KAMPUS AKADEMIK PUBLISING
Jurnal Ilmiah Penelitian Mahasiswa (JIPM)
Vol.4, No.2 April 2026
e-ISSN: 3025-5465, p-ISSN : 3025-7964, Hal 289-298
DOI : https://doi.org/10.61722/jipm.v4i2.2273

Implementasi Autentikasi dan Otorisasi pada Sistem Informasi Berbasis Web

Evan Adicandra[1], Yulindon[2], Ratna Dewi[3], Silfia Rifka[4]
Politeknik Negeri Padang
Limau Manis, Kecamatan Pauh, Kota Padang, Sumatra Barat, Indonesia, 25164
evancandraaaa@gmail.com[1]

Abstract. *The rapid development of web-based information systems demands security mechanisms capable of protecting data and effectively controlling user access. One of the main problems that often occurs is a weak authentication and authorization system, potentially leading to unauthorized access and data leaks. This research aims to design a security system model based on authentication and authorization for web-based information systems.The method used is a system design research approach, which includes requirements analysis, formulation of design principles, system architecture design, and development of authentication and authorization flows. The proposed system model applies the Role-Based Access Control (RBAC) concept to manage access rights, and hashing techniques to secure user passwords.The results show that the designed model can improve system security by separating authentication and authorization processes, limiting user access based on roles, and protecting login data from potential leaks. Furthermore, the use of session management on the backend helps maintain the stability of user access while interacting with the system.Thus, the proposed model can be a solution in improving the security of web-based information systems and can be used as a basis for developing a system that is more secure, structured, and easy to implement.*

Keywords: ***authentication, authorization, web security, information systems, role-based access control (RBAC)***

Abstrak. Perkembangan sistem informasi berbasis web yang semakin pesat menuntut adanya mekanisme keamanan yang mampu melindungi data dan mengontrol akses pengguna secara efektif. Salah satu permasalahan utama yang sering terjadi adalah lemahnya sistem autentikasi dan otorisasi, sehingga berpotensi menimbulkan akses tidak sah dan kebocoran data. Penelitian ini bertujuan untuk merancang model sistem keamanan berbasis autentikasi dan otorisasi pada sistem informasi berbasis web.Metode yang digunakan adalah pendekatan perancangan sistem (system design research) yang meliputi analisis kebutuhan, perumusan prinsip desain, perancangan arsitektur sistem, serta penyusunan alur autentikasi dan otorisasi. Model sistem yang diusulkan menerapkan konsep Role-Based Access Control (RBAC) untuk pengelolaan hak akses, serta teknik hashing untuk pengamanan password pengguna.Hasil penelitian menunjukkan bahwa model yang dirancang mampu meningkatkan keamanan sistem dengan memisahkan proses autentikasi dan otorisasi, membatasi akses pengguna berdasarkan peran, serta melindungi data login dari potensi kebocoran. Selain itu, penggunaan session management pada backend membantu menjaga stabilitas akses pengguna selama berinteraksi dengan sistem.Dengan demikian, model yang diusulkan dapat menjadi solusi dalam meningkatkan keamanan sistem informasi berbasis web serta dapat dijadikan sebagai dasar dalam pengembangan sistem yang lebih aman, terstruktur, dan mudah diimplementasikan.

Kata kunci: **autentikasi, otorisasi, keamanan web, sistem informasi, role-based access control (RBAC)**

LATAR BELAKANG

Perkembangan sistem informasi berbasis web semakin pesat dan digunakan dalam berbagai sektor seperti pendidikan, bisnis, dan layanan publik. Kemudahan akses dan

