JURNAL ILMIAH SISTEM INFORMASI (JUSI)
VOL 4, No. 3, November 2025, pp. 674 - 687
p-ISSN : 2803-1507 (media cetak) | e-ISSN : 2803-1531 (media online)
Link Publikasi: https://ejurnal.provisi.ac.id/index.php/JUISI/issue/view/151

Academic Portal with MFA (WhatsApp OTP via Fonnte), Role-Based Access Control, and Logging System for Network Monitoring

Albert Ramadhan Manik*[1], Dedy kiswanto[2], Muhammad Budi Akbar[3], Jogi Purba[4]
[1,2,3,4] Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Negeri Medan
Jl. William Iskandar Ps. V, 20221, Medan, Sumatera Utara, Indonesia
e-mail: albertmanik.4232550004@mhs.unimed.ac.id*[1]; dedykiswanto@unimed.ac.id[2];
mbudiakbar12@mhs.unimed.ac.id[3]; jogipurba25@mhs.unimed.ac.id[4]

ARTICLE INFO

Article History:

Received: 17-09-2025
Revised: 18-10-2025
Accepted: 25-10-2025
Published: 21-11-2025

ABSTRACT

This study aims to develop a web-based academic portal with a multi-layered security system to enhance data protection and operational efficiency. The system integrates Multi-Factor Authentication (MFA) using WhatsApp OTP via Fonnte, Role-Based Access Control (RBAC), and a user activity logging mechanism to ensure security, transparency, and accountability. Additionally, a web-based security monitoring feature is implemented, allowing administrators to observe user activities in real-time and respond promptly to potential threats. The testing results indicate that the combination of MFA, RBAC, and logging effectively strengthens the system against unauthorized access while improving its stability and reliability. Therefore, the developed system proves to be an effective solution for securing academic data, minimizing security risks, and optimizing the management of educational information.

Keywords: *Academic Portal, System Security, Multi-Factor Authentication (MFA), Role-Based Access Control (RBAC), Logging, Security Monitoring, WhatsApp OTP.*

Abstrak

Penelitian ini bertujuan mengembangkan portal akademik berbasis web dengan sistem keamanan berlapis untuk meningkatkan perlindungan data dan efektivitas operasional. Sistem ini mengintegrasikan *Multi-Factor Authentication* (MFA) melalui OTP WhatsApp via Fonnte, *Role-Based Access Control* (RBAC), serta mekanisme *logging* aktivitas pengguna guna memastikan keamanan, transparansi, dan akuntabilitas. Selain itu, fitur *security monitoring* berbasis web dirancang agar administrator dapat memantau aktivitas pengguna secara *real-time* dan menanggapi potensi ancaman dengan lebih cepat. Hasil pengujian menunjukkan bahwa penerapan kombinasi MFA, RBAC, dan *logging* mampu memperkuat sistem dari akses tidak sah sekaligus meningkatkan kestabilan dan keandalannya. Dengan demikian, sistem yang dikembangkan terbukti efektif dalam menjaga keamanan data, mengurangi risiko pelanggaran, serta mendukung pengelolaan informasi akademik secara optimal.

Kata Kunci: *Portal Akademik, Keamanan Sistem, Multi-Factor Authentication (MFA), Role-Based Access Control (RBAC), Logging, Security Monitoring, OTP WhatsApp.*

1. PENDAHULUAN

DOI: https://doi.org/10.51903/qwz6pt87

p-ISSN : 2803-1507 e-ISSN : 2803-1531

Perkembangan teknologi informasi dan komunikasi telah mendorong organisasi dan perusahaan untuk beralih dari sistem manual menuju sistem berbasis web yang lebih efisien dan fleksibel. Sistem berbasis web tidak hanya mempercepat proses kerja, tetapi juga memungkinkan monitoring secara *real-time* serta pencatatan data yang lebih akurat [1]. Implementasi sistem ini terbukti meningkatkan efisiensi dan kualitas produksi, seperti pada proses robot painting yang memanfaatkan *real-time monitoring* untuk mengoptimalkan hasil kerja [1]. Selain itu, *website* kini juga digunakan sebagai media promosi dan layanan informasi utama yang memperluas jangkauan publik dan meningkatkan daya saing perusahaan [2].

Dalam bidang jaringan, penerapan sistem berbasis *web* dimanfaatkan untuk layanan dan pemantauan infrastruktur.pengembangkan sistem monitoring jaringan *WiFi* berbasis *web mobile* yang mampu meningkatkan kualitas layanan dan mempermudah deteksi gangguan [3]. Sementara itu merancang antarmuka pengguna berbasis *web* untuk otomasi konfigurasi jaringan *multivendor* agar pengelolaan perangkat menjadi lebih efisien dan terintegrasi [4]. Penggunaan teknologi web dalam manajemen jaringan memberikan fleksibilitas tinggi serta mendukung pengawasan jarak jauh secara efektif.

Di bidang pendidikan dan lingkungan, sistem berbasis *web* juga berperan penting dalam meningkatkan transparansi dan efisiensi.mengembangkan sistem informasi *logbook* PKL berbasis *web* dengan fitur *real-time monitoring* untuk mempermudah pelaporan dan evaluasi akademik [5]. Dalam bidang lingkungan,mengimplementasikan teknologi *Human Machine Interface* (HMI) berbasis *web* untuk monitoring dan kendali kualitas air tambak udang berbasis IoT guna meningkatkan efektivitas pemantauan jarak jauh [6]. Kedua penelitian ini menunjukkan bahwa sistem berbasis *web* mampu meningkatkan produktivitas dan ketepatan pengelolaan data di berbagai bidang.

Selain itu, penerapan sistem berbasis web juga mendukung aspek keamanan dan pengawasan data. penerapan algoritma *Isolation Forest* untuk mendeteksi anomali pada *log web server* [7], sedangkan [8] memanfaatkan *Security Information and Event Management* (SIEM) *Splunk* untuk deteksi anomali jaringan secara *real-time*. [9] mengembangkan aplikasi deteksi anomali jaringan berbasis *Python* dengan implementasi SIEM, serta [10] menggunakan *Role-Based Access Control* (RBAC) untuk memperkuat keamanan data dalam sistem ERP berbasis *web*. Dengan demikian, sistem *logging* dan monitoring berbasis *web* menjadi solusi penting untuk meningkatkan efisiensi, transparansi, dan keamanan informasi di berbagai sektor.

Penelitian [6] membuktikan bahwa autentikasi OTP berbasis *WhatsApp* melalui penyedia API lokal *Fonnte* mampu memberikan waktu respons rata-rata 1,2 detik dalam sistem akademik, sementara studi [2] menekankan efektivitas integrasi *Multi-Factor Authentication (MFA)* dan *Role-Based Access Control (RBAC)* dalam memperkuat keamanan akses pada lingkungan *cloud*. Namun, [4] mengidentifikasi bahwa implementasi MFA di berbagai platform masih menghadapi inkonsistensi pengalaman pengguna dan kurangnya keterpaduan antara autentikasi, otorisasi, serta sistem pemantauan. Berdasarkan celah tersebut, penelitian ini berkontribusi dengan mengembangkan sistem keamanan portal akademik yang mengintegrasikan OTP *WhatsApp* berbasis *Fonnte* dalam skema MFA, dilengkapi mekanisme RBAC, *logging*, dan *monitoring* aktivitas secara terpadu untuk meningkatkan keamanan, keandalan, dan transparansi sistem informasi akademik. Integrasi beberapa mekanisme autentikasi tersebut diharapkan dapat menciptakan sistem yang lebih adaptif terhadap ancaman keamanan yang terus berkembang di lingkungan digital.

