Jurnal Ilmu Komputer Aceh

E-ISSN: 2986-7797
Edisi : Volume 3 Nomor 1 | Februari 2026

Available online at https://jurnal.fikompublisher.com/ilka

Penerapan Role-Based Access Control (RBAC) untuk Mengelola Hak Akses pada Sistem Informasi Sekolah Taman Kanak-Kanak (TK) Berbasis Multiuser

Sri Ramadhani[1], Dedy Armiady[2], Riyadhul Fajri[3]
[1,2,3] Universitas Almuslim Bireuen

ARTICLE INFO

Article history:

Received : 24 Februari 2026
Revised : 25 Februari 2026
Accepted : 02 Maret 2026

Keywords:
Role-Based Access Control, RBAC, Multiuser Information System, Kindergarten, Access Rights

ABSTRACT

[Implementation of Role-Based Access Control (RBAC) to Manage Access Rights in a Multi-User Kindergarten (TK) School Information System] This study aims to design and implement a multiuser information system based on Role-Based Access Control (RBAC) in a kindergarten (TK) environment to manage user access rights in a structured and secure manner. In multiuser-based school information systems, improper access control can lead to unauthorized data access, role conflicts, and security vulnerabilities. To address this issue, this research applies RBAC as the main authorization mechanism, where access rights are granted based on predefined user roles. The system is developed using a software engineering approach with a descriptive methodology, following stages of requirements analysis, system design, implementation, and testing. Three primary roles are defined in the system: Super Admin, School Admin, and Operator, each with different access privileges. The system is implemented using PHP with the CodeIgniter framework and MySQL as the database management system. To enhance responsiveness and accuracy in access control enforcement, a real-time mechanism using Pusher.js is integrated to synchronize access right changes without requiring manual page refresh. System testing is conducted using black-box testing to verify access restrictions, menu visibility, and data isolation between schools. The results show that the RBAC mechanism functions effectively in restricting access according to user roles, preventing unauthorized actions, and ensuring data separation across institutions. This research demonstrates that RBAC can be reliably applied as a foundational access control model for multiuser school information systems, particularly in early childhood education environments, and can be further developed for real-world implementation.

Kata kunci: Role-Based Access Control, RBAC, Sistem Informasi Multiuser, Taman Kanak-Kanak, Hak Akses

Corresponding Author:
Sri Ramadhani
Universitas Almuslim
Email:
sriramadani596@gmail.com

ABSTRAK

Penelitian ini bertujuan untuk merancang dan mengimplementasikan sistem informasi berbasis multiuser dengan menerapkan metode Role-Based Access Control (RBAC) pada lingkungan sekolah Taman Kanak-Kanak (TK) guna mengelola hak akses pengguna secara terstruktur dan aman. Pada sistem informasi sekolah yang melibatkan banyak pengguna, pengelolaan hak akses yang tidak terkontrol dapat menimbulkan risiko seperti akses data tidak sah, konflik peran, dan lemahnya keamanan sistem. Oleh karena itu, penelitian ini menerapkan RBAC sebagai mekanisme utama pengendalian akses, di mana hak akses

ditentukan berdasarkan peran pengguna. Metode penelitian yang digunakan adalah rekayasa perangkat lunak dengan pendekatan deskriptif, yang meliputi tahapan analisis kebutuhan, perancangan sistem, implementasi, dan pengujian. Sistem ini memiliki tiga peran utama, yaitu Super Admin, Admin Sekolah, dan Operator, dengan hak akses yang berbeda-beda sesuai fungsinya. Implementasi sistem dilakukan menggunakan bahasa pemrograman PHP dengan framework CodeIgniter dan basis data MySQL. Untuk meningkatkan efektivitas pengujian dan responsivitas sistem, mekanisme real-time menggunakan Pusher.js diterapkan guna memperbarui perubahan hak akses secara langsung tanpa memuat ulang halaman. Pengujian sistem dilakukan menggunakan metode black-box testing. Hasil pengujian menunjukkan bahwa penerapan RBAC mampu membatasi akses pengguna sesuai perannya, mencegah akses tidak berizin, serta menjaga pemisahan data antar sekolah. Penelitian ini membuktikan bahwa RBAC efektif digunakan sebagai model dasar pengelolaan hak akses pada sistem informasi sekolah berbasis multiuser, khususnya pada jenjang pendidikan anak usia dini.

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah mendorong transformasi digital pada berbagai sektor, termasuk dunia pendidikan. Implementasi sistem informasi berbasis web telah menjadi kebutuhan penting dalam mendukung efektivitas pengelolaan data dan layanan administrasi [1]. Namun, penerapan sistem informasi yang terstruktur dan aman pada jenjang pendidikan anak usia dini seperti Taman Kanak-kanak (TK) masih relatif terbatas dibandingkan pendidikan menengah dan perguruan tinggi. Padahal, sistem yang digunakan secara multiuser tetap memerlukan pengendalian akses yang jelas dan terukur. Dalam lingkungan sistem informasi multiuser, permasalahan utama yang sering muncul adalah lemahnya pengaturan hak akses. Sistem tanpa pembatasan peran yang tegas berpotensi menimbulkan konflik kepentingan, akses tidak sah, serta pelanggaran prinsip least privilege. Studi mengenai keamanan komputasi awan menunjukkan bahwa kontrol akses merupakan komponen kritis dalam menjaga keamanan sistem terdistribusi [2], [3]. Selain itu, pedoman NIST mengenai keamanan dan privasi pada cloud computing juga menegaskan pentingnya penerapan mekanisme kontrol akses yang sistematis untuk melindungi data pengguna[3].

