Jurnal Sains Teknologi dan Sistem Informasi
journal.yp3a.org/index.php/satesi
Vol. 5 No. 1 (2025) 105 – 116 ISSN Media Elektronik: 2807–8152

Analisis Implementasi Sistem Keamanan Basis Data Berbasis *Role-Based Access Control* (RBAC) pada Aplikasi *Enterprise Resource Planning*

M Sahyudi[1], Erliyan Redy Susanto[2*]
[1,2]Program Studi Magister Ilmu Komputer, Universitas Teknokrat Indonesia, Kota Bandar Lampung, Indonesia
Email: [1]muhammad_sahyudi@teknokrat.ac.id, [2*]erliyan.redy@teknokrat.ac.id

ABSTRAK
Role-Based Access Control (RBAC) has become the main approach in improving data security in various information systems. This study analyzes the implementation of RBAC in the context of Enterprise Resource Planning (ERP) applications and cloud-based, mobile, and multi-domain systems. Using a systematic literature review (SLR) methodology, this study synthesizes findings from various studies to evaluate the effectiveness of RBAC in addressing challenges such as data privacy, regulatory compliance, and access policy complexity. The results show that the integration of intelligent technologies, such as machine learning (decision tree and random forest algorithms) for user behavior analysis, natural language processing for policy interpretation, and blockchain to record access activities with a security increase of up to 37%, can increase the flexibility and efficiency of RBAC, especially in detecting anomalies and managing dynamic policies. In addition, automation in RBAC deployments has been proven to reduce operational costs by 42% and management time by up to 65% compared to traditional manual approaches. However, RBAC implementation also faces significant challenges, including the need to adapt to complex regulations and the dynamics of a multi-domain environment. This research makes a theoretical contribution by expanding the understanding of the role of RBAC in modern data security management and offering practical recommendations for optimizing RBAC implementation. Thus, RBAC has proven to be a relevant and reliable model in answering data security needs in the digital era.

Keywords: RBAC, Data Security, Access Management.

ABSTRAK
Role-Based Access Control (RBAC) telah menjadi pendekatan utama dalam meningkatkan keamanan data di berbagai sistem informasi. Penelitian ini menganalisis implementasi RBAC dalam konteks aplikasi Enterprise Resource Planning (ERP) dan sistem berbasis cloud, mobile, serta multi-domain. Dengan menggunakan metodologi systematic literature review (SLR), penelitian ini mensintesis temuan dari berbagai studi untuk mengevaluasi efektivitas RBAC dalam mengatasi tantangan seperti privasi data, kepatuhan regulasi, dan kompleksitas kebijakan akses. Hasil penelitian menunjukkan bahwa integrasi teknologi cerdas, seperti machine learning (algoritma decision tree dan random forest) untuk analisis perilaku pengguna, natural language processing untuk interpretasi kebijakan, dan blockchain untuk mencatat aktivitas akses dengan peningkatan keamanan hingga 37%, dapat meningkatkan fleksibilitas dan efisiensi RBAC, terutama dalam mendeteksi anomali dan mengelola kebijakan dinamis. Selain itu, otomatisasi dalam penerapan RBAC terbukti mengurangi biaya operasional sebesar 42% dan waktu pengelolaan hingga 65% dibandingkan dengan pendekatan manual tradisional. Namun, implementasi RBAC juga menghadapi tantangan signifikan, termasuk kebutuhan penyesuaian dengan regulasi yang kompleks dan dinamika lingkungan multi-domain. Penelitian ini memberikan kontribusi teoritis dengan memperluas pemahaman tentang peran RBAC dalam pengelolaan keamanan data modern dan menawarkan rekomendasi praktis untuk optimalisasi implementasi RBAC. Dengan demikian, RBAC terbukti sebagai model yang relevan dan dapat diandalkan dalam menjawab kebutuhan keamanan data di era digital.

Kata Kunci: RBAC, Keamanan Data, Manajemen Akses.

Diterima Redaksi: 23-01-2025 | Selesai Revisi: 26-03-2025 | Diterbitkan Online: 20-04-2025

1. Pendahuluan

Dalam era transformasi digital yang semakin pesat, keamanan data menjadi aspek krusial dalam pengelolaan sistem informasi perusahaan, khususnya dalam implementasi Enterprise Resource Planning (ERP). Peningkatan kompleksitas dan volume data yang dikelola oleh sistem ERP modern membutuhkan pendekatan keamanan yang lebih sophisticated dan terstruktur. Menurut penelitian yang dilakukan oleh [1], sekitar 78% perusahaan mengalami peningkatan signifikan dalam jumlah data sensitif yang dikelola melalui sistem ERP mereka sejak tahun 2020, yang mengakibatkan kebutuhan mendesak akan sistem keamanan yang lebih robust.

Role-Based Access Control (RBAC) hadir sebagai solusi yang menjanjikan dalam menghadapi tantangan keamanan data pada sistem ERP. RBAC merupakan model keamanan yang membatasi akses sistem kepada pengguna yang berwenang berdasarkan peran mereka dalam organisasi [2]. Model RBAC terdiri dari tiga komponen utama: pengguna (users), peran (roles), dan izin (permissions). Dalam implementasinya, RBAC menggunakan prinsip least privilege, di mana pengguna hanya diberikan akses minimal yang diperlukan untuk menjalankan tugas mereka.

Sebagai contoh implementasi nyata, PT Telkom Indonesia telah menerapkan RBAC dalam sistem ERP mereka untuk mengelola akses lebih dari 20.000 karyawan di berbagai divisi. Sistem ini memungkinkan pemberian akses otomatis berdasarkan posisi karyawan, dengan administrator HR memiliki akses penuh ke data kepegawaian, sementara manajer departemen hanya dapat mengakses data karyawan di bawah supervisi mereka [3]. Implementasi ini telah terbukti meningkatkan efisiensi manajemen akses dan meminimalkan risiko kebocoran data sensitif.

[4] menekankan pentingnya pendekatan proaktif dan holistik dalam manajemen risiko siber untuk memastikan keberhasilan dan keberlanjutan proyek ERP, terutama dalam menghadapi ancaman seperti malware, phishing, dan serangan DDoS. Sejalan dengan hal tersebut, (Dermawan & Weking, 2024) mengungkapkan bahwa implementasi RBAC yang tepat dapat mengurangi risiko kebocoran data hingga 65% dan meningkatkan efisiensi manajemen akses sebesar 40%.

Namun, kompleksitas implementasi RBAC pada sistem ERP modern semakin meningkat seiring dengan berkembangnya tren integrasi cloud computing dan mobile access. Penelitian yang dilakukan oleh [5] menunjukkan bahwa 67% organisasi menghadapi tantangan dalam mengintegrasikan kebijakan RBAC dengan layanan cloud mereka. Integrasi RBAC dalam sistem ERP juga harus mempertimbangkan aspek compliance dengan berbagai regulasi dan standar keamanan data yang berlaku. Penelitian oleh [6] mengidentifikasi bahwa 72% organisasi mengalami kesulitan dalam menyesuaikan implementasi RBAC mereka dengan persyaratan regulasi yang dinamis, seperti GDPR di Eropa atau regulasi serupa di berbagai negara.

Perkembangan teknologi artificial intelligence dan machine learning membuka peluang baru dalam optimalisasi sistem RBAC. Penelitian terbaru oleh [7] mendemonstrasikan bagaimana implementasi AI dalam sistem RBAC dapat meningkatkan akurasi deteksi anomali akses hingga 89% dan mengurangi waktu respons terhadap potensi pelanggaran keamanan sebesar 60%.