2. TINJAUAN PUSTAKA

Penelitian dalam bidang keamanan jaringan terus berkembang seiring meningkatnya kompleksitas infrastruktur digital dan potensi ancaman siber. Kajian [11] menjelaskan bahwa kriptografi dan protokol enkripsi menjadi dasar dalam melindungi data dari penyadapan serta menjaga komunikasi tetap aman. Dalam konteks sistem modern, [12] menyoroti kebutuhan arsitektur keamanan berlapis terutama untuk *smart grid* dan sistem IoT yang semakin rentan terhadap serangan terdistribusi. Di sisi lain, [13] menegaskan bahwa penerapan *artificial intelligence* dan *machine learning* dalam keamanan jaringan dapat mengidentifikasi pola anomali secara otomatis dan mempercepat deteksi ancaman. Hal ini sejalan dengan hasil [14] yang meneliti deteksi pencurian data pada perangkat mobile menggunakan model pembelajaran mesin untuk mengantisipasi serangan berbasis perilaku, menunjukkan relevansi tinggi antara pendekatan *AI-based threat detection* dan keamanan sistem jaringan terkini. Selain itu, penelitian [15] menyoroti pentingnya efisiensi energi dan praktik *green software* dalam pengembangan arsitektur sistem modern, yang berkontribusi terhadap keamanan dan keberlanjutan lingkungan komputasi awan.

p-ISSN : 2803-1507 e-ISSN : 2803-1531

Aspek lain yang banyak dikaji adalah penerapan sistem *logging* dan pemantauan (*monitoring*) dalam pengelolaan keamanan jaringan. Studi [16] mengembangkan mekanisme *secure logging* berkecepatan tinggi pada perangkat IoT dengan pendekatan tanda tangan kriptografi dan verifikasi *batch*, sementara [17] menunjukkan bagaimana integrasi *logging* ke dalam sistem *Security Information and Event Management* (SIEM) mampu menyaring ancaman secara efisien melalui *threat log filtering*. Hasil penelitian [18] juga mendukung temuan tersebut dengan menekankan pentingnya edukasi digital dan sistem log terintegrasi dalam perlindungan privasi pengguna serta mitigasi dampak sosial dari pelanggaran data. Penerapan sistem *logging* adaptif yang terhubung ke mekanisme monitoring berbasis *cloud* terbukti meningkatkan transparansi serta mempercepat respon terhadap anomali jaringan. Penelitian [19] juga mengembangkan sistem monitoring deteksi dini kebakaran berbasis IoT yang menunjukkan efektivitas pemantauan real-time terhadap kondisi infrastruktur server, sehingga mendukung keamanan operasional jaringan secara menyeluruh.

Dalam konteks keamanan aplikasi berbasis *web*, beberapa penelitian fokus pada penerapan sistem autentikasi berlapis seperti *Multi-Factor Authentication* (MFA) dan *One-Time Password* (OTP). Penelitian [20], [21] menunjukkan bahwa kombinasi MFA dengan OTP dapat meningkatkan ketahanan terhadap serangan *brute-force* dan *replay attack*. Temuan serupa juga diperkuat oleh [6], yang berhasil menerapkan OTP berbasis WhatsApp melalui API lokal Fonnte untuk mempercepat proses autentikasi pengguna pada sistem akademik. Namun, studi [4] mengidentifikasi masih adanya inkonsistensi pada penerapan MFA lintas platform yang tidak terintegrasi dengan sistem logging dan monitoring. Untuk menjawab tantangan tersebut, [22] menekankan pentingnya integrasi MFA, RBAC, dan mekanisme pemantauan berbasis web sebagai model keamanan akademik modern yang mampu menjamin keandalan autentikasi dan akuntabilitas pengguna.

Selain autentikasi, pengaturan otorisasi berbasis peran juga menjadi perhatian penting dalam sistem keamanan modern. Studi [10] mengimplementasikan *Role-Based Access Control* (RBAC) pada sistem ERP untuk meningkatkan efisiensi dan menjaga kerahasiaan data organisasi, sementara [20] mengembangkan sistem otorisasi terpusat berbasis *Flask* yang memperkuat konsistensi hak akses antar modul aplikasi. Implementasi RBAC yang terintegrasi dengan MFA seperti yang dijelaskan dalam [2] terbukti dapat menekan risiko akses tidak sah pada sistem *cloud*. Penelitian [23], [9] juga menegaskan pentingnya sistem deteksi anomali yang dikombinasikan dengan RBAC agar administrator dapat memantau dan mengontrol perilaku pengguna secara *real-time* melalui dashboard *web* yang interaktif dan adaptif terhadap perubahan lalu lintas jaringan.

Secara umum, penelitian-penelitian terdahulu menunjukkan bahwa kombinasi antara MFA, RBAC, logging, dan monitoring berbasis web memberikan perlindungan yang lebih komprehensif terhadap serangan jaringan dan pelanggaran data. [24] menerapkan algoritma Isolation Forest untuk mendeteksi aktivitas tidak wajar pada *log server* secara otomatis, sementara [25] mengembangkan sistem monitoring jaringan dengan notifikasi real-time yang mampu mempercepat respon terhadap gangguan. Berdasarkan berbagai temuan tersebut, penelitian ini berupaya memperkuat pendekatan keamanan holistik dengan mengintegrasikan OTP *WhatsApp* dalam skema MFA serta sistem RBAC, *logging*, dan *monitoring* yang berjalan secara sinkron pada portal akademik. Pendekatan ini diharapkan mampu mengatasi celah integrasi keamanan yang masih menjadi tantangan pada sistem akademik digital berbasis *web*.

3. METODOLOGI PENELITIAN

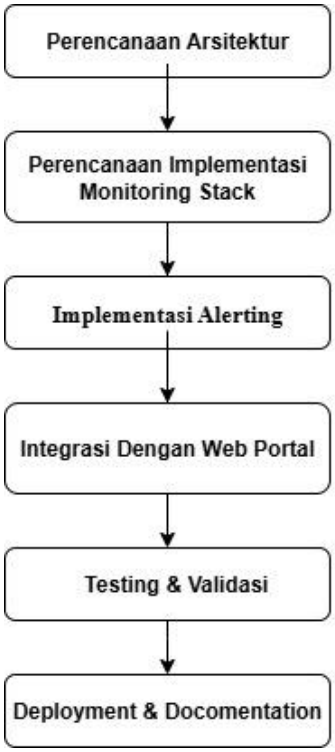
3.1. *Jenis Penelitian*

Pengembangan portal akademik berbasis *web* dengan fokus pada aspek keamanan dan transparansi data pribadi menjadi sangat penting di era digital saat ini. Sistem penilaian akademik dikembangkan dengan memanfaatkan teknologi modern agar setiap data nilai siswa tersimpan secara permanen, terlindungi, dan tidak dapat diubah. Pendekatan penelitian yang digunakan bersifat *Research and Development* (R&D), yang tidak hanya berorientasi pada pembuatan perangkat lunak, tetapi juga pada pengujian efektivitas dan keandalannya. Hasil pengujian menunjukkan peningkatan dalam efisiensi pengelolaan data, kepercayaan pengguna, serta perlindungan informasi pribadi sesuai ketentuan UU No. 27 Tahun 2022. Secara keseluruhan, penelitian ini menegaskan perlunya sinergi antara bidang pendidikan dan teknologi guna memperkuat keamanan serta integritas sistem akademik digital di Indonesia [24].

3.2. *Tahapan Penelitian*

p-ISSN : 2803-1507 e-ISSN : 2803-1531

Alur kerja proses autentikasi OTP dalam sistem ditunjukkan pada Gambar 1, yang menggambarkan tahapan mulai dari Perencanaan Arsitektur hingga *Deployment & Documentation*. Proses autentikasi ini dirancang untuk memastikan keamanan data pengguna dalam setiap tahap interaksi dengan sistem. Selain itu, setiap langkah dalam alur kerja telah diuji agar dapat berjalan secara konsisten di berbagai kondisi jaringan, in dapat dilihat melalui Gambar 1.



Gambar 1. Flowchart autentikasi yang diguanakan dalam penelitian

3.2.1. *Perencanaan Arsitektur*

Tahap ini mencakup perancangan struktur sistem portal akademik yang terhubung dengan komponen monitoring jaringan melalui aktivitas pengguna. Arsitektur dirancang agar data performa server dan aktivitas pengguna dapat dikumpulkan dan ditampilkan melalui *dashboard* portal secara efisien dan aman. Setiap komponen arsitektur memiliki peran tersendiri dalam mendukung efisiensi sistem secara keseluruhan. Struktur yang dirancang juga mempertimbangkan skalabilitas agar sistem dapat dikembangkan sesuai kebutuhan institusi di masa mendatang.

3.2.2. *Perencanaan Implementasi Monitoring Stack*

Pada tahap ini dilakukan perancangan sistem monitoring dengan menyiapkan *Windows Exporter* untuk pengumpulan data performa *server* dan jaringan. Data tersebut akan menjadi dasar untuk pemantauan kondisi sistem secara *real-time*. Sistem monitoring ini dirancang agar dapat mendeteksi perubahan performa server secara cepat dan akurat. Dengan demikian, administrator dapat mengambil langkah preventif sebelum terjadi penurunan kinerja sistem.

3.2.3. *Implementasi Alerting*

Tahap ini menerapkan sistem notifikasi otomatis menggunakan WhatsApp via *Fonnte*. Notifikasi dikirim kepada administrator apabila terdeteksi anomali atau gangguan pada sistem, sehingga masalah dapat segera ditangani. Mekanisme ini menggunakan *API* untuk mengirimkan pesan otomatis dengan format yang telah ditentukan. Pengujian dilakukan untuk memastikan bahwa setiap notifikasi dapat diterima dengan cepat dan tidak terjadi keterlambatan.

3.2.4. *Integrasi Dengan Web Portal*

p-ISSN : 2803-1507 e-ISSN : 2803-1531

Tahap ini menggabungkan sistem monitoring dan alerting dengan portal akademik. Proses integrasi juga mencakup penerapan *MFA (OTP WhatsApp)* dan *Role-Based Access Control (RBAC)* untuk menjamin keamanan akses pengguna. Integrasi dilakukan dengan menyesuaikan struktur basis data agar mendukung sistem keamanan berlapis. Proses ini juga melibatkan sinkronisasi antar modul agar fungsi autentikasi dan kontrol akses dapat berjalan tanpa konflik.