Model kontrol akses telah mengalami perkembangan signifikan. Pendekatan Risk-Based Access Control (RAdAC) mempertimbangkan faktor risiko dalam pengambilan keputusan akses[4]. Attribute-Based Access Control (ABAC) memberikan fleksibilitas dengan mendasarkan keputusan akses pada atribut pengguna dan lingkungan [5]. Model Usage Control (UCONABC) memperluas konsep kontrol akses dengan menambahkan aspek kontrol berkelanjutan selama proses penggunaan sumber daya [6]. Selain itu, model hybrid seperti HYARBAC dikembangkan untuk menggabungkan keunggulan RBAC dan atribut guna meningkatkan adaptivitas kebijakan keamanan [7]. Meskipun berbagai model telah dikembangkan, Role-Based Access Control (RBAC) tetap menjadi pendekatan yang paling banyak diadopsi karena kesederhanaan struktur dan kemudahan implementasinya. RBAC mendasarkan hak akses pada peran yang dimiliki pengguna, sehingga mempermudah pengelolaan otorisasi dalam sistem berskala organisasi. Implementasi RBAC telah diterapkan pada berbagai domain, termasuk sistem pendidikan berbasis biometrik [8], sistem log berbasis blockchain [9], arsitektur komunikasi aman [10], sistem ERP [11], sistem perpustakaan digital [10], aplikasi e-raport [12], supply chain berbasis cloud [13], koperasi mobile [14], serta sistem otorisasi terpusat [15]. Pada platform e-learning multi-role, RBAC terbukti mampu mengatur distribusi hak akses secara lebih terstruktur [16].

Namun demikian, kelemahan kontrol akses masih menjadi salah satu kerentanan utama pada aplikasi web. OWASP mengidentifikasi broken access control sebagai risiko keamanan paling dominan pada sistem akademik terintegrasi [17]. Analisis keamanan e-learning berbasis

OWASP menunjukkan bahwa ketidaktepatan konfigurasi hak akses dapat membuka celah eksploitasi [18]. Standar ISO/IEC 27001 juga menekankan pentingnya manajemen kontrol akses sebagai bagian dari sistem manajemen keamanan informasi [19], [20]. Studi keamanan situs perguruan tinggi menunjukkan bahwa lemahnya mekanisme otorisasi masih menjadi sumber kerentanan signifikan [4], sementara penelitian lain menegaskan bahwa sistem informasi tanpa pengaturan akses yang baik berpotensi meningkatkan risiko kebocoran data [21].Dalam konteks pendidikan anak usia dini, kebutuhan kontrol akses memiliki karakteristik tersendiri. Struktur organisasi relatif sederhana, tetapi tetap membutuhkan pembatasan akses yang jelas, terutama ketika sistem dirancang sebagai portal induk yang digunakan oleh lebih dari satu sekolah. Tanpa pemisahan hak akses dan data yang ketat, risiko pelanggaran privasi dapat meningkat [22]. Oleh karena itu, penerapan RBAC dalam konteks ini menjadi relevan sebagai solusi yang terstruktur dan efisien.

Penelitian ini bertujuan untuk membangun sebuah portal induk sistem informasi berbasis web yang mensimulasikan penerapan RBAC dalam lingkungan pendidikan anak usia dini berbasis multiuser. Sistem terdiri dari tiga peran utama, yaitu super admin, admin sekolah, dan operator, dengan struktur hierarkis yang terkontrol. Seluruh proses registrasi dilakukan secara terpusat, di mana super admin memiliki kewenangan menambahkan admin sekolah, dan admin sekolah hanya dapat menambahkan operator di bawahnya. Mekanisme ini dirancang untuk memastikan distribusi hak akses berjalan secara terstruktur dan meminimalkan potensi penyalahgunaan.Untuk meningkatkan konsistensi dan responsivitas sistem, penelitian ini juga mengintegrasikan mekanisme pembaruan hak akses secara real-time menggunakan teknologi komunikasi berbasis event. Pendekatan ini memungkinkan perubahan hak akses diterapkan secara langsung tanpa perlu melakukan penyegaran halaman secara manual, sehingga meningkatkan efektivitas pengendalian sistem [9], [10].Berbeda dengan penelitian sebelumnya yang umumnya berfokus pada implementasi RBAC pada sistem enterprise, cloud, atau pendidikan tingkat lanjut, penelitian ini secara khusus menitikberatkan pada simulasi teknis penerapan RBAC pada sistem informasi TK berbasis multiuser. Sistem dibangun menggunakan data dummy dan diuji melalui simulasi lokal tanpa melibatkan institusi sekolah secara langsung.Dengan pendekatan tersebut, penelitian ini diharapkan dapat memberikan kontribusi berupa rancangan arsitektur RBAC yang terstruktur, terkontrol, dan adaptif sebagai fondasi awal pengembangan sistem informasi pendidikan anak usia dini yang aman dan sesuai dengan prinsip keamanan modern.

METODE

A. Pendekatan Penelitian

Penelitian ini menggunakan metode rekayasa perangkat lunak (software engineering approach) dengan pendekatan deskriptif-eksperimental. Pendekatan ini dipilih karena penelitian berfokus pada perancangan, pembangunan, serta pengujian prototipe sistem sebagai media simulasi penerapan Role-Based Access Control (RBAC) dalam lingkungan multiuser, bukan pada implementasi operasional di institusi pendidikan nyata.Model pengembangan sistem dilakukan melalui tahapan terstruktur yang meliputi:

1. Analisis kebutuhan
2. Perancangan sistem
3. Implementasi
4. Pengujian dan validasi

Pendekatan ini selaras dengan penelitian implementatif pada sistem keamanan informasi yang menekankan validasi fungsional terhadap mekanisme kontrol akses [23], [2], [10].

B. Tahap Analisis Kebutuhan

Analisis kebutuhan dilakukan untuk mengidentifikasi:

1. Struktur Pengguna

Sistem dirancang dengan tiga peran utama:

1. Super Admin
2. Admin Sekolah
3. Operator

Struktur ini ditentukan berdasarkan prinsip least privilege dan pemodelan RBAC klasik yang memisahkan peran dan hak akses secara eksplisit [5], [8].

2. Kebutuhan Fungsional

1. Autentikasi berbasis username dan password
2. Pembatasan akses menu berdasarkan peran
3. Pembatasan data antar sekolah
4. Registrasi akun terpusat
5. Pembaruan hak akses secara real-time
6.

3. Kebutuhan Non-Fungsional

1. Sistem berbasis web
2. Mendukung multiuser
3. Responsif terhadap perubahan hak akses
4. Aman dari akses lintas peran

C. Perancangan Arsitektur Sistem

Arsitektur sistem menggunakan model client–server dengan komponen:

1. Web Client (Browser)
2. Application Server (PHP – CodeIgniter)
3. Database Server (MySQL)
4. Real-Time Engine (Pusher.js)

Alur Sistem:

1. Pengguna melakukan login.
2. Sistem memverifikasi kredensial.
3. Role pengguna diambil dari tabel users.
4. Sistem memvalidasi akses terhadap tabel role_permission.
5. Jika valid → akses diberikan.
6. Jika tidak valid → sistem mengembalikan HTTP 403.