Naskah Masuk: 25 Maret 2026; Revisi: 28 Maret 2026; Diterima: 11 April 2026; ; Terbit: 11 April 2026

fleksibilitas yang ditawarkan menjadikan sistem berbasis web sebagai solusi utama dalam pengelolaan data dan layanan digital. Namun, peningkatan penggunaan ini juga diiringi dengan meningkatnya ancaman keamanan, terutama terkait akses tidak sah dan kebocoran data pengguna (Bucko, A., Vishi, K., Krasniqi, B., & Rexha, B., 2023). Salah satu permasalahan utama dalam sistem informasi berbasis web adalah lemahnya mekanisme autentikasi dan otorisasi. Banyak sistem masih menggunakan metode login sederhana tanpa pengelolaan hak akses yang jelas, sehingga berpotensi menimbulkan penyalahgunaan sistem (Trnka, M., Abdelfattah, A. S., Shrestha, A., Coffey, M., & Cerny, T., 2022). Selain itu, kurangnya pemisahan antara proses autentikasi dan otorisasi menyebabkan inkonsistensi dalam pengaturan hak akses pengguna. Autentikasi merupakan proses verifikasi identitas pengguna, sedangkan otorisasi menentukan hak akses pengguna terhadap sumber daya sistem. Kedua mekanisme ini menjadi komponen penting dalam menjaga keamanan sistem informasi modern (Bast, C., & Yeh, K. H., 2024). Pendekatan seperti Role-Based Access Control (RBAC) telah banyak digunakan untuk meningkatkan efisiensi dan keamanan dalam pengelolaan hak akses (Ayyagari, A., Jain, S., & Aggarwal, A., 2023). Selain itu, penggunaan teknik keamanan seperti hashing password dan token-based authentication juga menjadi praktik umum dalam sistem berbasis web untuk melindungi data pengguna (Dalimunthe, S., Putra, E. H., & Ridha, M. A. F., 2023). Penelitian sebelumnya menunjukkan bahwa penerapan mekanisme keamanan yang kuat pada sistem berbasis web, termasuk autentikasi yang baik, dapat mengurangi risiko serangan dan meningkatkan perlindungan data pengguna (Alzahrani, B. A., 2023). Berdasarkan permasalahan tersebut, penelitian ini bertujuan untuk merancang dan mengimplementasikan mekanisme autentikasi dan otorisasi pada sistem informasi berbasis web secara konseptual. Model yang diusulkan diharapkan mampu meningkatkan keamanan sistem serta memberikan struktur pengelolaan akses yang lebih jelas dan terkontrol.

KAJIAN TEORITIS

Sistem Informasi Berbasis Web

Sistem informasi berbasis web merupakan sistem yang memanfaatkan teknologi internet sebagai media utama dalam pengolahan dan penyampaian informasi. Sistem ini

memungkinkan pengguna untuk mengakses data dan layanan secara fleksibel melalui browser tanpa memerlukan instalasi aplikasi khusus. Penggunaan sistem berbasis web terus meningkat karena kemudahan akses, efisiensi operasional, serta kemampuan integrasi dengan berbagai layanan digital. Namun demikian, sistem berbasis web juga memiliki tantangan utama dalam aspek keamanan, terutama terkait perlindungan data dan pengendalian akses pengguna.

Konsep Keamanan Sistem Informasi

Keamanan sistem informasi bertujuan untuk melindungi data dan sumber daya sistem dari ancaman yang dapat mengganggu kerahasiaan, integritas, dan ketersediaan informasi. Ancaman terhadap sistem informasi dapat berupa akses tidak sah, pencurian data, maupun manipulasi informasi. Oleh karena itu, diperlukan mekanisme keamanan yang mampu mengontrol akses pengguna serta memastikan bahwa hanya pihak yang berwenang yang dapat mengakses sistem.

Autentikasi (Authentication)

Autentikasi adalah proses verifikasi identitas pengguna sebelum diberikan akses ke dalam sistem. Proses ini biasanya dilakukan melalui kombinasi username dan password, namun dapat dikembangkan menjadi metode yang lebih kompleks seperti multi-factor authentication (MFA). Autentikasi yang kuat sangat penting untuk mencegah akses tidak sah serta melindungi data pengguna dari potensi penyalahgunaan.