3.2.5. *Testing & Validasi*

Tahap ini dilakukan untuk memastikan seluruh fungsi berjalan dengan baik. Pengujian difokuskan pada aspek fungsionalitas, integrasi antar komponen, serta keamanan sistem otentikasi dan pengiriman OTP. Pengujian dilakukan menggunakan skenario yang merepresentasikan kondisi nyata di lingkungan pengguna. Hasil pengujian menjadi dasar untuk menentukan kelayakan sistem sebelum diterapkan secara penuh.

3.2.6. *Deployment & Docomentation*

Tahap terakhir mencakup penerapan sistem ke server produksi serta penyusunan dokumentasi teknis dan panduan penggunaan agar sistem dapat dikelola dan dikembangkan secara berkelanjutan. Proses *deployment* dilakukan dengan memperhatikan konfigurasi keamanan server dan kebutuhan kapasitas sistem. Dokumentasi disusun secara sistematis agar dapat digunakan sebagai acuan untuk proses pengembangan selanjutnya.

4. HASIL DAN PEMBAHASAN

4.1. *Penjelasan Hasil*

Proyek ini merupakan *Sistem Logging* Berbasis *Website* pada *Portal* Akademik yang dibangun menggunakan *PHP native* dan *MySQL* melalui *XAMPP*, dengan *integrasi API Fonnte* sebagai *autentikasi OTP via WhatsApp*. Sistem ini menerapkan *Role-Based Access Control (RBAC)* dengan tiga peran Utama Admin, Dosen, dan Mahasiswa di mana seluruh aktivitas pengguna seperti *login*, *logout*, serta kegiatan akademik tercatat otomatis dalam *log read-only* yang hanya dapat diakses Admin. Demi keamanan, sistem menggunakan *hashing* password *(bcrypt/Argon2)*, OTP sekali pakai, pembatasan tiga kali *login* gagal, serta fitur keamanan lanjutan seperti *Integrity Log berbasis HMAC*, *rate-limiting* login*, prepared statements* untuk mencegah *SQL injection*, dan *enkripsi* kolom sensitif menggunakan *AES*. Dengan demikian, sistem ini memastikan keamanan, transparansi, dan pengawasan aktivitas pengguna secara menyeluruh dalam portal akademik.

Hasil penelitian ini mendukung temuan [6] mengenai efektivitas *OTP* berbasis *WhatsApp* menggunakan layanan *Fonnte* yang memiliki respons cepat, serta sejalan dengan studi [2] yang menegaskan bahwa penggabungan *MFA* dan *RBAC* meningkatkan ketahanan sistem terhadap akses tidak sah. Integrasi *MFA* dan *RBAC* pada sistem ini diuji dalam berbagai skenario autentikasi untuk memastikan efektivitasnya terhadap serangan siber. Selain itu, penggunaan *logging* berbasis *read-only* memperkuat validitas data karena setiap aktivitas tersimpan tanpa dapat diubah kembali. Dengan menerapkan alur autentikasi yang konsisten dan terintegrasi melalui fitur *logging* dan *monitoring*, penelitian ini sekaligus menjawab permasalahan inkonsistensi *MFA* yang diidentifikasi dalam studi [4], sehingga model sistem yang dikembangkan dinilai lebih komprehensif, mudah dipahami pengguna, dan adaptif terhadap kebutuhan keamanan akademik.

4.2. *Hasail Perancangan Database*

Gambar 2 menunjukkan halaman *Daftar Akun* pada portal akademik yang digunakan untuk registrasi pengguna baru dengan mengisi Nama Lengkap, Nomor *WhatsApp* untuk verifikasi *OTP*, *Password*, Konfirmasi *Password*, serta memilih *Role* seperti Dosen atau Mahasiswa. Setelah data terisi, pengguna dapat menekan tombol *Daftar* atau memilih tautan *Login* jika sudah memiliki akun. Desain struktur *database* ini juga memperhatikan hubungan antar tabel agar proses penyimpanan dan pengambilan data dapat dilakukan dengan efisien. Tampilan yang sederhana dan modern ini memudahkan proses pendaftaran agar berlangsung cepat dan aman, ini ditunjukkan pada gambar 2.

p-ISSN : 2803-1507 e-ISSN : 2803-1531

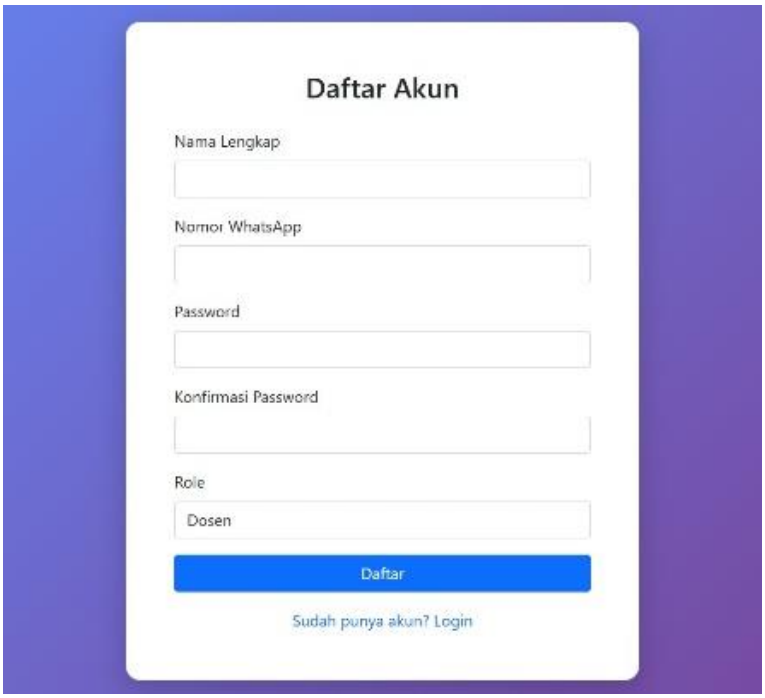
	Table	Action	Rows	Type	Collation	Size
☐	activity_logs	Browse Structure Search Insert Empty Drop	214	InnoDB	utf8mb4_general_ci	96.0 KiB
☐	jadwal_mengajar	Browse Structure Search Insert Empty Drop	0	InnoDB	utf8mb4_general_ci	48.0 KiB
☐	krs	Browse Structure Search Insert Empty Drop	2	InnoDB	utf8mb4_general_ci	48.0 KiB
☐	login_attempts_log	Browse Structure Search Insert Empty Drop	47	InnoDB	utf8mb4_general_ci	16.0 KiB
☐	mata_kuliah	Browse Structure Search Insert Empty Drop	8	InnoDB	utf8mb4_general_ci	32.0 KiB
☐	network_logs	Browse Structure Search Insert Empty Drop	0	InnoDB	utf8mb4_general_ci	64.0 KiB
☐	nilai	Browse Structure Search Insert Empty Drop	1	InnoDB	utf8mb4_general_ci	64.0 KiB
☐	otp_codes	Browse Structure Search Insert Empty Drop	35	InnoDB	utf8mb4_general_ci	32.0 KiB
☐	security_alerts	Browse Structure Search Insert Empty Drop	0	InnoDB	utf8mb4_general_ci	48.0 KiB
☐	threat_intelligence	Browse Structure Search Insert Empty Drop	4	InnoDB	utf8mb4_general_ci	32.0 KiB
☐	users	Browse Structure Search Insert Empty Drop	3	InnoDB	utf8mb4_general_ci	32.0 KiB
	11 tables	Sum	314	InnoDB	utf8mb4_general_ci	512.0

Add to Favorites

Gamabar 2. Rancang Database

4.3. *Form daftar*

Gambar 3 menunjukkan halaman *Daftar Akun* pada portal akademik yang berfungsi untuk membuat akun baru dengan mengisi Nama Lengkap, Nomor *WhatsApp* untuk verifikasi *OTP*, *Password*, *Konfirmasi Password*, serta memilih *Role* seperti Dosen atau Mahasiswa. Setelah data diisi, pengguna dapat menekan tombol *Daftar*, sedangkan tautan di bawahnya mengarahkan ke halaman *Login*. Elemen-elemen *form* ini dirancang agar responsif di berbagai ukuran layar, termasuk perangkat seluler. Tampilan yang sederhana dan responsif ini memudahkan proses *registrasi* agar lebih cepat dan aman.