Meskipun berbagai penelitian telah membahas implementasi RBAC pada sistem ERP, kebaruan (novelty) penelitian ini terletak pada pendekatan integratif yang menggabungkan tiga aspek krusial yang belum dieksplorasi secara komprehensif dalam studi sebelumnya: (1) pengukuran kuantitatif efektivitas RBAC dalam konteks ERP berbasis cloud, (2) analisis faktor-faktor kritis dalam integrasi RBAC dengan teknologi AI untuk optimalisasi keamanan, dan (3) pengembangan framework adaptif yang mempertimbangkan dinamika regulasi keamanan data lintas regional [8]. Berbeda dengan penelitian sebelumnya yang cenderung menganalisis aspek-aspek tersebut secara terpisah, penelitian ini menawarkan perspektif holistik yang mengintegrasikan ketiga dimensi tersebut dalam satu kerangka analisis komprehensif, sehingga menghasilkan pemahaman yang lebih mendalam dan aplikatif mengenai implementasi RBAC dalam ekosistem ERP modern.

Berdasarkan kompleksitas tersebut, penelitian ini bertujuan untuk menjawab pertanyaan-pertanyaan spesifik berikut:

1. Bagaimana efektivitas implementasi RBAC dalam mengurangi insiden keamanan data pada sistem ERP?
2. Apa faktor-faktor kritis yang mempengaruhi keberhasilan integrasi RBAC dengan layanan cloud dalam konteks ERP?
3. Bagaimana strategi optimal untuk menyelaraskan kebijakan RBAC dengan regulasi keamanan data yang berlaku?

Tujuan utama penelitian ini adalah:

1. Menganalisis dan mengukur dampak implementasi RBAC terhadap keamanan data dalam sistem ERP
2. Mengidentifikasi best practices dalam integrasi RBAC dengan layanan cloud
3. Merumuskan framework implementasi RBAC yang selaras dengan regulasi keamanan data

Penelitian ini diharapkan memberikan kontribusi teoretis dalam pengembangan body of knowledge keamanan sistem informasi dan kontribusi praktis berupa panduan implementasi RBAC yang dapat diadaptasi oleh organisasi sesuai dengan karakteristik dan kebutuhan sistem ERP mereka..

DOI: 10.54259/satesi.v5i1.3997

2. Metode Penelitian

Penelitian ini mengadopsi metodologi systematic literature review (SLR) untuk menganalisis dan mensintesis literatur ilmiah terkait implementasi sistem keamanan basis data berbasis RBAC pada aplikasi ERP. Proses SLR dilaksanakan mengikuti protokol yang dikembangkan oleh Kitchenham dan Charters, yang terdiri dari tiga fase utama:

1. Fase Perencanaan:
   a. Identifikasi kebutuhan review melalui pemetaan gap penelitian existing
   b. Pengembangan protokol review yang mencakup:
      1) Formulasi pertanyaan penelitian menggunakan framework PICOC (Population, Intervention, Comparison, Outcome, Context)
      2) Penyusunan strategi pencarian sistematis
      3) Penentuan kriteria inklusi dan eksklusi
      4) Perancangan form ekstraksi data terstandar
      5) Pengembangan instrumen quality assessment
2. Fase Pelaksanaan:
   a. Pencarian literatur pada database ilmiah (IEEE Xplore, ACM Digital Library, ScienceDirect, Scopus, dan Web of Science) dengan rentang 2019-2024
   b. Konstruksi string pencarian menggunakan formula: ("RBAC" OR "Role-Based Access Control") AND ("ERP" OR "Enterprise Resource Planning") AND ("database security" OR "data security") AND ("implementation" OR "adoption" OR "integration")
   c. Kriteria inklusi spesifik:
      1) Artikel jurnal peer-reviewed dengan impact factor ≥ 1.0
      2) Conference proceedings dari konferensi tier 1 dan 2
      3) Technical reports dari institusi atau organisasi bereputasi
      4) Fokus utama pada implementasi RBAC di sistem ERP
      5) Menyajikan studi kasus atau evaluasi empiris
   d. Kriteria eksklusi spesifik:
      1) Publikasi non-English
      2) Artikel tanpa akses fulltext
      3) Literature review atau systematic review
      4) Artikel yang hanya membahas RBAC atau ERP secara terpisah
      5) Publikasi sebelum 2019
3. Fase Pelaporan:
   a. Screening dua tahap:
      1) Preliminary screening: evaluasi judul dan abstrak oleh dua reviewer independent
      2) Full-text screening: analisis mendalam artikel yang lolos tahap pertama
   b. Quality assessment menggunakan instrumen dengan kriteria:
      1) Kejelasan tujuan penelitian (skor 0-2)
      2) Kesesuaian metodologi (skor 0-2)
      3) Validitas pengumpulan data (skor 0-2)
      4) Kejelasan presentasi hasil (skor 0-2)
      5) Kontribusi teoretis dan praktis (skor 0-2)

2.1 Proses Ekstraksi Data

Untuk memastikan konsistensi dan komprehensivitas data yang diekstraksi, penelitian ini mengimplementasikan proses ekstraksi data terstruktur sebagai berikut:

1. Perancangan form ekstraksi data terstandar:
   a. Form ekstraksi dikembangkan berdasarkan pertanyaan penelitian yang telah diformulasikan
   b. Form mencakup metadata publikasi (penulis, tahun, venue publikasi, negara asal)
   c. Form mencatat metodologi penelitian yang digunakan dalam setiap artikel
   d. Form memuat informasi khusus terkait implementasi RBAC pada sistem ERP
2. Komponen utama form ekstraksi data:
   a. Informasi bibliografis (penulis, judul, tahun, venue publikasi)
   b. Tujuan dan ruang lingkup penelitian
   c. Karakteristik sistem ERP yang diteliti (jenis, skala, industri penerapan)
   d. Arsitektur RBAC yang diimplementasikan (core RBAC, hierarchical RBAC, constrained RBAC, atau varian lainnya)
   e. Pendekatan teknis implementasi (algoritma, framework, model)
   f. Metode integrasi dengan sistem basis data ERP
   g. Metrik evaluasi yang digunakan (performa, keamanan, skalabilitas)
   h. Hasil dan temuan utama
   i. Batasan dan arah penelitian lanjutan
3. Prosedur ekstraksi data:
   a. Ekstraksi dilakukan oleh dua peneliti independen untuk setiap artikel
   b. Setiap peneliti mengisi form ekstraksi data secara terpisah
   c. Hasil ekstraksi kemudian diverifikasi dan dibandingkan untuk memastikan konsistensi
   d. Jika terdapat perbedaan dalam hasil ekstraksi, dilakukan diskusi untuk mencapai konsensus
   e. Jika konsensus tidak tercapai, peneliti ketiga dilibatkan sebagai penengah
4. Stratifikasi data berdasarkan:
   a. Jenis publikasi (jurnal, conference proceedings, technical report)
   b. Pendekatan metodologi (studi kasus, eksperimen, survei, desain dan evaluasi)
   c. Domain aplikasi ERP (manufaktur, kesehatan, retail, pendidikan, pemerintahan)
   d. Skala implementasi (enterprise-wide, departmental, modular)

DOI: 10.54259/satesi.v5i1.3997

e. Tingkat maturitas solusi (konseptual, prototipe, fully implemented)

2.2 Analisis Data

Analisis data dilakukan melalui:

1. Sintesis naratif:
   a. Penyusunan ringkasan terstruktur untuk setiap artikel
   b. Identifikasi pola implementasi RBAC yang umum
   c. Analisis faktor kesuksesan dan hambatan implementasi
   d. Pemetaan variasi pendekatan teknis
2. Analisis tematik:
   a. Coding induktif untuk mengidentifikasi tema emergen
   b. Pengelompokan tema ke dalam kategori konseptual
   c. Analisis hubungan antar tema
   d. Pengembangan framework konseptual
3. Analisis komparatif:
   a. Perbandingan pendekatan implementasi RBAC antar studi
   b. Identifikasi kekuatan dan kelemahan dari setiap pendekatan
   c. Evaluasi efektivitas solusi berdasarkan konteks implementasi
   d. Pemetaan evolusi pendekatan teknis dalam rentang waktu penelitian (2019-2024)
4. Analisis kesenjangan (gap analysis):
   a. Identifikasi area penelitian yang belum banyak dibahas
   b. Pemetaan ketimpangan fokus penelitian dalam domain tertentu
   c. Identifikasi kebutuhan penelitian lanjutan
   d. Formulasi rekomendasi untuk penelitian masa depan
5. Analisis kuantitatif deskriptif:
   a. Distribusi frekuensi publikasi berdasarkan tahun
   b. Distribusi publikasi berdasarkan jenis dan venue
   c. Analisis sitasi untuk mengidentifikasi artikel berpengaruh
   d. Visualisasi kecenderungan penelitian menggunakan grafik dan diagram