Pendekatan ini mengikuti konsep validasi berbasis role sebagaimana direkomendasikan dalam implementasi RBAC modern [7], [10].

D. Desain Model RBAC

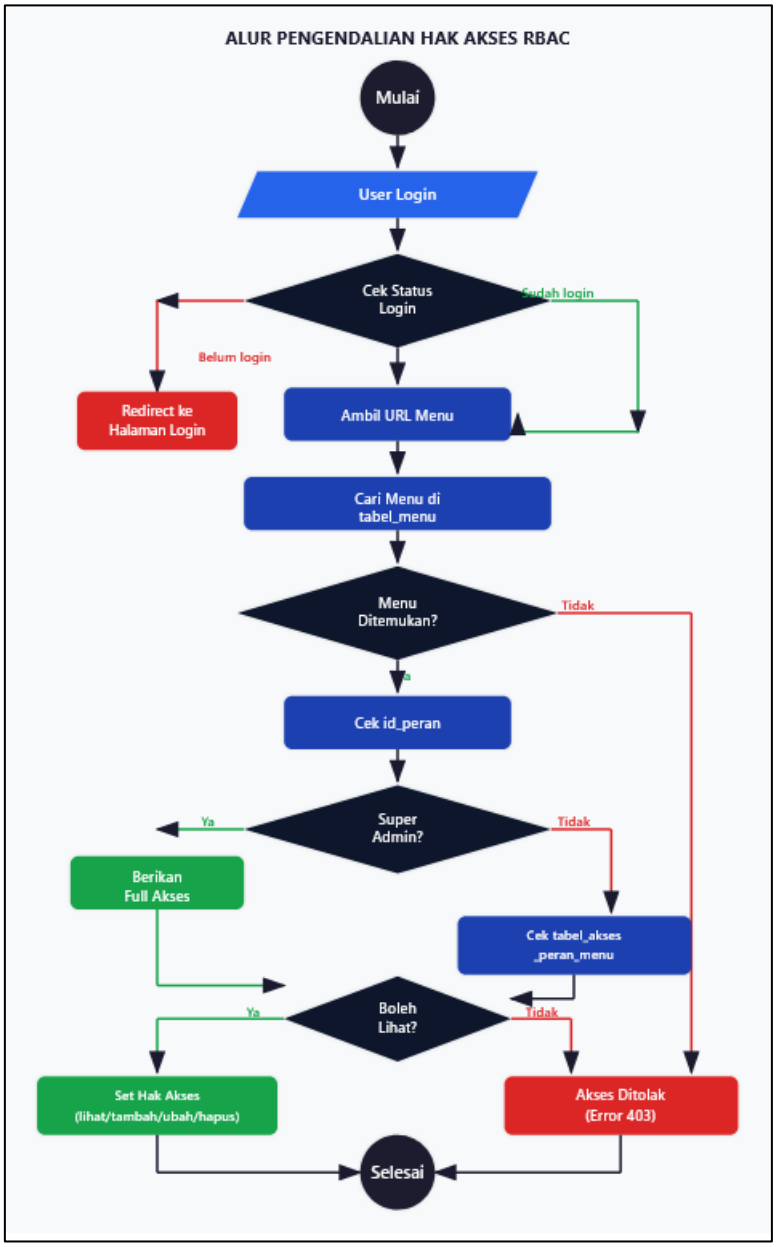
Model RBAC dalam penelitian ini terdiri dari empat entitas utama:

1. Users
2. Roles
3. Permissions
4. Menus

Relasi Model:

1. 1 User → 1 Role
2. 1 Role → Many Permissions
3. 1 Permission → 1 Menu

Validasi akses dilakukan pada setiap request URL dengan mencocokkan role pengguna terhadap tabel menu dan tabel akses peran menu.



Gambar 1. Alur Pengendalian Hak Akses Menu

Tindakan yang divalidasi meliputi:

1. View
2. Create
3. Update
4. Delete

Model ini mengacu pada standar implementasi RBAC yang terstruktur dan modular [22], [6].

E. Mekanisme Registrasi Terpusat

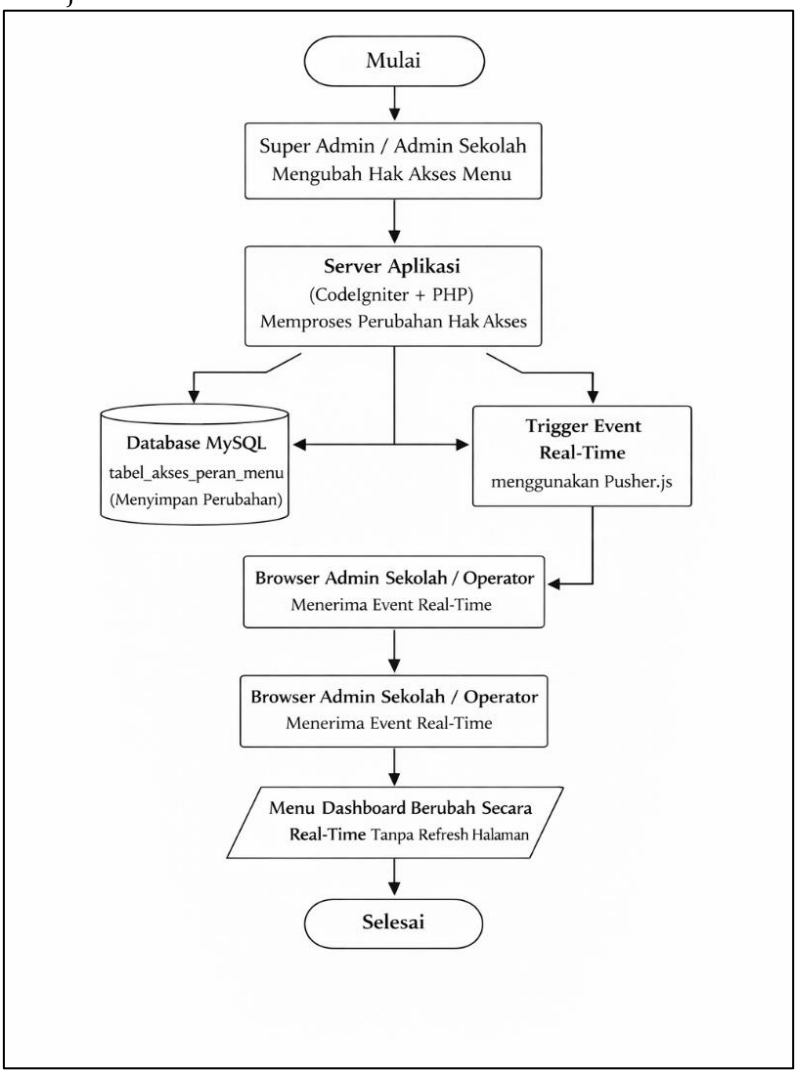
Sistem menerapkan model **single-gate registration**:

1. Tidak tersedia registrasi publik.
2. Super Admin membuat akun Admin Sekolah.
3. Admin Sekolah membuat akun Operator.
4. Operator tidak dapat membuat akun baru.

