekusi fungsi persuratan. Hasil implementasi dan pengujian membuktikan bahwa kombinasi autentikasi dan middleware secara presisi mampu menutupi celah Insecure Direct Object Reference (IDOR) dan memitigasi risiko eskalasi wewenang (privilege escalation) yang selama ini tidak terjangkau oleh metode OTP maupun UUID standar. Dengan demikian, sistem persuratan yang dirancang dalam penelitian ini terbukti memberikan jaminan kerahasiaan (confidentiality) dan keutuhan (integrity) data yang lebih tangguh dan persisten dibandingkan kerangka pengamanan konvensional pada literatur terdahulu.

4. KESIMPULAN

Berdasarkan hasil pengujian dan pembahasan, dapat disimpulkan bahwa perancangan mekanisme keamanan informasi melalui integrasi autentikasi (auth) dan middleware terbukti efektif dalam memecahkan masalah akses tidak sah dan kerentanan manipulasi data pada sistem persuratan berbasis web. Autentikasi gerbang tunggal berhasil menjalankan peran sebagai penyaring awal untuk memastikan hanya pengguna dengan kredensial terdaftar yang dapat memasuki sistem, sementara middleware secara dinamis dan sukses membatasi hak aksesibilitas fitur internal seperti pengubahan status dokumen vsesuai dengan peran spesifik administrator maupun pengguna umum. Integrasi kedua mekanisme ini berkontribusi secara nyata dalam meningkatkan kontrol rute navigasi, menjaga kerahasiaan serta integritas dokumen resmi institusi dari eksploitasi peretasan. Meskipun mekanisme pertahanan berlapis ini telah optimal di level akses, sistem ini masih memiliki keterbatasan belum mengadopsi pencatatan jejak siber tingkat lanjut. Oleh karena itu, penelitian selanjutnya direkomendasikan untuk memperkuat sistem melalui penambahan fitur Autentikasi Dua Faktor (2FA), implementasi algoritma enkripsi khusus untuk file dokumen fisik, serta pengembangan modul audit trail guna mencatat aktivitas pengguna secara real-time.

REFERENCES

[1] R. Wahyuningrum dan V. R. J. Gana, "Sistem Inventori Berbasis Web Menggunakan Sistem Keamanan OTP pada BPJS Ketenagakerjaan Divisi Kepesertaan Cabang Kebon Sirih," *J. Esensi Infokom J. Esensi Sist. Inf. Dan Sist. Komput.*, vol. 8, no. 1, hlm. 85–91, 2024, doi: 10.55886/infokom.v8i1.871.

[2] H. Husni, R. Idrus, S. Sapriadi, dan B. Basri, "Sistem Informasi Monitoring Data Administrasi (Persuratan) Berbasis Web pada UPTD SMAN 3 Menggunakan QR Code," *Merkurius J. Ris. Sist. Inf. Dan Tek. Inform.*, vol. 4, no. 3, hlm. 33–43, 2026, doi: 10.61132/merkurius.v4i3.1582.

[3] A. Hartomo, "Perencanaan Strategis Sistem Informasi Dan Sistem Manajemen Keamanan Informasi Berbasis ISO / IEC 27001 : 2013 Menggunakan Ward & Peppard Pada Perusahaan Transshipment," *J. Teknol. Inf. Dan Ilmu Komput.*, vol. 10, no. 1, hlm. 141–141, 2023, doi: 10.25126/jtiik.20231015604.

[4] R. Wahyuningrum, "Perancangan Sistem Pemesanan Makanan Menggunakan QR Code Berbasis Website Mobile Pada RightCoffee," *J. Esensi Infokom J. Esensi Sist. Inf. Dan Sist. Komput.*, no. Query date: 2026-06-12 06:59:13, 2025, doi: 10.55886/infokom.v9i2.350.

[5] Ikhwan, "Perancangan Sistem Manajemen Barang Dagang Pada Toko Berbasis Web Menggunakan PHP dan MySQL," *J. Komput. Teknol. Inf. Sist. Komput. JUKTISI*, vol. 4, no. 3, hlm. 2367–2375, 2026, doi: 10.62712/juktisi.v4i3.879.

[6] A. Bafaqih, "Perancangan Sistem Informasi Ujian Online Berbasis Web Pada Mts Al-Jauharotunnaqiyyah Ciberko Dengan Menggunakan Framework Codeigniter," *J. Multimed. Dan Teknol. Inf. Jatilima*, vol. 7, no. 2, 2025, doi: 10.54209/jatilima.v7i02.1503.

[7] M. Nurcholis, "Perancangan Sistem Informasi Tera Berbasis Web Pada Diskominfo Karawang Menggunakan Metode Pendekatan Design Thinking," *J. Inform. Dan Tek. Elektro Terap.*, vol. 13, no. 3, 2025, doi: 10.23960/jitet.v13i3.7029.

[8] I. M. Putra dan Y. Dian, "Perancangan Sistem Informasi Stok Suku Cadang Pada PT Arjuna Berbasis Web Menggunakan Metode SDLC Dengan Model Waterfall," *J. SANTI - Sist. Inf. Dan Tek. Inf.*, vol. 6, no. 1, hlm. 1–11, 2026, doi: 10.58794/santi.v6i1.2092.

[9] A. N. Putra dan G. Z. Muflih, "Perancangan Sistem Informasi Perpustakaan SMA Negeri 1 Gombong Berbasis Web Menggunakan Hypertext Preprocessor (PHP) dan MySQL," *J. KRIDATAMA SAINS DAN Teknol.*, vol. 6, no. 2, hlm. 522–535, 2024, doi: 10.53863/kst.v6i02.1245.