Otorisasi (Authorization)

Otorisasi merupakan proses penentuan hak akses pengguna terhadap sumber daya sistem setelah proses autentikasi berhasil dilakukan. Mekanisme ini memastikan bahwa setiap pengguna hanya dapat mengakses fitur atau data sesuai dengan peran dan kewenangannya. Salah satu metode yang umum digunakan adalah Role-Based Access Control (RBAC), di mana hak akses ditentukan berdasarkan peran pengguna dalam sistem.

Role-Based Access Control (RBAC)

RBAC adalah model pengendalian akses yang membagi pengguna ke dalam beberapa peran (role) dengan hak akses tertentu. Pendekatan ini mempermudah

pengelolaan hak akses karena tidak perlu mengatur izin secara individual untuk setiap pengguna. Selain itu, RBAC juga meningkatkan keamanan dan konsistensi dalam pengelolaan sistem karena setiap peran memiliki batasan akses yang jelas.

Teknik Keamanan Password

Salah satu aspek penting dalam autentikasi adalah pengamanan password. Password tidak disimpan dalam bentuk teks asli, melainkan menggunakan teknik hashing. Hashing merupakan proses mengubah data menjadi nilai unik yang tidak dapat dikembalikan ke bentuk semula. Teknik ini bertujuan untuk melindungi data pengguna apabila terjadi kebocoran database.

Multi-Factor Authentication (MFA) dan Two-Factor Authentication (2FA)

Perkembangan teknologi keamanan menunjukkan bahwa penggunaan satu lapisan autentikasi saja tidak cukup untuk melindungi sistem. Oleh karena itu, dikembangkan metode Multi-Factor Authentication (MFA) dan Two-Factor Authentication (2FA) yang menggabungkan beberapa metode verifikasi, seperti password dan kode OTP. Pendekatan ini terbukti mampu meningkatkan keamanan sistem secara signifikan dengan menambahkan lapisan perlindungan tambahan terhadap akses pengguna.

Token-Based Authentication

Token-based authentication merupakan metode autentikasi yang menggunakan token sebagai bukti identitas pengguna setelah proses login berhasil. Token ini digunakan untuk mengakses sistem tanpa perlu memasukkan ulang username dan password. Metode ini banyak digunakan pada aplikasi web modern karena lebih aman dan efisien dalam pengelolaan sesi pengguna.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan perancangan sistem (system design research) yang bertujuan untuk mengembangkan model autentikasi dan otorisasi pada sistem informasi berbasis web secara konseptual. Pendekatan ini menitikberatkan pada analisis kebutuhan, perancangan arsitektur sistem, serta penyusunan alur logika keamanan tanpa melibatkan pengujian empiris di lapangan.

Jenis dan Pendekatan Penelitian

Penelitian ini diklasifikasikan sebagai penelitian rekayasa sistem informasi (information system design research) dengan pendekatan konseptual. Pendekatan ini dipilih karena fokus penelitian adalah merancang model sistem keamanan berbasis autentikasi dan otorisasi yang dapat diterapkan pada berbagai jenis aplikasi web. Penelitian tidak melakukan pengumpulan data primer, melainkan mengacu pada studi literatur dan prinsip-prinsip keamanan sistem informasi modern.

Objek dan Ruang Lingkup Penelitian

Objek penelitian adalah sistem informasi berbasis web yang membutuhkan mekanisme pengamanan akses pengguna. Ruang lingkup penelitian meliputi :

- Perancangan sistem autentikasi pengguna (login system)
- Perancangan sistem otorisasi berbasis peran (Role-Based Access Control/RBAC)
- Pengamanan data pengguna menggunakan teknik hashing password
- Pengelolaan sesi pengguna (session management)

Penelitian ini tidak mencakup pengujian keamanan tingkat lanjut seperti penetration testing, enkripsi jaringan (SSL/TLS), maupun evaluasi performa sistem secara langsung.

Tahapan Metode Penelitian

A. Analisis Kebutuhan Sistem

Tahap ini dilakukan untuk mengidentifikasi kebutuhan sistem terkait mekanisme autentikasi dan otorisasi, serta potensi permasalahan keamanan seperti akses tidak sah dan kebocoran data.