Model ini dirancang untuk mencegah eskalasi hak akses yang tidak sah serta menjaga kontrol distribusi akun secara hierarkis.

F. Integrasi Mekanisme Real-Time (Pusher.js)

Untuk meningkatkan dinamika kontrol akses, sistem mengintegrasikan teknologi real-time menggunakan Pusher.js.



Gambar 2 Ilustrasi Mekanisme Sinkronisasi Hak Akses Real-Time Menggunakan Pusher.js

Integrasi ini memungkinkan pengujian kontrol akses secara dinamis dan mendukung konsistensi kebijakan dalam lingkungan multiuser [8], [24].

G. Desain Basis Data

Basis data dirancang menggunakan sistem manajemen basis data MySQL dengan total 13 tabel utama yang mendukung mekanisme kontrol akses dan operasional sistem.

Tabel inti yang mendukung implementasi RBAC meliputi:

1. tabel_pengguna
2. tabel_peran
3. tabel_akses_peran_menu
4. tabel_menu
5. tb_sekolah

Relasi utama dalam mekanisme kontrol akses adalah:

1. Setiap pengguna terhubung dengan satu peran melalui foreign key.
2. Setiap peran memiliki relasi many-to-many terhadap menu melalui tabel tabel_akses_peran_menu.
3. Setiap pengguna terikat pada satu entitas sekolah untuk mencegah akses lintas sekolah.

Struktur relasional ini dirancang untuk menjaga integritas data serta memastikan bahwa validasi akses dilakukan secara konsisten berdasarkan relasi antar tabel.

H. Metode Pengujian dan Validasi
Pengujian dilakukan menggunakan metode:
1. Black-Box Testing
Mengukur kesesuaian fungsi sistem terhadap spesifikasi.

2. Skenario Pengujian

Tabel 1. Skenario Pengujian

No	Skenario	Expected Result
1	Operator akses menu Admin	Ditolak (403)
2	Admin akses menu Super Admin	Ditolak
3	Perubahan role	Menu berubah real-time
4	Akses data sekolah lain	Ditolak

3. Validasi Real-Time
1. Uji simultan multiuser
2. Uji perubahan hak akses tanpa reload
3. Monitoring response event

HASIL DAN PEMBAHASAN

Hasil penelitian diperoleh melalui proses perancangan, implementasi, dan pengujian sistem informasi sekolah Taman Kanak-Kanak (TK) berbasis multiuser yang menerapkan mekanisme Role-Based Access Control (RBAC). Sistem dirancang sebagai portal induk simulatif yang digunakan oleh beberapa sekolah dalam satu lingkungan aplikasi, dengan tujuan utama untuk menguji efektivitas pengelolaan hak akses pengguna berdasarkan peran. Pada tahap perancangan, struktur RBAC dibangun dengan mendefinisikan tiga peran utama, yaitu Super Admin, Admin Sekolah, dan Operator, yang masing-masing memiliki ruang lingkup akses berbeda terhadap menu sistem maupun data sekolah [25], [8].

A. Hasil Implementasi Sistem
Hasil implementasi menunjukkan bahwa mekanisme pembatasan akses berjalan sesuai rancangan. Super Admin memiliki akses penuh terhadap seluruh data dan pengaturan sistem, termasuk pengelolaan sekolah, pengguna, dan hak akses menu. Admin Sekolah hanya dapat mengelola data dan pengguna dalam lingkup sekolahnya, sedangkan Operator memiliki akses sangat terbatas sesuai izin yang diberikan. Temuan ini mendukung penelitian terdahulu yang menyatakan bahwa pemetaan peran yang jelas merupakan kunci keberhasilan penerapan RBAC [22], [24].

Gambar 3. Tampilan Dashboard Admin Sekolah dengan Menu Sesuai Hak Akses

Gambar 4. Tampilan Dashboard Operator dengan Menu Terbatas

B. Hasil Pengujian Black-Box Testing

Pengujian dilakukan menggunakan metode black-box testing terhadap seluruh fitur inti sistem RBAC. Tabel 1 menyajikan rekapitulasi hasil pengujian yang mencakup autentikasi login, manajemen akses menu, validasi hak akses, pembatasan data antar sekolah, kontrol tombol CRUD, serta mekanisme real-time menggunakan Pusher.js.

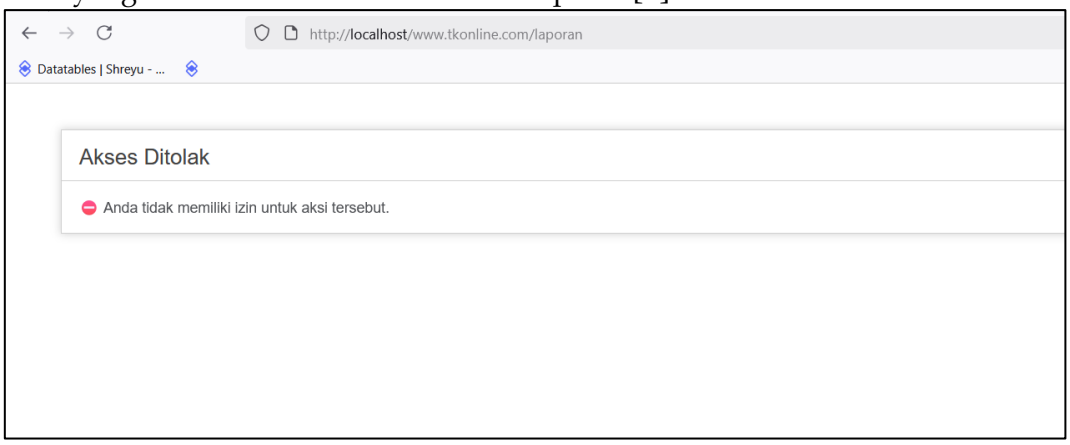
Tabel 2. Rekapitulasi Hasil Pengujian Black-Box Testing Sistem RBAC