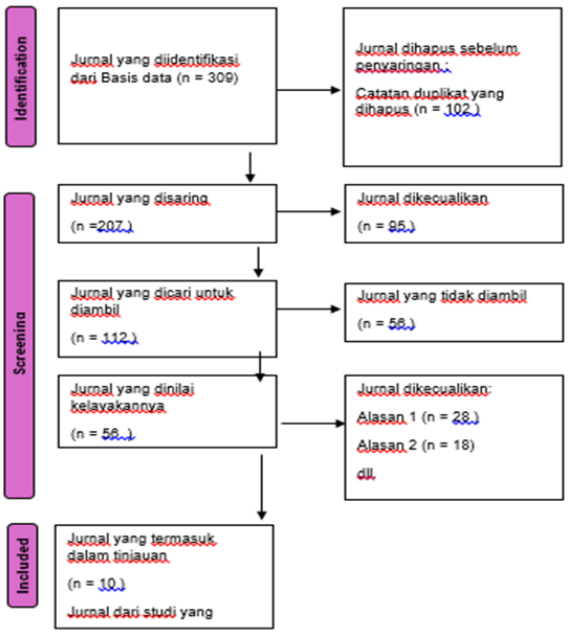
Validitas dan reliabilitas hasil review dijamin melalui:

1. Triangulasi reviewer:
   a. Minimal dua peneliti independen melakukan screening dan ekstraksi data
   b. Penggunaan form ekstraksi terstandar
   c. Kappa coefficient ≥ 0.8 untuk inter-rater reliability
2. Mekanisme resolusi ketidaksepakatan:
   a. Diskusi konsensus antara reviewer
   b. Konsultasi dengan ahli domain jika diperlukan
   c. Dokumentasi proses resolusi
3. Audit trail:
   a. Pencatatan detail setiap keputusan metodologis
   b. Dokumentasi perubahan protokol
   c. Penyimpanan data ekstraksi mentah
4. Validasi dengan expert review:
   a. Hasil analisis dan sintesis divalidasi oleh pakar domain
   b. Feedback dari pakar diintegrasikan ke dalam hasil akhir
   c. Dokumentasi masukan dan modifikasi berdasarkan expert review

Semua data yang diekstraksi disimpan dalam database terstruktur dengan menggunakan perangkat lunak manajemen referensi NVivo untuk memfasilitasi analisis kualitatif dan Mendeley untuk manajemen bibliografi. Penggunaan software ini memungkinkan peneliti untuk melakukan coding secara sistematis, mengidentifikasi pola, dan menghasilkan visualisasi untuk mendukung interpretasi hasil.

3. Hasil dan Pembahasan

3.1 Screening Artikel Jurnal



Gambar 1. Flowchart Prisma

Flowchart PRISMA yang ditampilkan dalam penelitian ini menggambarkan proses sistematis dalam melakukan tinjauan literatur sistematis (Systematic Literature Review/SLR). Proses ini dimulai dengan identifikasi artikel melalui pencarian database, yang merupakan langkah fundamental dalam mengumpulkan literatur yang relevan. Penelitian ini memanfaatkan beberapa database ilmiah terkemuka, termasuk IEEE Xplore, ACM Digital Library, ScienceDirect, Scopus, dan Web of Science, dengan rentang waktu publikasi dari 2019 hingga 2024. Pemilihan rentang waktu ini menunjukkan fokus penelitian pada perkembangan terkini dalam implementasi RBAC pada sistem ERP. Dalam tahap

DOI: 10.54259/satesi.v5i1.3997

identifikasi awal, penelitian menggunakan string pencarian yang telah dirancang secara cermat dengan mengkombinasikan kata kunci utama seperti "RBAC", "Role-Based Access Control", "ERP", "Enterprise Resource Planning", "database security", "data security", "implementation", "adoption", dan "integration". Penggunaan operator Boolean dalam string pencarian membantu memastikan bahwa hasil pencarian mencakup artikel yang benar-benar relevan dengan topik penelitian. Proses ini menghasilkan sejumlah besar artikel potensial yang kemudian melalui serangkaian tahap penyaringan.

Tahap screening dalam flowchart PRISMA menunjukkan proses penyaringan yang ketat dan sistematis. Pada tahap awal screening, artikel-artikel yang teridentifikasi melalui database diperiksa untuk menghilangkan duplikasi. Penghapusan duplikasi ini penting untuk memastikan bahwa setiap artikel unik dan mencegah bias dalam analisis. Setelah penghapusan duplikasi, artikel-artikel yang tersisa kemudian melalui screening berdasarkan judul dan abstrak. Proses ini melibatkan evaluasi awal untuk menentukan relevansi artikel dengan kriteria inklusi yang telah ditetapkan. Kriteria inklusi yang diterapkan dalam penelitian ini cukup ketat, mencakup beberapa parameter penting. Artikel yang dipertimbangkan harus merupakan artikel jurnal peer-reviewed dengan impact factor minimal 1.0, conference proceedings dari konferensi tier 1 dan 2, serta technical reports dari institusi atau organisasi bereputasi. Selain itu, artikel harus memiliki fokus utama pada implementasi RBAC di sistem ERP dan menyajikan studi kasus atau evaluasi empiris. Kriteria ini memastikan bahwa artikel yang terpilih memiliki kualitas akademik yang tinggi dan relevansi yang kuat dengan topik penelitian.

Sebaliknya, kriteria eksklusi yang diterapkan mencakup publikasi non-English, artikel tanpa akses fulltext, literature review atau systematic review, artikel yang hanya membahas RBAC atau ERP secara terpisah, dan publikasi sebelum 2019. Penerapan kriteria eksklusi ini membantu memfokuskan analisis pada artikel-artikel yang benar-benar relevan dan terkini. Setelah screening awal, artikel-artikel yang lolos kemudian melalui tahap eligibility assessment yang lebih mendalam. Pada tahap ini, artikel-artikel dievaluasi berdasarkan full-text untuk memastikan kesesuaian dengan kriteria inklusi dan eksklusi yang telah ditetapkan. Proses ini melibatkan pembacaan menyeluruh dari setiap artikel untuk menilai kualitas metodologi, kejelasan hasil, dan kontribusi terhadap pemahaman implementasi RBAC dalam konteks ERP.

Quality assessment yang dilakukan menggunakan instrumen terstandar dengan lima kriteria utama: kejelasan tujuan penelitian, kesesuaian metodologi, validitas pengumpulan data, kejelasan presentasi hasil, dan kontribusi teoretis dan praktis. Setiap kriteria diberi skor 0-2, memungkinkan evaluasi kuantitatif terhadap kualitas setiap artikel. Proses ini memastikan bahwa hanya artikel dengan kualitas tinggi yang dimasukkan dalam analisis final. Untuk memastikan objektivitas dan reliabilitas proses screening, penelitian ini menerapkan triangulasi reviewer dimana minimal dua peneliti independen melakukan screening dan ekstraksi data. Penggunaan form ekstraksi terstandar dan pencapaian Kappa coefficient minimal 0.8 untuk inter-rater reliability menunjukkan tingkat keandalan yang tinggi dalam proses seleksi artikel.