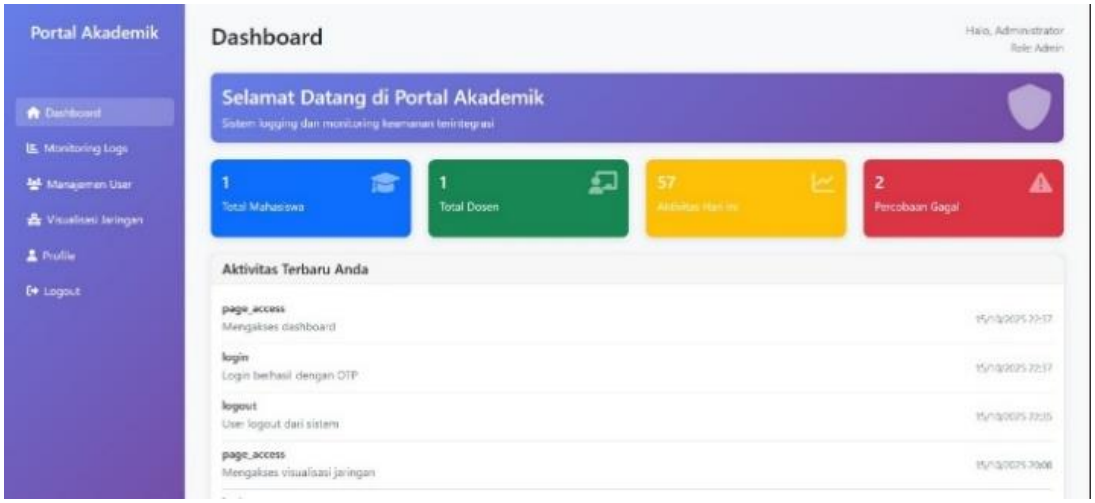


Gambar 3. Form Daftar

4.4. *Dashboard admin*

Gambar 4 menunjukkan *Dashboard* Admin pada portal akademik yang berperan dalam memantau aktivitas pengguna dan menjaga keamanan sistem. Tampilan ini menampilkan ringkasan data seperti Total Mahasiswa, Total Dosen, Aktivitas Hari Ini, serta Percobaan Login Gagal, disertai tabel Aktivitas Terbaru yang merekam aktivitas pengguna secara *real-time*. Setiap elemen pada *dashboard* dibuat dinamis agar data yang tampil selalu diperbarui tanpa perlu memuat ulang halaman. Desainnya yang sederhana dan informatif memudahkan admin dalam melakukan pengawasan sistem secara efisien.

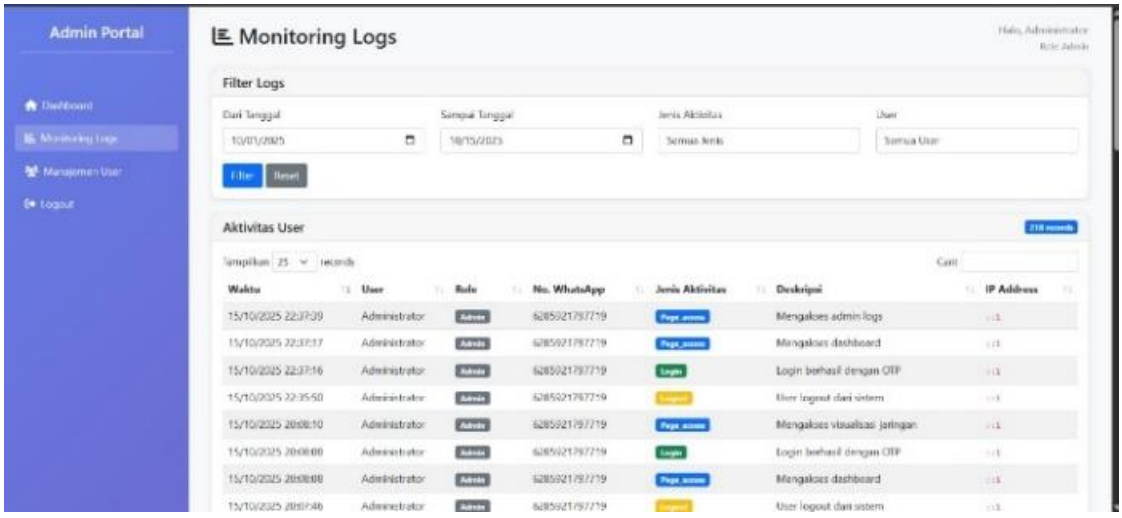
p-ISSN : 2803-1507 e-ISSN : 2803-1531



Gambar 4. Dashboard Admin

4.5. *Monitoring Log Aktivitas User didalam Website*

Gambar 5 menunjukkan halaman *Monitoring Logs* pada portal akademik yang berperan dalam memantau seluruh aktivitas pengguna. Admin dapat menggunakan fitur filter untuk menyeleksi data berdasarkan tanggal, jenis aktivitas, atau nama pengguna. Sistem pencatatan log ini menggunakan format waktu dan IP yang terstandarisasi agar memudahkan analisis keamanan. Tabel di bawahnya menampilkan informasi seperti waktu, nama, peran, nomor WhatsApp, jenis dan deskripsi aktivitas, serta alamat IP. Fitur ini membantu admin mengawasi aktivitas sistem dan mengidentifikasi potensi ancaman keamanan dengan lebih efektif.

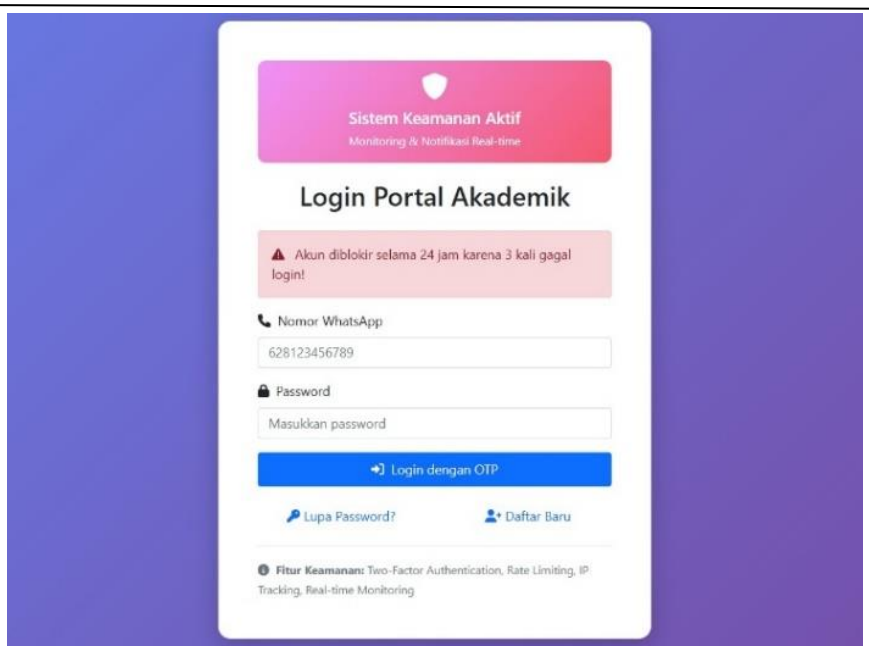


Gambar 5. Monitoring Log Aktivitas User didalam Website

4.6. *Halaman Login Portal Akademik dengan Fitur Pemblokiran Akun Otomatis*

Gambar 6 menunjukkan halaman Login Portal Akademik yang dilengkapi fitur keamanan pemblokiran akun otomatis setelah tiga kali percobaan *login* gagal. Pesan peringatan berwarna merah menandakan bahwa akun diblokir selama 24 jam. Formulir *login* meminta pengguna memasukkan Nomor WhatsApp dan Password, serta menyediakan opsi Lupa Password? dan Daftar. Fitur ini berfungsi mencegah serangan *brute-force* dan menjaga keamanan akses serta data pengguna.