No	Skenario Pengujian	Output yang Diharapkan	Status	Status
1	Login berhasil dengan kredensial valid, diarahkan ke dashboard sesuai role	Redirect ke dashboard sesuai role	Sesuai	Lulus
2	Login gagal dengan email atau password salah	Muncul pesan error autentikasi	Sesuai	Lulus
3	Operator membuka URL menu Admin secara langsung	Ditolak, muncul pesan error 403	Sesuai	Lulus
4	Admin Sekolah mengakses URL menu Super Admin	Muncul tampilan "Akses Ditolak"	Sesuai	Lulus
5	Tombol Tambah/Hapus tidak muncul jika tidak punya izin CRUD	Tombol tidak tampil di antarmuka	Sesuai	Lulus
6	Admin Sekolah hanya melihat data sekolahnya sendiri (siswa & guru)	Data sekolah lain tidak tampil	Sesuai	Lulus
7	Super Admin melihat data seluruh sekolah	Semua data dari semua sekolah tampil	Sesuai	Lulus
8	Perubahan hak akses diterapkan real-time via Pusher.js tanpa reload	Menu langsung berubah di sisi pengguna aktif	Sesuai	Lulus
9	Logout dan akses URL langsung tanpa login	Sesi hilang, redirect ke halaman login	Sesuai	Lulus

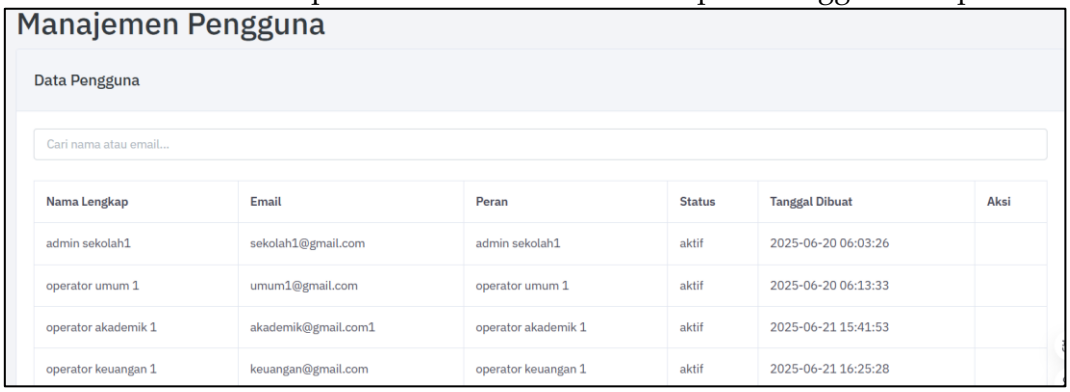
Berdasarkan Tabel 2, seluruh 9 skenario pengujian menghasilkan status Pass dengan tingkat keberhasilan 100% (9/9 skenario). Hasil ini membuktikan bahwa sistem RBAC yang dibangun berfungsi sesuai spesifikasi, mencakup validasi autentikasi, pembatasan akses berbasis peran, isolasi data antar sekolah, kontrol antarmuka CRUD, serta pembaruan hak akses secara real-time[23], [8].

C. Pembahasan Validasi Hak Akses dan Kontrol Antarmuka

Pengujian validasi hak akses membuktikan bahwa mekanisme RBAC bekerja pada dua lapis perlindungan secara bersamaan. Pertama, pada lapisan antarmuka, tombol aksi seperti Tambah, Edit, dan Hapus hanya ditampilkan apabila pengguna memiliki izin yang sesuai (boleh_tambah, boleh_ubah, boleh_hapus). Kedua, pada lapisan logika sistem, setiap permintaan URL divalidasi terhadap tabel role_permission sehingga akses langsung melalui URL pun tetap ditolak dengan kode HTTP 403. Pendekatan berlapis ini sejalan dengan rekomendasi keamanan sistem berbasis web yang menyatakan bahwa kontrol akses harus diterapkan baik di sisi tampilan maupun sisi server[12]. Hasil ini konsisten dengan penelitian Khairi et al. yang menyimpulkan bahwa RBAC efektif mencegah akses tidak berizin pada sistem multiuser[23], serta penelitian Agung dan Manongga yang membuktikan bahwa validasi berbasis role pada setiap request URL merupakan pendekatan yang andal untuk sistem otorisasi terpusat [8].



Gambar 5. Tampilan Pesan Penolakan Akses pada Pengguna Tanpa Izin"



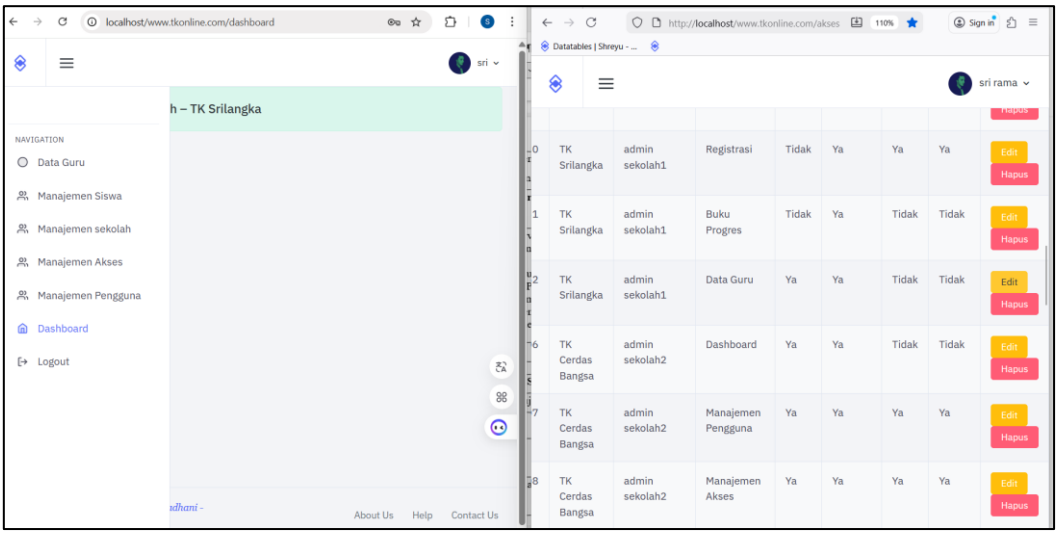
Gambar 6. Kontrol Tombol Aksi Berdasarkan Hak Akses CRUD