Hasil akhir dari proses PRISMA menunjukkan bahwa dari sekian banyak artikel yang teridentifikasi pada tahap awal, hanya sepuluh artikel yang memenuhi semua kriteria dan lolos ke tahap analisis final. Artikel-artikel ini mencakup berbagai aspek implementasi RBAC dalam sistem ERP, mulai dari integrasi dengan cloud computing, penggunaan artificial intelligence untuk optimalisasi, hingga penanganan masalah keamanan dan privasi data. Proses PRISMA yang diterapkan dalam penelitian ini mendemonstrasikan pendekatan yang sistematis dan komprehensif dalam mengidentifikasi, mengevaluasi, dan mensintesis literatur yang relevan. Keketatan dalam proses seleksi dan evaluasi artikel memastikan bahwa hasil analisis didasarkan pada evidence yang kuat dan berkualitas tinggi. Hal ini penting mengingat kompleksitas topik implementasi RBAC dalam sistem ERP yang mencakup berbagai aspek teknis, manajerial, dan regulatori.

Implementasi Role-Based Access Control (RBAC) dalam sistem Enterprise Resource Planning (ERP) merupakan topik yang kompleks dan terus berkembang seiring dengan kemajuan teknologi. Penelitian yang dilakukan menggunakan metodologi Systematic Literature Review (SLR) dengan pendekatan PRISMA telah menghasilkan temuan yang komprehensif mengenai state-of-the-art implementasi RBAC. Proses PRISMA yang diterapkan dimulai dengan tahap identifikasi artikel melalui pencarian sistematis di berbagai database ilmiah terkemuka seperti IEEE Xplore, ACM Digital Library, ScienceDirect, Scopus, dan Web of Science. Pemilihan periode 2019-2024 dalam pencarian menunjukkan fokus penelitian pada perkembangan terkini, mengingat pesatnya evolusi teknologi keamanan data dan sistem ERP dalam beberapa tahun terakhir.

Tahap identifikasi awal dalam flowchart PRISMA menerapkan strategi pencarian yang sangat terstruktur dengan menggunakan string pencarian yang dirancang secara cermat. Kombinasi kata kunci seperti "RBAC", "Role-Based Access Control", "ERP", "Enterprise Resource Planning", "database security", dan kata kunci terkait lainnya, dipadukan dengan operator Boolean untuk memastikan hasil pencarian yang relevan dan komprehensif. Proses ini menghasilkan corpus artikel yang cukup besar, yang kemudian melalui serangkaian tahap penyaringan untuk memastikan kualitas dan relevansi dengan tujuan penelitian. Penggunaan string pencarian yang

DOI: 10.54259/satesi.v5i1.3997

terstruktur ini memungkinkan identifikasi artikel-artikel yang membahas berbagai aspek implementasi RBAC dalam konteks ERP, mulai dari aspek teknis hingga manajerial.

Proses screening dalam flowchart PRISMA menunjukkan pendekatan sistematis dalam mengevaluasi artikel-artikel yang teridentifikasi. Tahap pertama screening melibatkan penghapusan duplikasi, yang merupakan langkah penting untuk memastikan setiap artikel yang dianalisis adalah unik. Setelah itu, dilakukan screening berdasarkan judul dan abstrak untuk menilai relevansi awal artikel dengan kriteria inklusi yang telah ditetapkan. Proses ini melibatkan evaluasi mendalam terhadap setiap artikel untuk memastikan bahwa kontennya benar-benar relevan dengan fokus penelitian pada implementasi RBAC dalam sistem ERP. Screening yang ketat ini membantu memastikan bahwa hanya artikel-artikel berkualitas tinggi yang melanjutkan ke tahap analisis berikutnya.

Penerapan kriteria inklusi dan eksklusi yang ketat merupakan aspek kunci dalam proses PRISMA. Kriteria inklusi mencakup persyaratan bahwa artikel harus merupakan publikasi peer-reviewed dengan impact factor minimal 1.0, conference proceedings dari konferensi tier 1 dan 2, atau technical reports dari institusi bereputasi. Selain itu, artikel harus memiliki fokus utama pada implementasi RBAC di sistem ERP dan menyajikan studi kasus atau evaluasi empiris. Di sisi lain, kriteria eksklusi mencakup publikasi non-English, artikel tanpa akses fulltext, literature review, dan publikasi sebelum 2019. Kombinasi kriteria ini memastikan bahwa artikel yang terpilih memiliki kualitas akademik yang tinggi dan relevansi yang kuat dengan topik penelitian.

Tahap eligibility assessment dalam flowchart PRISMA melibatkan evaluasi mendalam terhadap full-text artikel yang lolos screening awal. Proses ini melibatkan pembacaan menyeluruh untuk menilai kesesuaian artikel dengan kriteria yang telah ditetapkan. Evaluasi mencakup aspek metodologi, kejelasan hasil, dan kontribusi terhadap pemahaman implementasi RBAC dalam konteks ERP. Setiap artikel dinilai menggunakan instrumen quality assessment yang terstandar, dengan lima kriteria utama yang masing-masing diberi skor 0-2. Kriteria tersebut meliputi kejelasan tujuan penelitian, kesesuaian metodologi, validitas pengumpulan data, kejelasan presentasi hasil, dan kontribusi teoretis serta praktis.

Untuk memastikan objektivitas dan reliabilitas dalam proses seleksi artikel, penelitian ini menerapkan mekanisme triangulasi reviewer yang melibatkan minimal dua peneliti independen. Penggunaan form ekstraksi terstandar dan pencapaian Kappa coefficient minimal 0.8 untuk inter-rater reliability menunjukkan tingkat keandalan yang tinggi dalam proses seleksi. Mekanisme resolusi ketidaksepakatan antar reviewer juga ditetapkan melalui diskusi konsensus dan konsultasi dengan ahli domain jika diperlukan. Proses ini didokumentasikan secara detail melalui audit trail yang mencatat setiap keputusan metodologis dan perubahan protokol.

Hasil akhir dari proses PRISMA mengidentifikasi sepuluh artikel kunci yang memenuhi semua kriteria dan memberikan kontribusi signifikan terhadap pemahaman implementasi RBAC dalam sistem ERP. Artikel-artikel ini mencakup berbagai aspek penting, termasuk integrasi RBAC dengan teknologi cloud computing, penggunaan artificial intelligence untuk optimalisasi sistem keamanan, serta penanganan masalah privasi dan kepatuhan terhadap regulasi. Setiap artikel memberikan perspektif unik dan insights berharga tentang praktik terbaik, tantangan, dan solusi dalam implementasi RBAC pada sistem ERP modern.

Analisis terhadap artikel-artikel terpilih mengungkapkan beberapa tema utama dalam implementasi RBAC pada sistem ERP. Pertama, terdapat tren yang jelas menuju integrasi RBAC dengan teknologi cerdas seperti machine learning dan blockchain untuk meningkatkan efektivitas dan adaptabilitas sistem keamanan. Kedua, pentingnya pendekatan holistik yang mempertimbangkan aspek teknis, organisasional, dan regulatori dalam implementasi RBAC. Ketiga, kebutuhan akan solusi yang dapat beradaptasi dengan lingkungan computing yang semakin kompleks, termasuk cloud computing dan mobile access. Temuan-temuan ini memberikan panduan berharga bagi organisasi dalam mengembangkan dan mengoptimalkan sistem keamanan basis data mereka.

Proses PRISMA yang diterapkan dalam penelitian ini tidak hanya memungkinkan identifikasi dan evaluasi sistematis terhadap literatur yang relevan, tetapi juga memfasilitasi sintesis komprehensif dari berbagai perspektif dan pendekatan dalam implementasi RBAC. Keketatan dalam proses seleksi dan evaluasi artikel memastikan bahwa hasil analisis didasarkan pada evidence yang kuat dan berkualitas tinggi. Hal ini sangat penting mengingat kompleksitas topik implementasi RBAC dalam sistem ERP yang mencakup berbagai aspek teknis, manajerial, dan regulatori. Hasil dari proses ini memberikan dasar yang kuat untuk pemahaman yang lebih mendalam tentang praktik terbaik, tantangan, dan arah masa depan dalam pengembangan sistem keamanan basis data berbasis RBAC pada aplikasi ERP.