B. Perumusan Prinsip Desain Sistem

Berdasarkan hasil analisis, ditentukan prinsip desain sistem yang meliputi pemisahan antara autentikasi dan otorisasi, penerapan Role-Based Access Control (RBAC), serta penggunaan teknik hashing untuk pengamanan password.

C. Perancangan Arsitektur Sistem

Sistem dirancang menggunakan arsitektur client-server yang terdiri dari frontend, backend, dan database, di mana backend berperan sebagai pusat pengolahan logika keamanan.

D. Perancangan Model Data

Tahap ini meliputi penyusunan struktur database yang mencakup tabel pengguna, peran (role), serta relasi antar data untuk mendukung pengelolaan hak akses.

E. Perancangan Alur Sistem

Dirancang alur proses sistem yang mencakup login, verifikasi data, pembuatan session, serta pembatasan akses berdasarkan peran pengguna.

F. Penyusunan Model Sistem Keamanan

Tahap akhir menghasilkan model sistem autentikasi dan otorisasi yang terstruktur, yang dapat dijadikan acuan dalam pengembangan sistem informasi berbasis web yang lebih aman.

HASIL DAN PEMBAHASAN

Bagian ini menyajikan hasil penelitian berupa model konseptual sistem autentikasi dan otorisasi pada sistem informasi berbasis web. Pembahasan difokuskan pada analisis struktur sistem, mekanisme keamanan, serta implikasi dari model yang diusulkan dalam meningkatkan keamanan akses pengguna.

Model Arsitektur Sistem Keamanan

Hasil utama penelitian ini adalah terbentuknya model arsitektur sistem keamanan berbasis pendekatan client-server yang terdiri dari tiga lapisan utama, yaitu frontend, backend, dan database. Dalam model ini, backend berfungsi sebagai pusat pengolahan logika keamanan, termasuk proses autentikasi, otorisasi, serta manajemen sesi pengguna. Pendekatan ini memberikan keuntungan berupa sentralisasi kontrol keamanan, sehingga seluruh keputusan terkait akses pengguna tidak dilakukan di sisi client, melainkan di server. Secara konseptual, hal ini mampu mengurangi risiko manipulasi data dari sisi pengguna serta meningkatkan integritas sistem.

Pemisahan Autentikasi dan Otorisasi

Temuan penting dalam penelitian ini adalah pemisahan yang jelas antara proses autentikasi dan otorisasi. Autentikasi hanya berfungsi untuk memverifikasi identitas pengguna, sedangkan otorisasi menentukan hak akses terhadap sistem. Pada banyak sistem konvensional, kedua proses ini sering digabungkan, sehingga menyebabkan

kompleksitas dalam pengelolaan akses. Dengan pemisahan ini, sistem menjadi lebih modular dan mudah dikembangkan. Selain itu, pendekatan ini memungkinkan peningkatan keamanan karena setiap proses memiliki fungsi yang spesifik dan terkontrol.

Implementasi Role-Based Access Control (RBAC)

Model yang diusulkan menerapkan konsep Role-Based Access Control (RBAC) sebagai mekanisme utama dalam pengaturan hak akses. Dalam implementasinya, setiap pengguna diklasifikasikan ke dalam peran tertentu, seperti admin dan user. Keunggulan utama RBAC adalah kemampuannya dalam menyederhanakan pengelolaan akses. Sistem tidak perlu mengatur izin secara individual untuk setiap pengguna, melainkan cukup berdasarkan peran. Secara konseptual, pendekatan ini meningkatkan efisiensi pengelolaan sistem serta mengurangi potensi kesalahan dalam pemberian hak akses. Selain itu, RBAC juga mendukung prinsip keamanan least privilege, di mana pengguna hanya diberikan akses sesuai kebutuhan, sehingga dapat meminimalkan risiko penyalahgunaan sistem.