D. Pembahasan Mekanisme Real-Time Menggunakan Pusher.js

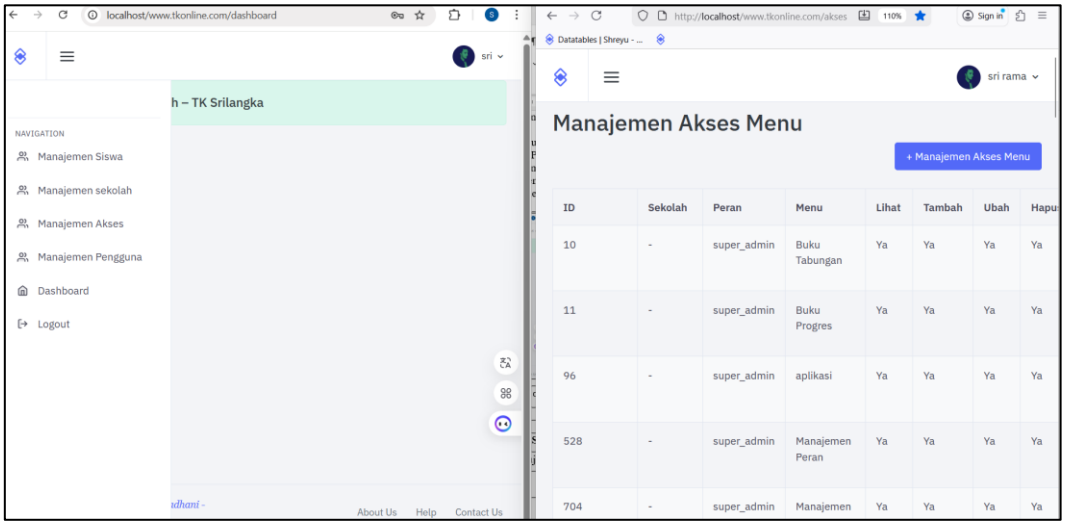
Salah satu kontribusi teknis penelitian ini adalah integrasi mekanisme pembaruan hak akses secara real-time menggunakan Pusher.js. Pusher.js merupakan layanan berbasis WebSocket yang memungkinkan komunikasi dua arah antara server dan client secara event-driven. Dalam sistem ini, mekanismenya bekerja melalui tahapan berikut: (1) Super Admin atau Admin Sekolah mengubah hak akses melalui halaman Manajemen Akses; (2) perubahan tersebut disimpan ke database oleh server PHP/CodeIgniter; (3) server memicu event melalui channel Pusher yang telah dikonfigurasi; (4) browser pengguna yang sedang aktif menerima event tersebut secara otomatis; (5) menu navigasi di sisi pengguna langsung diperbarui tanpa perlu memuat ulang halaman.

Hasil pengujian menunjukkan bahwa menu yang sebelumnya tersedia bagi Admin Sekolah dapat langsung disembunyikan sesaat setelah Super Admin menonaktifkan izin, dan sebaliknya menu baru yang diberikan izin langsung muncul tanpa perlu logout maupun reload. Pendekatan ini memberikan keunggulan signifikan dibandingkan sistem RBAC statis yang mengharuskan pengguna melakukan logout dan login kembali agar perubahan hak akses

berlaku [21]. Dengan integrasi Pusher.js, konsistensi kebijakan akses dapat terjaga secara dinamis dalam lingkungan multiuser aktif [6], [21].



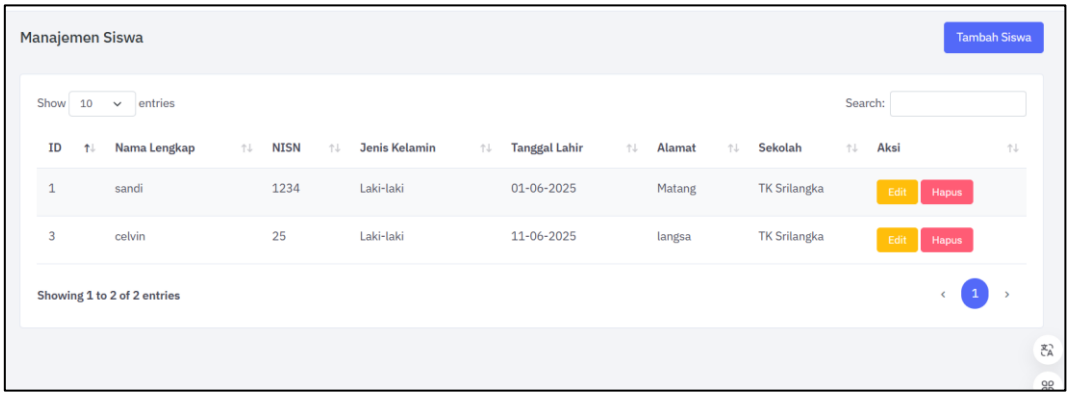
Gambar 7. Tampilan Menu Admin Sekolah Sebelum Hak Akses Diubah oleh Super Admin



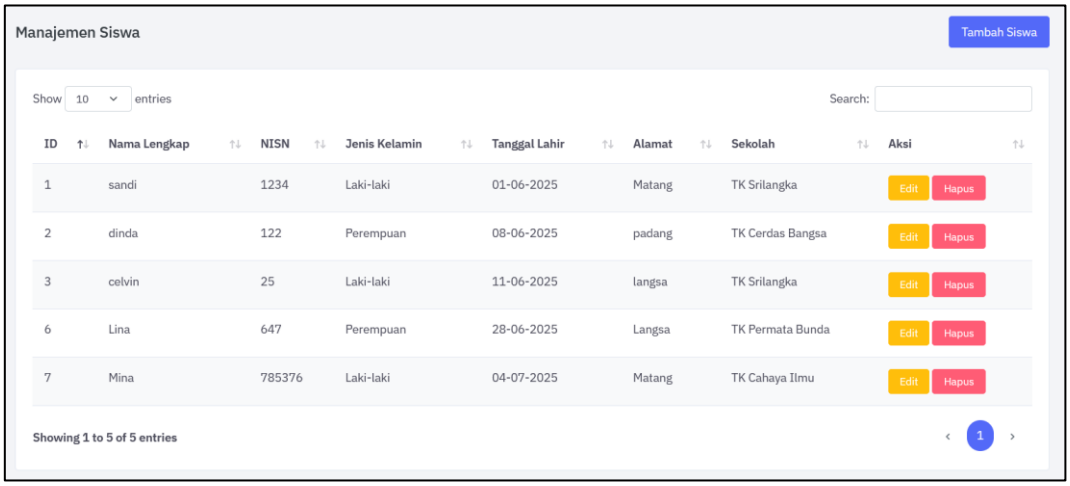
Gambar 8. Tampilan Menu Admin Sekolah Sesudah Hak Akses Diubah Secara Real-Time via Pusher.js