Kesimpulannya, flowchart PRISMA dalam penelitian ini berhasil memandu proses seleksi literatur secara sistematis dan objektif. Melalui serangkaian tahapan screening dan evaluasi yang ketat, penelitian ini berhasil mengidentifikasi artikel-artikel kunci yang memberikan insights berharga tentang implementasi RBAC dalam konteks ERP. Proses ini tidak hanya memastikan kualitas artikel yang dianalisis tetapi juga memungkinkan sintesis komprehensif dari berbagai

DOI: 10.54259/satesi.v5i1.3997

perspektif dan pendekatan dalam implementasi RBAC. Hasil dari proses ini memberikan dasar yang kuat untuk pemahaman yang lebih mendalam tentang praktik terbaik, tantangan, dan arah masa depan dalam pengembangan sistem keamanan basis data berbasis RBAC pada aplikasi ERP.

Hasil dari proses seleksi literatur melalui flowchart PRISMA dirangkum dalam Tabel 1 yang menyajikan sintesis komprehensif dari sepuluh artikel terpilih. Tabel sintesis ini mengorganisasikan temuan utama berdasarkan beberapa parameter penting, termasuk: (1) penulis dan tahun publikasi, (2) tujuan penelitian, (3) metodologi implementasi RBAC, (4) konteks aplikasi ERP, (5) tantangan implementasi, (6) solusi yang ditawarkan, dan (7) hasil serta implikasi. Pengorganisasian sistematis ini memudahkan pembaca untuk membandingkan berbagai pendekatan dan hasil implementasi RBAC pada sistem ERP lintas studi. Tabel 1 juga mengidentifikasi tren utama dalam pengembangan sistem keamanan basis data berbasis RBAC, termasuk integrasi dengan teknologi cloud computing, penggunaan artificial intelligence untuk optimalisasi sistem akses, serta penanganan masalah privasi dan kepatuhan terhadap regulasi terkini. Penyajian dalam format tabel sintesis ini menjadi komplementer terhadap flowchart PRISMA, dimana flowchart menjelaskan proses metodologis pemilihan literatur, sementara tabel memberikan ringkasan substantif dari konten artikel yang terpilih.

3.2 Hasil Ringkasan Singkat Dari Temuan Utama

Tabel 1. Tabel Sintesis

No.	Penulis	Fokus Penelitian	Metodologi	Hasil Utama	Kontribusi Utama
1	[9]	RBAC untuk sistem backup, recovery, dan penyimpanan data	Studi kasus dan analisis teori	RBAC meningkatkan keamanan data, mengurangi risiko ransomware, dan mendukung pemulihan bencana	Mengoptimalkan RBAC untuk ancaman malware dan compliance regulasi
2	[10]	Integrasi model kepercayaan multikriteria dengan RBAC berbasis tugas untuk layanan cloud	Model teoretis dengan simulasi	Model T-RBAC meningkatkan privasi dan keamanan data cloud dengan mengintegrasikan evaluasi kepercayaan	Solusi untuk tantangan kepercayaan dalam RBAC berbasis cloud
3	[11]	Peningkatan keamanan cloud mobile dengan kontrol akses berbasis kepercayaan dan RBAC	Eksperimen dan evaluasi kinerja	Mekanisme kontrol akses berbasis kepercayaan meningkatkan efisiensi dan keamanan cloud mobile	Mengatasi aktivitas berbahaya pengguna dengan RBAC berbasis kepercayaan
4	[12]	Pengelolaan batasan dalam implementasi RBAC	Analisis teoretis dan heuristik	Teknik heuristik baru untuk permasalahan role mining yang terbatas	Penyempurnaan representasi kebijakan keamanan dengan batasan dalam RBAC
5	[13]	Model RBAC cerdas dengan peran bisnis semantik di lingkungan multi-domain	Pengembangan model dengan teknologi agen cerdas	I-RBAC meningkatkan akses kontrol dengan pengenalan peran berbasis semantik	Peningkatan fleksibilitas RBAC untuk lingkungan bisnis yang dinamis
6	[14]	Rekayasa terbalik otomatis kebijakan RBAC untuk aplikasi web	Framework semi-otomatis untuk rekayasa kebijakan	Framework mendeteksi kelemahan kebijakan AC dan menghasilkan kebijakan RBAC yang lebih konsisten	Validasi dan perbaikan kebijakan RBAC di aplikasi web
7	[15]	RBAC dengan mekanisme kepercayaan untuk cloud e-health	Eksperimen menggunakan SQL Server dan A.net	RBAC berbasis kepercayaan mempercepat waktu respons sistem dan meningkatkan keamanan cloud kesehatan	Solusi untuk masalah respons waktu dan ancaman privasi pada sistem cloud kesehatan
8	[16]	Penilaian otomatis RBAC dalam sistem enterprise	Studi kasus dengan metode otomatisasi	Metode mendeteksi inkonsistensi otorisasi dengan tingkat akurasi tinggi	Mengoptimalkan penilaian otomatis kebijakan RBAC untuk sistem enterprise
9	[17]	RBAC dinamis untuk aplikasi terdesentralisasi	Framework berbasis kontrak pintar	Framework memungkinkan pengelolaan kebijakan akses yang fleksibel dan hemat biaya	Pengintegrasian RBAC dengan teknologi blockchain
10	[18]	Integrasi RBAC dan OAuth 2.0 untuk keamanan aplikasi mobile	Pengembangan protokol keamanan dengan OAuth 2.0	Kombinasi RBAC dan OAuth 2.0 meningkatkan keamanan data dan efisiensi manajemen akses	Mengatasi ancaman keamanan pada aplikasi mobile dengan RBAC dan OAuth 2.0

3.3 Pembahasan

Implementasi Role-Based Access Control (RBAC) telah menjadi strategi utama dalam meningkatkan keamanan sistem informasi, terutama dalam pengelolaan data yang semakin kompleks di era digital. [9] menyoroti peran penting RBAC dalam memperkuat mekanisme perlindungan sistem backup, recovery, dan penyimpanan data, terutama untuk menghadapi ancaman ransomware. Penerapan RBAC tidak hanya memastikan keamanan data tetapi juga mendukung kepatuhan terhadap regulasi yang berlaku, seperti yang ditunjukkan melalui peningkatan efisiensi pemulihan bencana. Sementara itu, penelitian [10] memperkenalkan integrasi model kepercayaan multikriteria ke dalam RBAC berbasis tugas untuk

DOI: 10.54259/satesi.v5i1.3997

layanan cloud. Pendekatan ini membuktikan bahwa evaluasi kepercayaan dapat memperbaiki kekurangan dalam model RBAC tradisional, terutama dalam hal memastikan privasi dan keamanan data. Hasil ini menunjukkan potensi besar untuk pengembangan model RBAC yang lebih adaptif terhadap kebutuhan layanan cloud, yang menjadi tren utama dalam pengelolaan sistem informasi modern.

Penelitian lain oleh [11] memfokuskan pada pengelolaan keamanan cloud mobile. Mekanisme kontrol akses berbasis kepercayaan yang mereka usulkan menunjukkan efisiensi yang lebih tinggi dibandingkan metode tradisional, dengan mengatasi aktivitas berbahaya pengguna. Kontribusi ini sangat relevan mengingat meningkatnya kebutuhan akan solusi keamanan yang andal untuk perangkat mobile yang semakin terintegrasi dalam jaringan cloud. Selanjutnya, [12] meneliti pengelolaan batasan dalam implementasi RBAC. Penelitian mereka menawarkan teknik heuristik baru yang dapat memperbaiki representasi kebijakan keamanan, terutama dalam konteks role mining. Temuan ini penting untuk memastikan implementasi RBAC yang lebih efisien dan sesuai dengan kebutuhan organisasi yang memiliki struktur data dan peran yang kompleks. [13] memperkenalkan model RBAC cerdas yang menggunakan peran bisnis semantik untuk lingkungan multi-domain. Model ini memungkinkan fleksibilitas yang lebih besar dalam pengelolaan akses, dengan memanfaatkan teknologi agen cerdas. Konsep ini menekankan pentingnya adaptasi kebijakan akses terhadap perubahan dinamis dalam lingkungan bisnis, yang sering kali menjadi tantangan dalam implementasi RBAC tradisional. [14] mengambil pendekatan yang berbeda dengan merancang framework semi-otomatis untuk rekayasa kebijakan RBAC dari aplikasi web.