Mekanisme Keamanan Password

Salah satu aspek penting dalam sistem ini adalah penggunaan teknik hashing untuk mengamankan password pengguna. Password tidak disimpan dalam bentuk teks asli, melainkan dalam bentuk hash yang dihasilkan melalui fungsi satu arah. Pendekatan ini memberikan perlindungan terhadap data pengguna apabila terjadi kebocoran database. Dalam kondisi tersebut, pihak yang tidak berwenang tidak dapat mengetahui password asli karena sifat hashing yang tidak dapat dibalik. Secara konseptual, penerapan hashing merupakan standar dalam sistem keamanan modern dan menjadi langkah fundamental dalam melindungi kredensial pengguna.

Alur Proses Autentikasi dan Manajemen Session

Alur autentikasi yang dirancang mencakup proses input data pengguna, verifikasi kredensial, serta pembuatan session setelah login berhasil. Session digunakan untuk menjaga status autentikasi pengguna selama berinteraksi dengan sistem. Penggunaan session memberikan efisiensi karena pengguna tidak perlu melakukan login ulang pada setiap permintaan akses. Namun demikian, sistem juga harus memastikan bahwa session dikelola dengan aman untuk mencegah serangan seperti session hijacking. Dalam model

ini, session dikelola oleh backend sehingga lebih aman dibandingkan jika disimpan di sisi client.

Mekanisme Otorisasi Berbasis Peran

Setelah proses autentikasi berhasil, sistem akan menjalankan mekanisme otorisasi dengan memeriksa peran pengguna. Setiap permintaan akses terhadap fitur sistem akan divalidasi berdasarkan hak akses yang dimiliki. Sebagai contoh, pengguna dengan peran admin dapat mengakses seluruh fitur sistem, sedangkan user hanya dapat mengakses fitur tertentu. Pendekatan ini memastikan bahwa setiap aktivitas pengguna berada dalam batasan yang telah ditentukan. Secara konseptual, mekanisme ini mampu mencegah akses tidak sah serta menjaga konsistensi pengelolaan sistem.

Analisis Keunggulan Model Sistem

Model sistem yang diusulkan memiliki beberapa keunggulan utama, antara lain:

- Keamanan yang lebih baik
  Dengan adanya autentikasi, otorisasi, dan hashing, sistem mampu mengurangi risiko akses ilegal.
- Struktur sistem yang terorganisir
  Pemisahan fungsi membuat sistem lebih mudah dipahami dan dikembangkan.
- Efisiensi pengelolaan pengguna
  RBAC mempermudah pengaturan hak akses tanpa perlu konfigurasi kompleks.
- Scalability
  Model ini dapat dikembangkan untuk sistem yang lebih besar dengan menambahkan peran atau fitur keamanan lainnya.

Keterbatasan dan Implikasi Penelitian

Meskipun model yang diusulkan memiliki berbagai keunggulan, penelitian ini masih memiliki keterbatasan karena bersifat konseptual dan belum dilakukan implementasi secara langsung. Oleh karena itu, efektivitas sistem dalam kondisi nyata belum dapat diukur secara kuantitatif. Namun demikian, model ini memberikan dasar yang kuat dalam pengembangan sistem keamanan berbasis web. Implikasi dari penelitian ini adalah bahwa penerapan autentikasi dan otorisasi yang terstruktur dapat meningkatkan keamanan

sistem serta mengurangi risiko serangan siber pada aplikasi berbasis web. Penelitian lanjutan disarankan untuk mengimplementasikan model ini dalam sistem nyata serta melakukan pengujian terhadap performa dan tingkat keamanannya.