E. Pembahasan Pembatasan Data Antar Sekolah (Multi-Tenancy)

Sistem ini menerapkan prinsip multi-tenancy di mana setiap pengguna hanya dapat mengakses data yang berasal dari sekolah yang berafiliasi dengannya. Implementasi dilakukan dengan mengaitkan setiap entitas data (siswa, guru, pengguna) pada foreign key identitas sekolah (school_id). Pada setiap query data, sistem secara otomatis menyaring hasil berdasarkan school_id pengguna yang aktif, kecuali untuk Super Admin yang memiliki akses lintas sekolah. Hasil pengujian membuktikan bahwa Admin Sekolah hanya dapat melihat dan mengelola data siswa dan guru dari sekolahnya sendiri, sementara Super Admin dapat mengakses seluruh data dari semua sekolah yang terdaftar. Pendekatan ini efektif mencegah kebocoran data antar institusi, yang merupakan salah satu risiko utama pada sistem informasi berbasis portal induk [26], [15].



Gambar 9. Admin Sekolah Hanya Dapat Melihat Data Siswa dari Sekolahnya Sendiri



Gambar 10. Super Admin Dapat Mengakses Data Siswa dari Seluruh Sekolah

F. Perbandingan dengan Penelitian Terdahulu

Jika dibandingkan dengan penelitian terdahulu, hasil penelitian ini menunjukkan sejumlah persamaan sekaligus perbedaan yang signifikan. Persamaannya adalah RBAC terbukti efektif meningkatkan keamanan dan keteraturan akses pada sistem multiuser, sebagaimana ditunjukkan pada penelitian di domain koperasi mobile[4], sistem ERP[23], maupun sistem otorisasi terpusat [8]. Perbedaan utama penelitian ini terletak pada tiga aspek: pertama, konteks penerapan yang secara khusus berfokus pada lingkungan pendidikan anak usia dini (TK) dengan karakteristik organisasi yang lebih sederhana namun tetap membutuhkan kontrol akses ketat; kedua, penambahan dimensi pembatasan data berbasis identitas sekolah yang memungkinkan satu portal digunakan banyak institusi secara aman; dan ketiga, integrasi mekanisme real-time menggunakan Pusher.js yang belum ditemukan pada penelitian RBAC sebelumnya di domain pendidikan. Kombinasi ketiga aspek ini menghasilkan arsitektur RBAC yang lebih adaptif dan responsif dibandingkan implementasi statis pada penelitian-penelitian terdahulu [3],[27]. Secara keseluruhan, sistem RBAC yang dikembangkan berhasil mencapai seluruh tujuan penelitian: mengelola hak akses secara terstruktur, menjaga pemisahan data antar sekolah, mencegah akses tidak berizin baik melalui antarmuka maupun URL langsung, serta memberikan respons real-time terhadap perubahan kebijakan akses. Integrasi Pusher.js memberikan nilai tambah yang nyata dan menunjukkan potensi pengembangan sistem informasi sekolah yang lebih adaptif dan aman di masa mendatang [8],[4].

KESIMPULAN

Penelitian ini berhasil merancang dan mengimplementasikan sistem informasi sekolah Taman Kanak-Kanak (TK) berbasis multiuser dengan menerapkan mekanisme Role-Based Access Control (RBAC) sebagai model utama pengelolaan hak akses. Berdasarkan hasil pengujian black-box testing terhadap 9 skenario pengujian, seluruh skenario menghasilkan status

Pass dengan tingkat keberhasilan 100%, yang membuktikan bahwa sistem berfungsi sesuai spesifikasi fungsional yang dirancang.Sistem mampu membedakan hak akses antara tiga peran utama, yaitu Super Admin, Admin Sekolah, dan Operator, sehingga setiap pengguna hanya dapat mengakses menu, fungsi, dan data sesuai kewenangannya. Pengendalian akses diterapkan pada dua lapis perlindungan secara bersamaan, yaitu pada lapisan antarmuka melalui kontrol visibilitas tombol CRUD, dan pada lapisan logika sistem melalui validasi setiap permintaan URL terhadap tabel role_permission, sehingga akses tidak berizin dicegah baik melalui antarmuka maupun melalui akses URL langsung. Penerapan prinsip multi-tenancy berbasis identitas sekolah (school_id) terbukti efektif dalam menjaga isolasi data antar institusi, di mana pengguna selain Super Admin hanya dapat mengelola data yang berasal dari sekolahnya sendiri. Pendekatan ini mendukung keamanan lingkungan sistem multiuser dan multi-sekolah secara konsisten. Integrasi mekanisme pembaruan hak akses secara real-time menggunakan Pusher.js memberikan nilai tambah yang signifikan, di mana perubahan hak akses yang dilakukan oleh Super Admin atau Admin Sekolah dapat langsung diterapkan pada pengguna aktif tanpa memerlukan pemuatan ulang halaman. Hal ini menjadikan sistem lebih responsif dan adaptif dibandingkan implementasi RBAC statis pada penelitian-penelitian sebelumnya. Penelitian ini berkontribusi dalam menyediakan model arsitektur RBAC yang terstruktur, berlapis, dan responsif sebagai fondasi pengembangan sistem informasi pendidikan anak usia dini berbasis multiuser. Untuk pengembangan lebih lanjut, disarankan agar sistem diuji pada lingkungan sekolah nyata dengan penambahan fitur keamanan seperti enkripsi data, audit log aktivitas pengguna, serta penerapan autentikasi dua faktor guna meningkatkan ketahanan sistem secara menyeluruh.