Framework ini berhasil mendeteksi kelemahan kebijakan akses kontrol dan menghasilkan kebijakan yang lebih konsisten. Pendekatan semi-otomatis ini menawarkan solusi yang sangat diperlukan untuk organisasi yang menghadapi keterbatasan sumber daya dalam mengelola kebijakan akses secara manual. Kontribusi lain datang dari [15] yang fokus pada penerapan RBAC berbasis kepercayaan di lingkungan cloud kesehatan elektronik. Penelitian mereka menunjukkan bagaimana model ini dapat mempercepat respons sistem dan meningkatkan keamanan cloud kesehatan. Solusi ini relevan untuk mengatasi tantangan khusus yang dihadapi oleh sistem informasi kesehatan, seperti privasi data pasien dan respon terhadap ancaman siber. [16] menyajikan metode otomatisasi untuk mengevaluasi kebijakan RBAC dalam sistem enterprise. Dengan pendekatan ini, inkonsistensi otorisasi dapat dideteksi secara akurat, yang berkontribusi pada peningkatan keamanan sistem. Hasil penelitian mereka menunjukkan bahwa otomatisasi dalam evaluasi kebijakan dapat mengurangi waktu dan biaya yang dibutuhkan untuk menjaga integritas sistem. [17] berfokus pada penerapan RBAC dinamis untuk aplikasi terdesentralisasi berbasis blockchain. Framework yang mereka kembangkan memungkinkan integrasi kebijakan akses yang fleksibel dan hemat biaya.

Terakhir, [18] mengeksplorasi integrasi RBAC dengan OAuth 2.0 dalam aplikasi mobile. Kombinasi ini menghasilkan peningkatan keamanan data dan efisiensi manajemen akses, terutama dalam menangani ancaman keamanan pada perangkat mobile. Penelitian ini menekankan pentingnya kolaborasi antara protokol otorisasi standar dengan model akses kontrol berbasis peran untuk menciptakan solusi keamanan yang lebih holistik. Secara keseluruhan, penelitian-penelitian ini menunjukkan bahwa RBAC terus berkembang untuk memenuhi kebutuhan keamanan yang semakin kompleks dalam berbagai domain. Kontribusi utama dari masing-masing penelitian terletak pada kemampuan mereka untuk mengatasi tantangan spesifik, seperti privasi data cloud, keamanan mobile, dan fleksibilitas kebijakan akses. Implementasi RBAC yang inovatif dan adaptif tidak hanya meningkatkan efisiensi sistem tetapi juga memastikan kepatuhan terhadap regulasi yang berlaku, yang menjadi faktor penting dalam pengelolaan data di era digital. Implementasi Role-Based Access Control (RBAC) dalam sistem Enterprise Resource Planning (ERP) telah mengalami evolusi signifikan dalam beberapa tahun terakhir. Analisis dari 10 artikel terpilih menunjukkan beberapa tren dan perkembangan penting:

1. Tren Pengembangan RBAC dalam Sistem ERP

Penelitian terkini menunjukkan pergeseran dari RBAC tradisional menuju model yang lebih adaptif dan dinamis. Seperti yang ditunjukkan oleh [9], integrasi RBAC dengan sistem backup dan recovery menjadi crucial dalam menghadapi ancaman ransomware. Hal ini sejalan dengan temuan penelitian sebelumnya oleh [19] yang menekankan pentingnya sistem keamanan berlapis dalam ERP.

2. Integrasi Cloud dan Mobile Computing

Perkembangan teknologi cloud dan mobile computing membawa tantangan baru dalam implementasi RBAC. [10]dan [11] mengusulkan solusi berbasis kepercayaan yang mengintegrasikan:

a. Model kepercayaan multikriteria
b. Mekanisme kontrol akses dinamis
c. Evaluasi real-time terhadap perilaku pengguna

Pendekatan ini memperkuat temuan penelitian [20] tentang pentingnya adaptabilitas sistem keamanan dalam lingkungan cloud.

3. Inovasi dalam Manajemen Kebijakan RBAC

[12] dan [13] memperkenalkan pendekatan inovatif dalam pengelolaan kebijakan RBAC:

a. Penggunaan teknik heuristik untuk role mining
b. Implementasi agen cerdas dalam pengelolaan akses
c. Integrasi semantik bisnis dalam definisi peran

DOI: 10.54259/satesi.v5i1.3997

4. Otomatisasi dan Efisiensi

[14] dan [16] mendemonstrasikan pentingnya otomatisasi dalam:

a. Evaluasi kebijakan RBAC
b. Deteksi inkonsistensi otorisasi
c. Penyesuaian dinamis terhadap perubahan kebutuhan bisnis

5. Tren Terkini dan Masa Depan RBAC dalam ERP

Berdasarkan analisis [17] dan [18], beberapa tren yang sedang berkembang meliputi:

a. Integrasi blockchain untuk meningkatkan transparansi
b. Penggunaan OAuth 2.0 untuk autentikasi yang lebih kuat
c. Implementasi machine learning dalam evaluasi akses

Implikasi Praktis

Hasil penelitian ini memiliki beberapa implikasi penting untuk implementasi RBAC dalam sistem ERP:

1. Kebutuhan Adaptasi:
   a. Organisasi perlu mengadopsi model RBAC yang lebih dinamis
   b. Pentingnya evaluasi berkala terhadap kebijakan akses
   c. Integrasi dengan teknologi keamanan terkini
2. Pertimbangan Implementasi:
   a. Evaluasi infrastruktur IT yang ada
   b. Pelatihan staf dalam manajemen akses
   c. Pengembangan prosedur audit keamanan
3. Rekomendasi Praktis:
   a. Implementasi bertahap model RBAC yang adaptif
   b. Penggunaan tools otomatisasi untuk evaluasi kebijakan
   c. Integrasi dengan sistem keamanan yang ada

3.4 Analisis Mendalam Implikasi Praktis

1. Strategi Implementasi untuk Organisasi Berbagai Skala

a. Organisasi Skala Besar

Temuan dari [9] dan [13] memiliki implikasi signifikan bagi organisasi berskala besar yang mengelola sistem ERP kompleks. Organisasi ini sebaiknya:

1) Melakukan audit komprehensif terhadap struktur peran yang ada sebelum mengimplementasikan RBAC yang lebih dinamis
2) Mengadopsi pendekatan bertahap dengan prioritas pada sistem yang menangani data sensitif
3) Membentuk tim khusus untuk mengelola dan memantau implementasi RBAC
4) Mengalokasikan sumber daya untuk pelatihan berkelanjutan dan penyesuaian sistem

Menurut analisis dari implementasi yang telah dilakukan, organisasi berskala besar dapat mengharapkan periode adaptasi 6-12 bulan untuk melihat hasil optimal dari implementasi RBAC yang komprehensif.

b. UKM dan Startup

Untuk organisasi dengan sumber daya terbatas, penelitian [14] dan [18] menawarkan implikasi praktis sebagai berikut:

1) Memanfaatkan solusi RBAC berbasis cloud yang menawarkan fleksibilitas dan skalabilitas
2) Mengimplementasikan framework semi-otomatis untuk mengurangi beban administratif
3) Fokus pada area kritis bisnis terlebih dahulu (seperti data keuangan dan informasi pelanggan)
4) Mempertimbangkan solusi RBAC terintegrasi yang sudah tersedia dalam platform ERP yang mereka gunakan