KESIMPULAN DAN SARAN

Berdasarkan hasil perancangan dan pembahasan yang telah dilakukan, penelitian ini berhasil mengembangkan model sistem keamanan berbasis autentikasi dan otorisasi pada sistem informasi berbasis web. Model yang diusulkan menekankan pemisahan yang jelas antara proses autentikasi sebagai mekanisme verifikasi identitas pengguna dan otorisasi sebagai mekanisme pengaturan hak akses terhadap sistem. Pendekatan ini terbukti secara konseptual mampu meningkatkan struktur keamanan sistem serta meminimalkan potensi kesalahan dalam pengelolaan akses pengguna. Penerapan konsep Role-Based Access Control (RBAC) dalam model sistem memberikan kemudahan dalam pengelolaan hak akses karena setiap pengguna dikelompokkan berdasarkan peran tertentu. Dengan demikian, sistem dapat mengontrol akses secara lebih efisien dan konsisten tanpa perlu melakukan pengaturan izin secara individual. Selain itu, penerapan prinsip least privilege memastikan bahwa setiap pengguna hanya memiliki akses sesuai dengan kebutuhan, sehingga dapat mengurangi risiko penyalahgunaan sistem. Dari sisi keamanan data, penggunaan teknik hashing pada password menjadi salah satu komponen penting dalam melindungi informasi pengguna. Password yang disimpan dalam bentuk hash tidak dapat dikembalikan ke bentuk asli, sehingga mampu memberikan perlindungan tambahan terhadap kemungkinan kebocoran data. Mekanisme ini menunjukkan bahwa penerapan teknik keamanan dasar yang tepat dapat memberikan dampak signifikan dalam menjaga kerahasiaan data. Selain itu, pengelolaan sesi (session management) yang terpusat pada backend sistem juga berkontribusi dalam menjaga stabilitas dan keamanan akses pengguna. Dengan adanya session, sistem dapat mempertahankan status autentikasi pengguna selama proses interaksi berlangsung, sekaligus membatasi akses secara dinamis berdasarkan hak yang dimiliki.

Secara keseluruhan, model sistem yang dirancang dalam penelitian ini memiliki beberapa keunggulan utama, yaitu meningkatkan keamanan akses sistem, memberikan struktur pengelolaan pengguna yang lebih terorganisir, serta mendukung pengembangan sistem yang lebih scalable dan fleksibel. Model ini juga dapat dijadikan sebagai dasar

dalam pengembangan sistem informasi berbasis web yang lebih kompleks dengan penambahan fitur keamanan lanjutan seperti multi-factor authentication dan token-based authentication. Namun demikian, penelitian ini masih memiliki keterbatasan karena hanya berfokus pada perancangan konseptual tanpa implementasi dan pengujian secara langsung. Oleh karena itu, penelitian selanjutnya disarankan untuk mengembangkan model ini ke dalam bentuk sistem nyata serta melakukan evaluasi terhadap kinerja, keamanan, dan efektivitasnya dalam kondisi operasional. Dengan adanya pengujian empiris, model yang diusulkan dapat divalidasi lebih lanjut dan disempurnakan sesuai dengan kebutuhan sistem yang lebih kompleks. Dengan demikian, penelitian ini diharapkan dapat memberikan kontribusi dalam pengembangan sistem keamanan informasi berbasis web, khususnya dalam penerapan mekanisme autentikasi dan otorisasi yang terstruktur, aman, dan mudah diimplementasikan.

DAFTAR REFERENSI

Bucko, A., Vishi, K., Krasniqi, B., & Rexha, B. (2023). Enhancing JWT authentication and authorization in web applications based on user behavior history. *Computers*, 12(4), 78.

Trnka, M., Abdelfattah, A. S., Shrestha, A., Coffey, M., & Cerny, T. (2022). Systematic review of authentication and authorization advancements for the internet of things. *Sensors*, 22(4), 1361.

Bast, C., & Yeh, K. H. (2024). Emerging authentication technologies for zero trust on the internet of things. *Symmetry*, 16(8), 993.

Ayyagari, A., Jain, S., & Aggarwal, A. (2023). Innovations in multi-factor authentication: Exploring OAuth for enhanced security. *Innovative Research Thoughts*, 9(4), 254–267.

Dalimunthe, S., Putra, E. H., & Ridha, M. A. F. (2023). RESTful API security using JSON web token (JWT) with HMAC-SHA512 algorithm. *IT Journal Research and Development*, 8(1), 81–94.

Alzahrani, B. A., (2023). *Secure Authentication and Authorization for Web Applications Using Token-Based Mechanisms*.
Applied Sciences, 13(10), 6142.