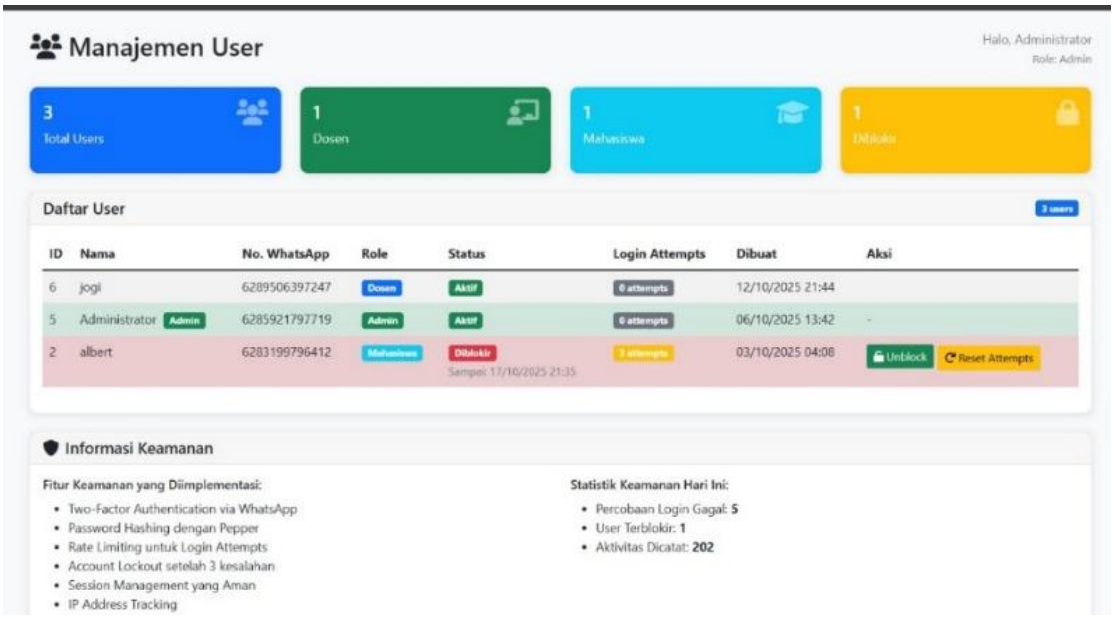
p-ISSN : 2803-1507 e-ISSN : 2803-1531



Gambar 6. Halaman Login Portal Akademik dengan Fitur Pemblokiran Akun Otomatis

4.7. *Manajemen User untuk Unblock*

Gambar 7 memperlihatkan tampilan halaman Manajemen User pada portal akademik yang digunakan admin untuk mengatur akun pengguna. Di bagian atas terdapat informasi ringkas mengenai jumlah Total *Users*, Dosen, Mahasiswa, serta akun yang Diblokir. Sementara itu, tabel di bawah menampilkan data pengguna meliputi nama, nomor WhatsApp, peran, status, jumlah percobaan login, dan waktu pembuatan akun. Admin dapat melakukan tindakan seperti membuka blokir *(Unblock)* atau mengatur ulang percobaan l*ogin (Reset Attempts)* guna mempermudah pengelolaan akun dan menjaga keamanan sistem.



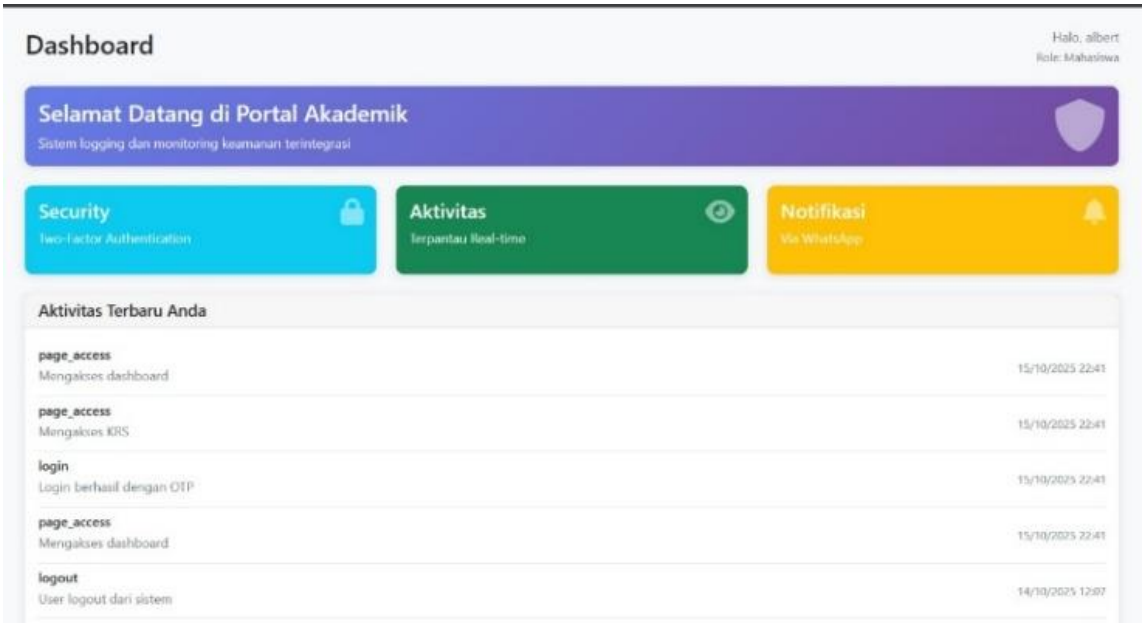
Gambar 7. Manajemen User untuk Unblock

4.8. *Dashboard Mahasiswa*

Gambar 8 menunjukkan *Dashboard* Mahasiswa pada portal akademik yang menampilkan fitur *Security*, Aktivitas, dan *Notifikasi*, serta daftar Aktivitas Terbaru seperti *login*, akses halaman, dan *logout*. Menu *Security* menampilkan status keamanan akun seperti aktivitas *login* terakhir dan peringatan potensi ancaman.

p-ISSN : 2803-1507 e-ISSN : 2803-1531

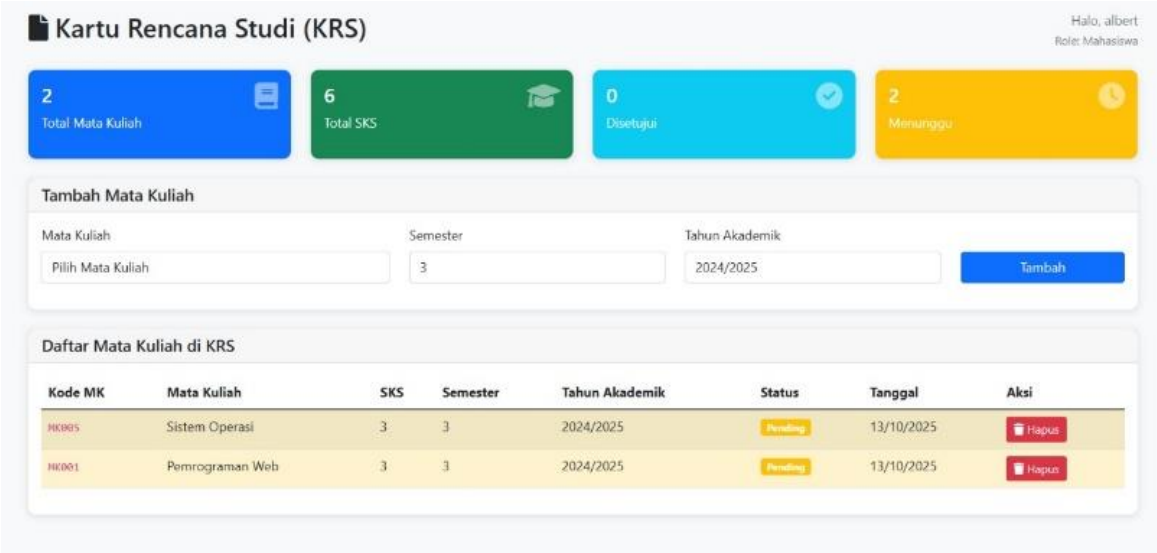
Selain itu, bagian *Notifikasi* memberikan pemberitahuan otomatis ketika sistem mendeteksi aktivitas yang tidak biasa. Tampilan ini membantu mahasiswa memantau aktivitas dan keamanan akun secara *real-time*.



Gambar 8. Dashboard Mahasiswa

4.9. *Fitur KRS*

Gambar 9 memperlihatkan halaman KRS pada portal akademik yang berfungsi bagi mahasiswa untuk menambahkan, mengatur mata kuliah, memantau total SKS, dan melihat status persetujuan dengan tampilan yang sederhana dan efisien. Setiap mata kuliah dapat dipilih berdasarkan program studi dan semester yang sedang dijalani. Sistem otomatis menghitung total SKS agar mahasiswa tidak melebihi batas maksimum yang diperbolehkan. Proses validasi dilakukan untuk memastikan setiap pengambilan mata kuliah sesuai dengan prasyarat yang telah ditetapkan.