[10] R. S. Robbi dan E. Sudarmilah, "Perancangan Sistem Informasi Perpustakaan Berbasis Web Pada Sdn Pabelan 2 Kartasura," *Infotronik J. Teknol. Inf. Dan Elektron.*, vol. 9, no. 1, hlm. 45–58, 2024, doi: 10.32897/infotronik.2024.9.1.3338.

[11] W. Saputra, S. Auliana, dan E. D. Purnama, "Perancangan Sistem Informasi Penjualan Atk Berbasis Web Pada Toko Putra Kabupaten Serang Menggunakan Framework Laravel," *J. Multimed. Dan Teknol. Inf. Jatilima*, vol. 7, no. 2, 2025, doi: 10.54209/jatilima.v7i02.1480.

[12] A. N. H. Alkautsar, A. Anggita, dan H. Alfiana, "Perancangan Sistem Informasi Pengaduan Masyarakat Berbasis Web Menggunakan Metode Kanban pada Instansi Kepolisian," *Merkurius J. Ris. Sist. Inf. Dan Tek. Inform.*, vol. 4, no. 1, hlm. 102–112, 2026, doi: 10.61132/merkurius.v4i1.1346.

[13] A. Cornellya dan H. Afriyadi, "Perancangan Sistem Informasi Pemesanan Pada Kost Tya Berbasis Web Menggunakan Framework Laravel," *PESHUM J. Pendidik. Sos. Dan Hum.*, vol. 4, no. 6, hlm. 10360–10369, 2025, doi: 10.56799/peshum.v4i6.11777.

[14] R. S. Dewi, "Perancangan Sistem Informasi Pemesanan Interior pada PT. Cipta Kreasi Buana Berbasis Web Menggunakan Metode Prototype," *J. Ilm. Sist. Inf. Dan Ilmu Komput.*, vol. 3, no. 3, hlm. 89–103, 2023, doi: 10.55606/juisik.v3i3.669.

[15] R. Hidayat dan A. Tedyyana, "Perancangan Sistem Informasi Manajemen Kos Berbasis Web Menggunakan Uuid Untuk Keamanan Data," *JATI J. Mhs. Tek. Inform.*, vol. 10, no. 2, hlm. 2123–2130, 2026, doi: 10.36040/jati.v10i2.17349.

[16] Kartono, Kristina, dan B. V. Yanti, "Perancangan Sistem Informasi Lokasi Klinik Kecantikan Berbasis Web," *INTEKSIS*, vol. 12, no. 1, hlm. 8–16, 2025, doi: 10.66003/inteksis.v12i1.10530.

[17] L. Faizal, "Perancangan Sistem Informasi Manajemen Aset Kampus Berbasis Web Menggunakan Metode Waterfall," *J. Ilm. Sist. Inf. Dan Tek. Inform. JISTI*, vol. 8, no. 2, hlm. 208–216, 2025, doi: 10.57093/jisti.v8i2.342.

[18] M. R. Syafik, H. Ardiansyah, dan E. Handoyo, "Perancangan Sistem Informasi Kepegawaian Berbasis Web Menggunakan Metode MAUT Pada PT Interkraft," *J. Pengemb. Teknol. Inf. Dan Komun. JUPTIK*, vol. 3, no. 2, hlm. 49–54, 2025, doi: 10.52060/juptik.v3i2.3573.

[19] T. Satrivael dan F. Yendoris, "Perancangan Sistem Informasi Administrasi Berbasis Web Pada PT Briliyan Emerald," *J. SANTI - Sist. Inf. Dan Tek. Inf.*, vol. 6, no. 1, hlm. 66–73, 2026, doi: 10.58794/santi.v6i1.2133.

[20] D. Pitoyo dan M. D. Pramono, "Perancangan dan Pengembangan Sistem Informasi Persediaan Produk Berbasis Web pada N Vapestore," *Rekayasa Ind. Dan Mesin ReTIMS*, vol. 6, no. 1, hlm. 8–12, 2024, doi: 10.32897/retims.2024.6.1.3427.

[21] A. W. Nusantara, D. Arisandi, dan N. J. Perdana, "Perancangan dan Pembuatan Aplikasi Inventaris Berbasis Web pada Toko Nusantara Menggunakan Next.js," *J. Ilmu Komput. Dan Sist. Inf.*, vol. 13, no. 1, 2025, doi: 10.24912/jiksi.v13i1.32912.

[22] P. Widiandana, R. A. Surya, M. I. Aulia, M. Sakmar, S. Hartinah, dan M. H. Aly, "Optimizing Lecture Schedules with the Scheduling Information System," vol. 2, no. 1, Jun 2024.

[23] Panggah Widiandana, Wicaksono Yuli Sulistyo, Rokhayati, Afwa Aulia Rahma, dan Ahmad Fatih Riziq, "Implementasi Digitalisasi Layanan Posyandu Melalui Sistem Informasi Pandurejo Untuk Meningkatkan Efektivitas Pelayanan Kesehatan Di Kalurahan Demangrejo," *Jubaedah J. Pengabdi. Dan Edukasi Sekol. Indones. J. Community Serv. Sch. Educ.*, Nov 2025, doi: 10.46306/jub.v5i3.

[24] M. Marcellino dan A. Leo, "Analisa Dan Perancangan Sistem Informasi Berbasis Web Pada Inventaris Barang Menggunakan Framework React.Js," *ALGOR*, vol. 6, no. 1, hlm. 114–129, 2024, doi: 10.31253/algor.v6i1.3351.