DAFTAR PUSTAKA

[1] S. Winar, E. Rizki Putra, and I. Muslem R., "Sistem Informasi Kalkulasi Zakat Pada Kantor Baitul Mal Kabupaten Bireuen Berbasis Android," *Jurnal TIKA*, vol. 7, no. 3, 2022, doi: 10.51179/tika.v7i3.1584.

[2] P. E. Pemberdayaan and E. Perempuan, "Perancangan sistem autentikasi multi-role berbasis rbac pada platform e-learning pemberdayaan ekonomi perempuan 1) 1,2,3)," vol. 11, no. 1, pp. 1094–1104, 2026.

[3] A. Muliani Harahap, "Implementasi Metode Role-Based Access Control Pada Aplikasi E-Raport di MIN 15 Langkat Berbasis Android," 2024.

[4] A. S. Khairi, M. Alda, U. Islam, N. Sumatera, S. Utara, and H. Akses, "Implementasi Role Based Access Control dalam Pengelolaan Hak Akses Koperasi Berbasis Mobile," vol. 09, pp. 85–95, 2024.

[5] M. Noor and H. Siregar, "Analisis Keamanan Data pada Sistem Informasi Menggunakan Metode ISO / IEC 27001," vol. 1, no. 2, pp. 58–64, 2025.

[6] P. Y. Agung and D. Manongga, "Role-based access control (rbac) untuk sistem otorisasi terpusat berbasis flask studi kasus pt. xyz," vol. 9, no. 4, pp. 1768–1778, 2024.

[7] I. Artikel and A. Info, "Implementasi OWASP untuk Analisis Kerentanan dan Keamanan pada Sistem Informasi Akademik Terintegrasi Universitas Bina Darma," vol. 4, no. 1, pp. 1–7, 2025.

[8] E. Islam, R. Islam, M. Chetty, S. Lim, and M. Chadhar, "User authentication and access control to blockchain - based forensic log data," *EURASIP Journal on Information Security*, 2023, doi: 10.1186/s13635-023-00142-3.

[9] N. B. Adinugroho, P. Hendradi, and D. Sasongko, "ANALISIS KEAMANAN E-LEARNING MENGGUNAKAN OPEN WEB APPLICATION SECURITY PROJECT (OWASP) (STUDI KASUS : MOCA UNIMMA)," vol. 22, no. 02, pp. 132–138, 2022.

[10] U. Merangin, "PERANCANGAN SISTEM INFORMASI PERPUSTAKAAN DIGITAL BERBASIS ROLE-BASED ACCESS CONTROL (RBAC) PERPUSTAKAAN UNIVERSITAS MERANGIN Ichsandi 1 , Ranita Nurhidayah 2," vol. 2, no. 2, pp. 72–82, 2025.

[11] N. Ramadhanty and K. Informasi, "Implementasi Kerangka Keamanan NIST Dan ISO / IEC 27001 Dalam Menghadapi Ancaman Risiko Siber," no. 4, pp. 1–9, 2024.
[12] H. F. Atlam, M. A. Azad, M. O. Alassafi, A. A. Alshdadi, and A. Alenezi, "Risk-Based Access Control Model : A Systematic Literature Review," pp. 1–23.
[13] O. Houhou, S. Bitam, and A. Hamida, "HyARBAC : A New Hybrid Access Control Model for Cloud Computing," vol. 1, no. 1, 2024.
[14] K. V Brw, J. S. Supriadi, and N. Sukun, "SECURITY ANALYSIS OF COLLEGE WEBSITES," vol. 2, no. 1, pp. 13–20, 2025.
[15] S. Track and W. Product, "eXtensible Access Control Markup," no. January, pp. 1–154, 2013.
[16] Y. Zhang, "A ribute-based Encryption for Cloud Computing Access Control : A Survey Attribute-based Encryption for Cloud Computing Access Control : A Survey," vol. 53, no. 4, 2026, doi: 10.1145/3398036.
[17] W. Jansen, T. Grance, W. Jansen, and T. Grance, "Guidelines on Security and Privacy in Public Cloud Computing".
[18] M. Al Morsy, J. Grundy, and I. Müller, "An Analysis of the Cloud Computing Security Problem".
[19] A. Renaldy, A. Fauzi, A. N. Shabrina, and H. N. Ramadhan, "Peran Sistem Informasi dan Teknologi Informasi Terhadap Peningkatan Keamanan Informasi Perusahaan," vol. 2, no. 1, pp. 15–22, 2023.
[20] J. Park and U. States, "The UCONABC usage control model," vol. 7, no. 1, 2026, doi: 10.1145/984334.984339.
[21] I. K. Phan, "The Implementation of Role Based Access Control in a Cloud-Based Supply Chain Management System Penerapan Role Based Access Control dalam Sistem Supply Chain Management Berbasis Cloud," vol. 3, no. October, pp. 339–348, 2023.
[22] M. K. Kabier, A. A. Yassin, Z. A. Abduljabbar, and S. Lu, "Role Based Access Control Using Biometric the in Educational System," vol. 49, no. 1, pp. 85–101, 2023.
[23] E. R. Susanto *et al.*, "Analisis Implementasi Sistem Keamanan Basis Data Berbasis Role-Based Access Control (RBAC) pada Aplikasi Enterprise Resource Planning," vol. 5, no. 1, pp. 105–116, 2025, doi: 10.54259/satesi.v5i1.3997.
[24] I. P. Microgrids, S. Shin, M. Park, T. Kim, and H. Yang, "Architecture for Enhancing Communication Security with RBAC," pp. 1–18, 2024.
[25] V. C. Hu, K. Scarfone, R. Kuhn, and K. Sandlin, "Guide to Attribute Based Access Control (ABAC) Definition and Considerations NIST Special Publication 800-162 Guide to Attribute Based Access Control (ABAC) Definition and Considerations".
[26] N. Rahma and N. Mayesti, "Pengendalian Hak Akses pada Electronic Document and Records Management System di Kementerian Kelautan dan Perikanan Republik Indonesia," vol. 5, no. 1, pp. 33–48, 2019, doi: 10.14710/lenpust.v5i1.23578.
[27] O. M. Oluoha, A. Odeshina, O. Reis, V. Attipoe, and O. H. Orieno, "A Privacy-First Framework for Data Protection and Compliance Assurance in Digital Ecosystems," vol. 7, no. 4, pp. 620–646, 2023.