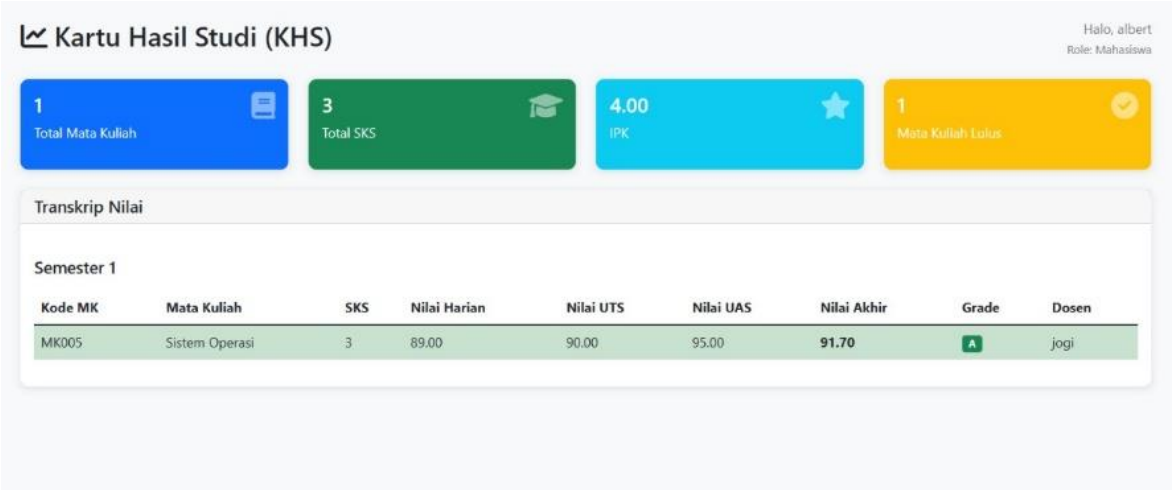
Gambar 9. Fitur KRS

4.10. *Fitur KHS*

Gambar 10 menampilkan halaman *Kartu Hasil Studi (KHS)* yang berisi hasil akademik mahasiswa pada mata kuliah Sistem Operasi dengan 3 SKS, memperoleh nilai akhir 91,70 *(grade A)*, serta menunjukkan ringkasan total mata kuliah, jumlah SKS, IPK, dan mata kuliah yang telah lulus. Data nilai ditampilkan secara otomatis

p-ISSN : 2803-1507 e-ISSN : 2803-1531

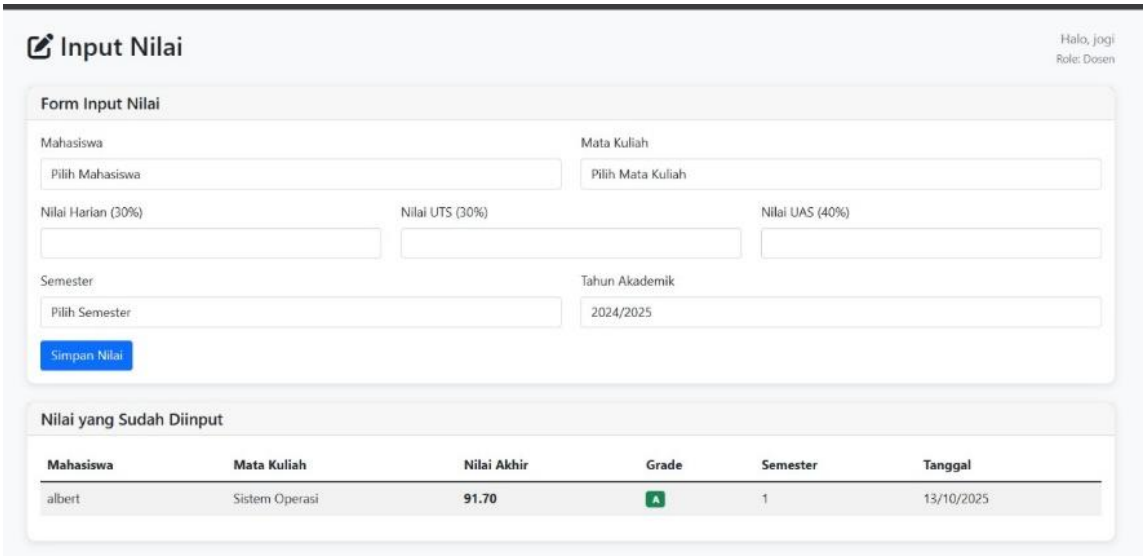
setelah dosen menyelesaikan proses input melalui sistem. Mahasiswa dapat melihat ringkasan hasil studi per semester beserta total SKS yang telah diselesaikan. Tampilan ini dirancang agar memudahkan mahasiswa dalam memantau perkembangan akademiknya dari waktu ke waktu.



Gambar 10. Fitur KHS

4.11. *Fitur Input Nilai Dosen*

Gambar 11 menunjukkan tampilan halaman Input Nilai pada portal akademik yang berfungsi bagi dosen untuk mengisi nilai mahasiswa. Formulir ini memuat data seperti nama mahasiswa, mata kuliah, nilai harian, nilai UTS, nilai UAS, semester, serta tahun akademik. Setiap data nilai yang disimpan akan dienkripsi dan diverifikasi untuk memastikan integritas informasi yang tersimpan di sistem. Setelah nilai disimpan, hasil input akan muncul di tabel bawah yang menampilkan nilai akhir, *grade*, semester, dan tanggal pengisian.

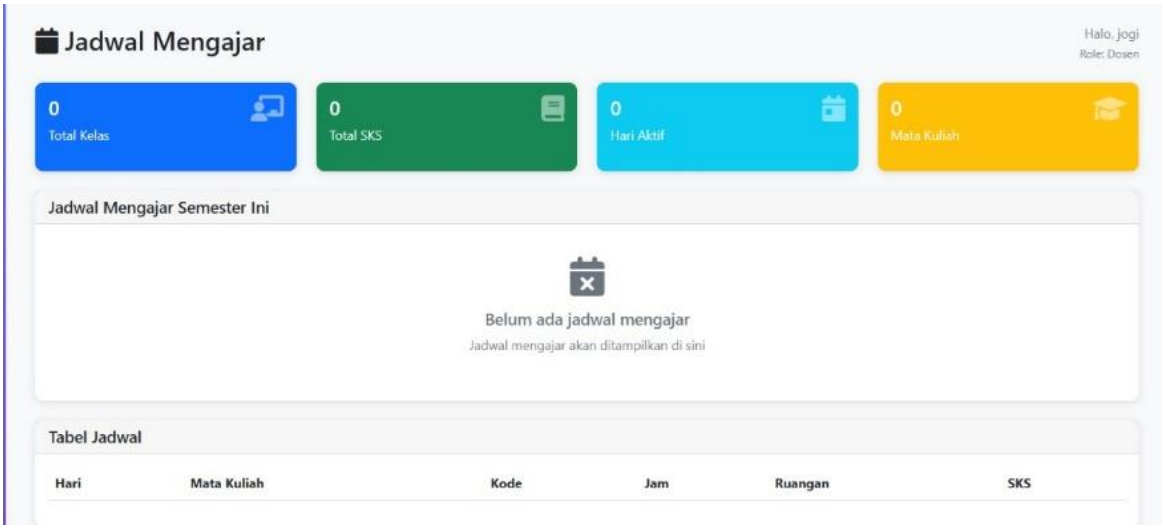


Gamabr 11. Fitur Input Nilai Dosen

4.12. *Fitur Jadwal Mengajar*

Gambar 12 menunjukkan halaman Jadwal Mengajar pada sistem akademik dosen yang menampilkan informasi total kelas, SKS, hari aktif, dan mata kuliah. Dosen dapat menambahkan jadwal mengajar berdasarkan hari, waktu, dan ruang kelas yang tersedia. Fitur ini juga terhubung dengan *dashboard* utama agar pembaruan jadwal langsung terlihat pada tampilan ringkasan kegiatan mengajar. Saat ini semua data masih bernilai nol dan tabel jadwal belum terisi karena belum ada jadwal mengajar yang dimasukkan untuk semester ini.