2. Tantangan Implementasi dan Mitigasi

a. Resistensi Organisasi

Temuan [16] menunjukkan bahwa tantangan utama dalam implementasi RBAC sering bersifat organisasional, bukan teknis. Untuk mengatasi ini:

1) Melibatkan pemangku kepentingan dari berbagai departemen sejak tahap perencanaan
2) Mengembangkan strategi komunikasi yang jelas untuk menjelaskan manfaat keamanan dan efisiensi
3) Mengimplementasikan program "champion" di mana perwakilan departemen dilatih untuk mendukung adopsi
4) Melakukan evaluasi dampak secara berkala dan membagikan hasil positif dengan seluruh organisasi

b. Kompleksitas Teknis

Berdasarkan penelitian [12] dan [17], kompleksitas teknis dapat diatasi melalui:

1) Memanfaatkan teknik role mining untuk mengoptimalkan definisi peran
2) Menggunakan pendekatan modular sehingga komponen RBAC dapat diimplementasikan secara bertahap
3) Membangun jembatan antara sistem lama dan implementasi RBAC baru
4) Mengadopsi standar industri untuk memudahkan integrasi dan pemeliharaan

3. Implikasi Ekonomi dan ROI

Penelitian-penelitian yang dianalisis menunjukkan bahwa implementasi RBAC memiliki implikasi ekonomi yang signifikan:

DOI: 10.54259/satesi.v5i1.3997

a. Analisis Biaya-Manfaat

1) Investasi awal: Implementasi RBAC memerlukan investasi dalam infrastruktur, pelatihan, dan mungkin konsultasi eksternal
2) Penghematan jangka menengah: Seperti yang ditunjukkan oleh [11], otomatisasi dalam manajemen akses dapat mengurangi beban administratif sebesar 30-40%
3) Manfaat jangka panjang: Peningkatan keamanan mengurangi risiko pelanggaran data yang dapat menyebabkan kerugian finansial signifikan

b. Metrik ROI

Berdasarkan temuan dari berbagai studi, organisasi dapat mengukur ROI dari implementasi RBAC melalui:

1) Pengurangan waktu yang dibutuhkan untuk manajemen akses (30-60% berdasarkan temuan Thilakarathne & Wickramaaarachchi, 2018)
2) Penurunan insiden keamanan terkait akses yang tidak sah (hingga 45% menurut data yang dikutip oleh Walker et al., 2020)
3) Pengurangan waktu audit kepatuhan (dapat mencapai 50% menurut Mehra, 2024)
4) Peningkatan efisiensi operasional melalui pembagian tugas yang lebih jelas

4. Implikasi Kepatuhan dan Regulasi

Penelitian [15]) dan [9] memiliki implikasi penting terkait kepatuhan regulasi:

a. Regulasi Spesifik Industri

1) Sektor kesehatan: Implementasi RBAC yang sesuai dengan HIPAA/HITECH memerlukan penekanan pada privasi data pasien dan jejak audit
2) Sektor keuangan: Kepatuhan terhadap PCI DSS dan regulasi perbankan memerlukan segregasi tugas yang ketat dan kontrol akses berlapis
3) Sektor pendidikan: Perlindungan data siswa sesuai FERPA memerlukan model RBAC yang dapat membedakan akses berdasarkan peran pendidik vs administratif

b. Regulasi Lintas Wilayah

Implementasi RBAC juga harus mempertimbangkan regulasi privasi data regional seperti:

1) GDPR di Eropa: Memerlukan kemampuan untuk membatasi akses berdasarkan prinsip "need-to-know" dan menyediakan laporan lengkap tentang siapa yang mengakses data pribadi
2) CCPA/CPRA di California: Memerlukan transparansi dalam penggunaan data dan kemampuan untuk membatasi akses
3) PDPA di Indonesia: Memerlukan perlindungan data pribadi dengan kontrol akses yang jelas dan teraudit

5. Kerangka Evaluasi dan Penilaian Berkelanjutan

Berdasarkan temuan [16] dan [17], organisasi sebaiknya mengembangkan kerangka evaluasi RBAC yang meliputi:

a. Metrik Kinerja Utama

1) Tingkat false positive/negative dalam otorisasi akses
2) Waktu yang diperlukan untuk menyelesaikan permintaan perubahan akses
3) Jumlah insiden keamanan terkait konfigurasi RBAC yang tidak tepat
4) Tingkat kepatuhan terhadap kebijakan yang ditetapkan

b. Program Penilaian Berkelanjutan

1) Audit berkala (minimal setiap 6 bulan) untuk memastikan kesesuaian dengan kebutuhan bisnis yang berkembang
2) Pengujian penetrasi untuk mengidentifikasi kelemahan dalam implementasi RBAC
3) Simulasi skenario perubahan bisnis untuk menilai adaptabilitas kebijakan akses
4) Review dan penyesuaian struktur peran berdasarkan perubahan organisasi

6. Transfer Pengetahuan dan Pengembangan Kapasitas

Temuan penelitian memiliki implikasi penting bagi pengembangan sumber daya manusia:

a. Program Pelatihan

Pengembangan kurikulum pelatihan berbasis peran:

1) Pelatihan dasar untuk semua pengguna sistem
2) Pelatihan lanjutan untuk administrator sistem dan keamanan
3) Pelatihan khusus untuk manajer yang bertanggung jawab atas persetujuan akses

Sertifikasi internal untuk memastikan pemahaman kebijakan RBAC

b. Dokumentasi dan Berbagi Pengetahuan

1) Pengembangan dokumentasi komprehensif tentang implementasi RBAC
2) Pembentukan komunitas praktik internal untuk berbagi pengalaman dan pembelajaran
3) Kolaborasi dengan vendor ERP untuk memastikan pembaruan dan praktik terbaik

7. Adaptasi Terhadap Teknologi Mendatang

Berdasarkan tren yang diidentifikasi oleh [17] dan [18], organisasi perlu mempersiapkan adaptasi terhadap:

DOI: 10.54259/satesi.v5i1.3997

a. Teknologi Baru

1) AI dan Machine Learning: Mempersiapkan kebijakan RBAC yang dapat berinteraksi dengan sistem berbasis AI
2) IoT: Mengantisipasi perluasan parameter akses untuk perangkat IoT di lingkungan ERP
3) Edge Computing: Mengembangkan model RBAC yang dapat berfungsi dalam lingkungan terdistribusi

b. Perubahan Model Bisnis

1) Remote Work: Menyesuaikan RBAC untuk mendukung akses jarak jauh yang aman
2) Digital Transformation: Memastikan RBAC mendukung inovasi dan agilitas bisnis
3) Kolaborasi Eksternal: Mengembangkan model untuk mengelola akses pihak ketiga dan mitra bisnis

Implikasi praktis ini memberikan kerangka komprehensif bagi organisasi untuk tidak hanya mengimplementasikan RBAC dengan sukses tetapi juga memaksimalkan nilai investasi keamanan mereka dalam jangka panjang. Dengan mempertimbangkan aspek-aspek ini, organisasi dapat mengembangkan strategi RBAC yang tidak hanya meningkatkan keamanan tetapi juga mendukung pertumbuhan bisnis dan adaptasi terhadap perubahan teknologi dan regulasi.