p-ISSN : 2803-1507 e-ISSN : 2803-1531

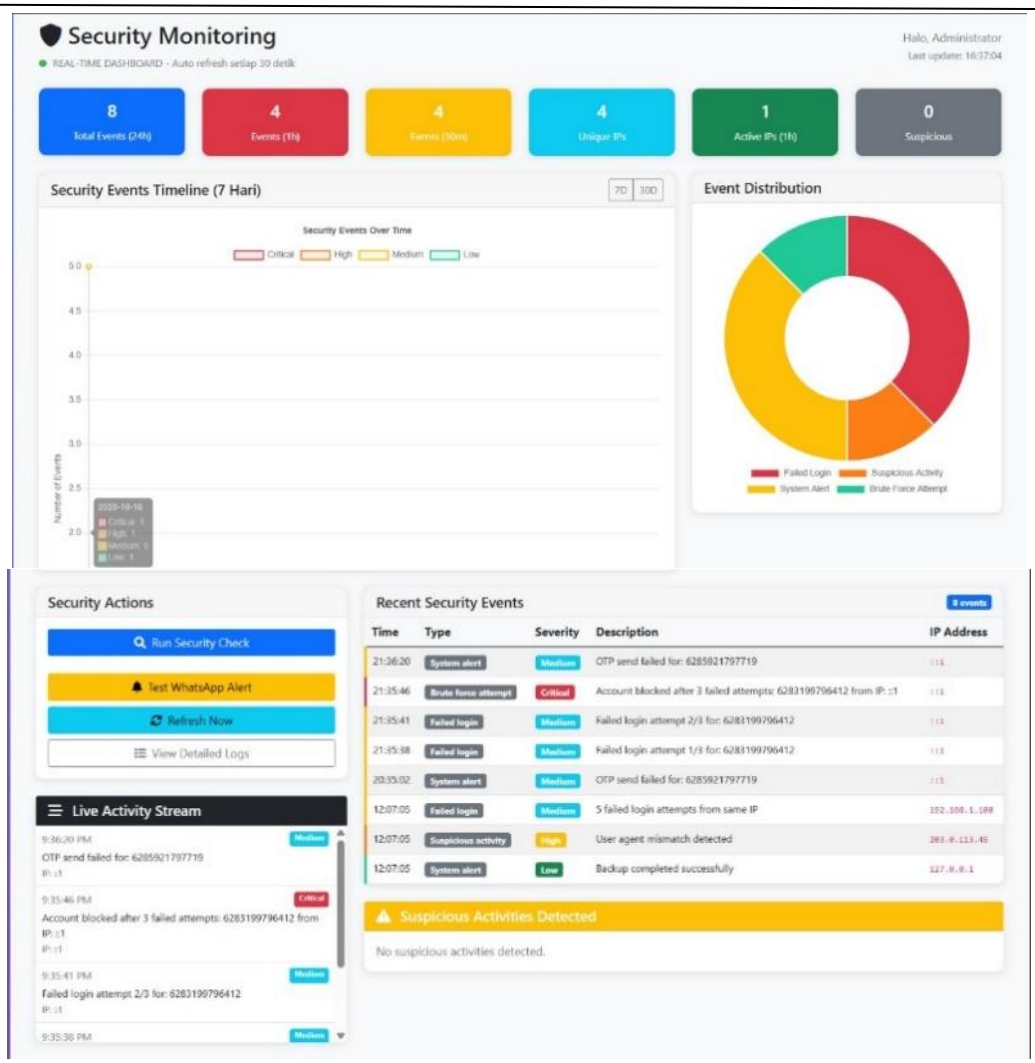


Gambar 12. Fitur Jadwal Mengajar

4.13. *Security Monitoring*

Dashboard *Security Monitoring* ini memberikan gambaran real-time mengenai status keamanan sistem. Dalam 24 jam terakhir tercatat 8 kejadian keamanan, dengan 4 di antaranya tergolong penting atau kritis. Sistem juga mendeteksi 4 alamat IP unik dengan 1 IP yang masih aktif, dan tidak ditemukan aktivitas mencurigakan. Grafik timeline menampilkan tren kejadian selama tujuh hari terakhir, sedangkan diagram distribusi memperlihatkan persentase berbagai jenis insiden seperti *failed login*, *suspicious activity*, *system alert*, dan *brute force attempt*. Gambar 13 memperlihatkan tampilan *Dashboard Security Monitoring* yang menampilkan data-data tersebut secara visual.

p-ISSN : 2803-1507 e-ISSN : 2803-1531



Gambar 13. Security Monitoring

Pada Gambar 14 dapat kita lihat pesan tersebut adalah notifikasi peringatan keamanan dengan *level medium* yang dikirim oleh sistem *monitoring*. Isinya mencakup waktu kejadian, alamat IP terkait, serta himbauan agar kode *OTP* yang hanya berlaku lima menit tidak dibagikan kepada siapa pun untuk menjaga keamanan. Notifikasi ini dikirim secara otomatis melalui *webhook* yang terhubung dengan layanan *Fonnte*. Informasi tersebut membantu *admin* untuk segera melakukan pemeriksaan terhadap aktivitas yang terdeteksi berisiko..



Gambar 14. Contoh *Security Alert* yang Dikirim Melalui *Webhook Fonnte*

5. DISKUSI

Hasil penelitian menunjukkan bahwa integrasi *Multi-Factor Authentication* (MFA) menggunakan OTP WhatsApp via Fonnte memberikan proses autentikasi yang stabil dan cepat dalam portal akademik. Temuan

p-ISSN : 2803-1507 e-ISSN : 2803-1531

ini memperkuat hasil studi [6] yang melaporkan bahwa OTP WhatsApp memiliki waktu respons yang konsisten untuk kebutuhan autentikasi sistem pendidikan digital. Penerapan MFA dalam penelitian ini juga memiliki kesesuaian dengan studi sebelumnya [2], [20], [21] yang menegaskan bahwa autentikasi berlapis mampu meningkatkan ketahanan sistem dari serangan *brute-force* dan akses tidak sah. Implementasi OTP melalui API lokal Fonnte menunjukkan bahwa layanan autentikasi berbasis pesan singkat tetap dapat bekerja optimal di lingkungan akademik dengan keterbatasan infrastruktur.

Penerapan *Role-Based Access Control* (RBAC) dalam portal akademik ini menunjukkan bahwa mekanisme otorisasi berbasis peran mampu menjaga keteraturan akses dan mencegah penyalahgunaan hak pengguna. Temuan tersebut memiliki relevansi kuat dengan penelitian [10], [2], [23] yang menunjukkan bagaimana RBAC meningkatkan efisiensi kontrol akses serta memperkuat perlindungan data sensitif. Integrasi RBAC yang berjalan berdampingan dengan MFA pada penelitian ini menantang sebagian temuan penelitian [4] yang melaporkan adanya inkonsistensi pengalaman pengguna ketika MFA tidak terhubung dengan sistem otorisasi secara langsung. Keberhasilan integrasi ini memberikan bukti bahwa sinkronisasi autentikasi dan otorisasi dapat dicapai melalui desain basis data dan struktur modul yang terkoordinasi.

Mekanisme *logging* berbasis *read-only* yang diterapkan pada portal akademik menunjukkan kemampuan mencatat aktivitas pengguna secara detail, termasuk waktu akses, IP address, aktivitas login, dan perubahan data. Hasil ini sejalan dengan penelitian [7], [16], [17] yang menekankan pentingnya pencatatan log terstruktur untuk mendeteksi pola anomali dan memperkuat keamanan jaringan. Fitur monitoring log pada penelitian ini memberikan visualisasi aktivitas pengguna secara real-time, yang memiliki kemiripan dengan pendekatan SIEM dalam penelitian [8], [9], [25]. Meskipun demikian, terdapat beberapa ketidakkonsistenan minor pada pencatatan aktivitas dari perangkat dengan kondisi jaringan tidak stabil, yang mencerminkan keterbatasan teknis serupa seperti dilaporkan pada studi IoT dan sistem monitoring terdistribusi [19].

Hasil monitoring keamanan melalui dashboard menunjukkan bahwa sistem mampu mengidentifikasi *failed login*, aktivitas mencurigakan, dan percobaan serangan ringan seperti *brute force attempt* dalam kurun waktu 24 jam. Kemampuan deteksi ini memperkuat temuan studi [23], [24] yang menjelaskan bahwa integrasi log, autentikasi, dan pemantauan dapat meningkatkan transparansi serta mempercepat respons terhadap ancaman. Dashboard interaktif yang menampilkan distribusi kategori insiden juga memberikan gambaran operasional yang relevan bagi administrator dalam mengevaluasi pola ancaman. Penelitian ini tetap memiliki keterbatasan pada cakupan pengujian yang belum melibatkan skala pengguna besar, sehingga performa deteksi ancaman pada kondisi beban tinggi belum sepenuhnya terukur.

6. KESIMPULAN DAN SARAN

6.1. *Kesimpulan*

Penelitian ini telah berhasil mengembangkan portal akademik berbasis web dengan sistem keamanan berlapis yang menggabungkan *Multi-Factor Authentication (OTP WhatsApp via Fonnte), Role-Based Access Control* (RBAC), dan mekanisme logging aktivitas pengguna. Implementasi berbagai fitur keamanan seperti enkripsi data, pembatasan percobaan login gagal, serta pemantauan real-time melalui dashboard keamanan terbukti mampu meningkatkan perlindungan data, transparansi, dan akuntabilitas pengguna. Berdasarkan hasil pengujian, sistem ini efektif dalam mencegah akses ilegal, menjaga kestabilan, serta mempermudah proses pengawasan dan pengelolaan data akademik secara efisien. Seluruh fitur dan mekanisme yang diterapkan dapat membantu administrator memantau aktivitas pengguna secara lebih terstruktur dan mengurangi risiko kesalahan operasional.

6.2. *Saran*

Ke depannya, sistem dapat dikembangkan lebih lanjut dengan menambahkan teknologi deteksi intrusi otomatis dan algoritma machine learning agar mampu mendeteksi potensi ancaman dengan lebih cepat dan akurat. Pengoptimalan dashboard interaktif dengan fitur analitik yang lebih mendalam juga perlu dilakukan untuk membantu admin dalam melakukan evaluasi keamanan dan pengambilan keputusan. Selain itu, disarankan agar dilakukan pengujian dengan skala pengguna yang lebih besar guna mengukur kinerja, keandalan, serta ketahanan sistem dalam berbagai kondisi operasional. Pemanfaatan umpan balik dari pengguna dan pengujian berulang dapat membantu memperbaiki kekurangan sistem serta menyesuaikan fitur sesuai kebutuhan akademik.

DAFTAR PUSTAKA

p-ISSN : 2803-1507 e-ISSN : 2803-1531

[1] R. Maududy and D. Rizal Nursyamsi, "Pengembangan Real-Time Monitoring dan Data Logging Berbasis Web Pada Proses Robot Painting untuk Meningkatkan Efisiensi Produksi," *Informatics Digit. Expert*, vol. 5, no. 2, pp. 89–94, 2024, doi: 10.36423/index.v5i1.1586.

[2] J. Madre, H. Yudi Sukmono, and S. Gunawan, "Perancangan Sistem Informasi Berbasis Website Sebagai Salah Satu Media Promosi Pada Perusahaan," *J. Ind. Manuf. Eng.*, vol. 5, no. 2, pp. 121–129, 2021, doi: 10.31289/jime.v5i2.5594.

[3] S. Ipnuwati, S. Mukodimah, and S. Alvionita, "Perancangan Sistem Informasi Layanan Dan Monitoring Pada Lintas Data Wifi Pt Tanggamus Mitra Media Berbasis Web Mobile," *J. Multimed. dan Android*, vol. 5, no. 2, pp. 1–18, 2024, doi: 10.30865/jurikom.v8i6.3631.

[4] R. Manalu, "Pengembangan Antarmuka Pengguna Website Sistem Otomasi Konfigurasi dan Monitoring Perangkat Jaringan Multivendor," *JIME*, vol. 11, no. 6, pp. 6093–6098, 2024, [Online]. Available: https://openlibrary.telkomuniversity.ac.id/pustaka/files/215551/jurnal_eproc/perancangan-dan-implementasi-sistem-otomasi-konfigurasi-dan-monitoring-perangkat-jaringan-multivendor-pada-arsitektur-microservice-capstone.pdf

[5] R. Kriswibowo, F. K. Suhada, and M. A. Riskyansah, "Pengembangan Sistem Informasi Logbook PKL Berbasis Web dengan Fitur Real-Time Monitoring," *J. Sist. Inf.*, vol. 3, no. 7, pp. 478–489, 2025, doi: 10.35134/komtekinfo.v11i4.595.

[6] M. Somantri, M. Arfan, and O. S. Siregar, "Adaptasi Human Machine Interface (HMI) dalam Monitoring dan Kendali Kualitas Air pada Tambak Udang," *J. Sist. Inf. Bisnis*, vol. 12, no. 2, pp. 73–80, 2022, doi: 10.21456/vol12iss2pp73-80.

[7] D. B. Santoso and Y. Wahyuni, "Sestem Log Web Server Sebagai Pendeteksi Anomali Menggunakan Isolation Forest," *J. Apl. Bisnis dan Komput.*, vol. 4, no. 3, pp. 2807–5986, 2024, doi: 10.33751/jubikom.v4i3.10941.

[8] M. R. Kamal and M. A. Setiawan, "Deteksi Anomali dengan Security Information and Event Management (SIEM) Splunk pada Jaringan UII," *Automata*, vol. 2, no. 2, pp. 1–6, 2021, [Online]. Available: https://journal.uii.ac.id/automata/article/view/19522

[9] Issenoro, H. Trisnawati, S. O. Tarigan, N. M. Faizah, and Veranita, "Perancangan dan Pengembangan Aplikasi Deteksi Anomali pada Jaringan Internet Gedung Disaster Recovery Center Badan Diklat Kejaksaan RI dengan Implementasi Sistem Manajemen Informasi dan Keamanan (SIEM) Berbasis Web," *J. Ilmu Komput. dan Teknol. Inf.*, vol. 2, no. 1, pp. 12–21, 2025, doi: 10.35870/jikti.v2i1.1341.

[10] M Sahyudi and Erliyan Redy Susanto, "Analisis Implementasi Sistem Keamanan Basis Data Berbasis Role-Based Access Control (RBAC) pada Aplikasi Enterprise Resource Planning," *SATESI J. Sains Teknol. dan Sist. Inf.*, vol. 5, no. 1, pp. 105–116, 2025, doi: 10.54259/satesi.v5i1.3997.

[11] Mr. Pradeep V, Vaishali, Vandan M Shetty, and Varsha A M, "A Review Paper on Network Security and Cryptography," *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 2, no. 1, pp. 133–138, 2022, doi: 10.48175/ijarsct-7081.

[12] D. Agnew, S. Boamah, A. Bretas, and J. McNair, "Network Security Challenges and Countermeasures for Software-Defined Smart Grids: A Survey," *Smart Cities*, vol. 7, no. 4, pp. 2131–2181, 2024, doi: 10.3390/smartcities7040085.

[13] O. El Gharbaoui, I. Kiyadi, and H. El Boukhari, "Evaluating AI and ML in Network Security: A Comprehensive Literature Review," *Procedia Comput. Sci.*, vol. 251, pp. 727–733, 2024, doi: 10.1016/j.procs.2024.11.176.

[14] N. Nikhlis, M. Jamal, and U. Ghofur, "Deteksi Dini Pencurian Data pada Perangkat Seluler Menggunakan Machine Learning," *J. Ilm. Sist. Inf.*, vol. 4, no. 2, pp. 110–129, May 2025, doi: 10.51903/fz0xzt26.

[15] N. Qosidah, "Systematic Literature Review: Energy Metrics, Trade-Offs, and Best Practices in Green IT and Green Software," *J. Ilm. Sist. Inf.*, vol. 4, no. 1, pp. 58–69, Jan. 2025, doi: 10.51903/zezhdt51.

p-ISSN : 2803-1507 e-ISSN : 2803-1531

[16] S. E. Nouma and A. A. Yavuz, "Lightweight and High-Throughput Secure Logging for Internet of Things and Cold Cloud Continuum," *arXiv CoRR*, vol. 1, no. 1, p. 1, 2025, doi: 10.48550/arXiv.2506.08781.

[17] S. C. Kusuma, Y. F. Soleman, B. Berlinton, Jamaludin, and S. Karya, "A SIEM-Driven Solution for Cyber Attack Detection in Educational Websites: Implementing Threat Log Filtering for Enhanced Security," *JUPITER J. Comput. Inf. Technol.*, vol. 6, no. 1, pp. 10–25, 2025, doi: 10.53990/jupiter.v6i1.419.

[18] A. S. Hakim, P. J. Mustaqim, and A. Naufal, "Peran Pendidikan Digital dalam Melindungi Privasi Pengguna dan Mencegah Dampak Sosial," *J. Ilm. Sist. Inf.*, vol. 4, no. 2, pp. 162–174, May 2025, doi: 10.51903/k9cvkc90.

[19] T. Ardiyanto, C. Supriadi, and Priyadi, "Rancang Bangun Sistem Monitoring Deteksi Dini Kebakaran Ruang Server Berbasis IoT," *J. Ilm. Sist. Inf.*, vol. 3, no. 3, pp. 35–45, Jan. 2024, doi: 10.51903/432zjf74.

[20] H. Haeruddin, S. E. Prasetyo, and A. Mindy, "Implementasi Multi-Factor Authentication untuk Optimalisasi Keamanan Akses Data Di PT.ABC," *J. Manaj. Inform.*, vol. 15, no. 1, p. 85096, 2025, doi: 10.34010/5rdjmw37.

[21] I. Melyana, M. S. Darmawan, S. Syukur, M. I. A. Syah, and F. Purwani, "Algoritma Autentikasi Multi Factor Sebagai Solusi Untuk Meningkatkan Keamanan Sistem Pembayaran E-Commerce," *Digit. Transform. Technol.*, vol. 4, no. 2, pp. 984–989, 2024, doi: 10.47709/digitech.v4i2.4969.

[22] S. U. Anggono and S. Supriyanto, "Peluang dan Tantangan Sistem Pelatihan Berbasis AI dalam Meningkatkan Keterampilan Tenaga Kerja di Era Digital," *J. Ilm. Sist. Inf.*, vol. 4, no. 2, pp. 224–231, May 2025, doi: 10.51903/6mbmzk12.

[23] K. A. Nugroho, "Deteksi Anomali Trafik Jaringan dan Aktivitas Pengguna Menggunakan Isolation Forest untuk Meningkatkan Keamanan Jaringan," *J. Pendidik. dan Teknol. Indones.*, vol. 5, no. 5, pp. 1365–1376, 2025, doi: 10.52436/1.jpti.790.

[24] M. F. Hidayat *et al.*, "Desain dan Implementasi Sistem Penilaian Akademik untuk Perlindungan Data Pribadi," *JATI (Jurnal Mhs. Tek. Inform.*, vol. 9, no. 4, pp. 6812–6817, 2025, doi: 10.36040/jati.v9i4.14190.

[25] M. Y. Ishaq and F. Firmansyah, "Implementasi Sistem Monitoring Menggunakan Zabbix dan Notifikasi Realtime Telegram," *J. Insa. J. Inf. Syst. Manag. Innov.*, vol. 3, no. 2, pp. 72–77, 2023, doi: 10.31294/jinsan.v3i2.2432.