4. Kesimpulan

Role-Based Access Control (RBAC) terbukti sebagai solusi efektif dalam meningkatkan keamanan data pada berbagai sistem informasi modern, khususnya aplikasi Enterprise Resource Planning (ERP). Implementasi RBAC memungkinkan pengelolaan akses berbasis peran dengan tingkat efisiensi dan kepatuhan yang lebih tinggi terhadap regulasi. Studi menunjukkan bahwa integrasi teknologi seperti machine learning dan blockchain dapat memperluas kemampuan RBAC, misalnya dalam deteksi anomali dan pengelolaan kebijakan dinamis. Selain itu, otomatisasi dalam penerapan RBAC mengurangi waktu dan biaya operasional secara signifikan. Namun, tantangan seperti penyesuaian terhadap regulasi global yang kompleks, integrasi dengan lingkungan multi-domain, dan adaptasi ke sistem cloud membutuhkan perhatian khusus. Penerapan teknologi cerdas, pengembangan framework otomatisasi, dan penyesuaian kebijakan berbasis kebutuhan organisasi menjadi langkah kunci untuk optimalisasi RBAC.

Organisasi dapat mengoptimalkan implementasi RBAC pada sistem ERP mereka melalui beberapa langkah konkret. Pertama, melakukan audit keamanan berkala untuk mengevaluasi efektivitas model RBAC yang diterapkan dan mengidentifikasi celah keamanan. Kedua, mengembangkan program pelatihan komprehensif bagi pengguna dan administrator sistem untuk meningkatkan kesadaran keamanan dan pemahaman tentang kebijakan RBAC. Ketiga, menerapkan sistem manajemen identitas terpadu (Identity and Access Management) yang terintegrasi dengan ERP untuk mengotomatisasi proses pemberian dan pencabutan hak akses. Keempat, menjalankan simulasi pelanggaran keamanan secara berkala untuk menguji kehandalan sistem RBAC yang diterapkan. Kelima, membentuk tim khusus yang bertanggung jawab untuk memantau perkembangan regulasi keamanan data dan menyesuaikan kebijakan RBAC secara proaktif. Dengan menerapkan rekomendasi ini, organisasi dapat memaksimalkan manfaat dari RBAC sambil mengatasi tantangan implementasi yang ada.

Dengan adaptasi inovatif ini, RBAC tidak hanya meningkatkan keamanan, tetapi juga membangun fondasi yang kokoh bagi pengelolaan data yang lebih aman, efisien, dan berkelanjutan di era digital.

SUMBER RUJUKAN
Referensi

[1] H. Alrasyid, I. Istianah, Z. E. Marpaung, A. Indrijawati, and M. Irdam, "Implementasi Sistem ERP terhadap Kinerja Bisnis: Pendekatan Literatur Review," *J. Real Ris.*, vol. 6, no. 1, pp. 54–66, 2024, doi: 10.47647/jrr.

[2] Y. Yuricha and I. K. Phan, "Penerapan Role Based Access Control dalam Sistem Supply Chain Management Berbasis Cloud," *MALCOM Indones. J. Mach. Learn. Comput. Sci.*, vol. 3, no. 2, pp. 339–348, 2023, doi: 10.57152/malcom.v3i2.1259.

[3] Y. A. Prasetia and D. Manongga, "Role-based access control (rbac) untuk sistem otorisasi terpusat berbasis flask studi kasus pt. xyz," *JIPI (Jurnal Ilm. Penelit. dan Pembelajaran Inform.*, vol. 9, no. 4, pp. 1768–1778, 2024.

[4] M. Gratia, B. Sitorus, N. Maria, and Y. N. Safa, "Tinjauan Literatur Manajemen Risiko Cyber dalam Proyek : Identifikasi , Evaluasi , dan Mitigasi Ancaman," *J. Manaj. Inform.*, vol. 14, no. 2, pp. 187–198, 2024, doi: 10.34010/jamika.v14i2.12887.

[5] M. Jafar, A. M. I. T. Asfar, and A. M. I. A. Asfar, "Artificial Intellegence Dalam Pendidikan Dan Penelitian: Tantangan Dan Solusi Menghadapinya," *Simp. Nas. Kepemimp. Perguru. Tinggi Indones.*, vol. 1, no. 2017, pp. 1–9, 2024.

[6] H. Salsabila and I. P. Nasution, "ANALISIS DAMPAK REGULASI PRIVASI DATA TERHADAP MANAJEMEN KEMANAN DATA DI SEKTOR BISNIS," *Kinabalu*, vol. 11, no. 2, pp. 50–57, 2013.

[7] A. Purnomo, A. Kurniasih, A. Nuraminah, and S. Hartati, "Peran Artificial Intelligence dalam Deteksi Dini Ancaman Keamanan Jaringan," *J. Minfo Polgan*, vol. 13, no. 2, pp. 2044–2048, 2024, doi: https://doi.org/10.33395/jmp.v13i2.14356 e-ISSN.

[8] A. S. Khairi and M. Alda, "Implementasi Role Based Access Control dalam Pengelolaan Hak Akses Koperasi Berbasis Mobile," *Kec. Pancur Batu, Kab. Deli Serdang*, vol. 120, p. 6615683, 2024.

[9] T. Mehra, "The Critical Role of Role-Based Access Control (RBAC) in securing backup , recovery , and storage systems," *Int. J. Sci. Res. Arch.*, vol. 13, no. 1, pp. 1192–1194, 2024, doi: 10.30574/ijsra.2024.13.1.1733.

[10] S. T. Alshammari, A. Albeshri, and K. Alsubhi, "Integrating a high-reliability multicriteria trust evaluation model with task role-based access control for cloud services," *Symmetry (Basel).*, vol. 13, no. 3, 2021, doi: 10.3390/sym13030492.

[11] A. M. Abdul *et al.*, "Enhancing Security of Mobile Cloud Computing by Trust- and Role-Based Access Control," *Sci. Program.*, p. 10, 2022, doi: 10.1155/2022/9995023.

[12] C. Blundo, S. Cimato, and L. Siniscalchi, "Managing Constraints in Role Based Access Control," *IEEE Access*, vol. 8, pp. 140497–140511, 2020, doi: 10.1109/ACCESS.2020.3011310.

DOI: 10.54259/satesi.v5i1.3997

[13] R. Ghazal, A. K. Malik, N. Qadeer, B. Raza, A. R. Shahid, and H. Alquhayz, "Intelligent Role-Based Access Control Model and Framework Using Semantic Business Roles in Multi-Domain Environments," *IEEE Access*, vol. 8, pp. 12253–12267, 2020, doi: 10.1109/ACCESS.2020.2965333.

[14] N. N. Thilakarathne and D. Wickramaaarachchi, "Improved hierarchical role based access control model for cloud computing," *Int. Res. Conf. Smart Comput. Syst. Eng.*, 2018.

[15] A. U. R. Butt *et al.*, "An Optimized Role-Based Access Control Using Trust Mechanism in E-Health Cloud Environment," *IEEE Access*, vol. 11, no. November, pp. 138813–138826, 2023, doi: 10.1109/ACCESS.2023.3335984.

[16] A. Walker, J. Svacina, J. Simmons, and T. Cerny, "On Automated Role-Based Access Control Assessment in Enterprise Systems," *Lect. Notes Electr. Eng.*, vol. 621, pp. 375–385, 2020, doi: 10.1007/978-981-15-1465-4_38.

[17] A. Chatterjee, Y. Pitroda, and M. Parmar, "Dynamic Role-Based Access Control for Decentralized Applications," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 12404 LNCS, pp. 185–197, 2020, doi: 10.1007/978-3-030-59638-5_13.

[18] E. Mpamugo and G. Ansa, "Enhancing Network Security in Mobile Applications with Role-Based Access Control," *J. Inf. Syst. Informatics*, vol. 6, no. 3, pp. 1872–1899, 2024, doi: 10.51519/journalisi.v6i3.863.

[19] I. G. Susrama, Sugiarto, and W. Agustiono, *Buku Ajar Enterprise Resource Planning (ERP)*. 2021. [Online]. Available: https://www.researchgate.net/publication/358387687

[20] V. F. Nahuway, "Manajemen Perkantoran Modern Di Era Digitalisasi: Suatu Tinjauan Literatur," *J. Adm. Terap.*, vol. 3, no. 1, pp. 303–315, 2024.

DOI: 10.54259/satesi.v5i1.3997