SAKOLA - Journal of Sains Cooperative Learning and Law
E-ISSN: 3046-7179 P-ISSN: 3046-787X
Vol. 3 No. 1 April 2026

Implementasi Zero Trust Architecture pada Sistem Pengaduan Masyarakat Berbasis Web untuk Meningkatkan Keamanan Data dan Akses Pengguna

Dedy Kiswanto[1] Gerhard Hasangapon Parapat[2]
Fakultas Matematika dan Ilmu Pengetahuan Alam, Program Studi Ilmu Komputer, Universitas Negeri Medan, Medan, Indonesia[1,2]
Email: dedykiswanto@unimed.ac.id[1] parapatgerhard@gmail.com[2]

Abstrak

Sistem pengaduan masyarakat berbasis web memiliki peran penting dalam meningkatkan kualitas pelayanan publik serta transparansi informasi antara masyarakat dan pemerintah. Namun, permasalahan keamanan data dan akses pengguna masih menjadi tantangan utama, terutama terkait potensi kebocoran data dan penyalahgunaan akses. Oleh karena itu, penerapan konsep Zero Trust Architecture (ZTA) menjadi solusi untuk meningkatkan keamanan sistem melalui mekanisme verifikasi yang ketat. Penelitian ini bertujuan untuk mengimplementasikan dan menganalisis penerapan Zero Trust Architecture pada sistem pengaduan masyarakat berbasis web guna meningkatkan keamanan data dan kontrol akses pengguna. Metode penelitian yang digunakan adalah Research and Development (R&D) dengan tahapan analisis kebutuhan, perancangan arsitektur, implementasi sistem, dan pengujian keamanan. Sistem dikembangkan dengan fitur utama seperti registrasi, login dengan verifikasi OTP, pengaduan masyarakat, serta kritik dan saran, yang dilengkapi dengan mekanisme autentikasi dan otorisasi berbasis peran. Hasil penelitian menunjukkan bahwa penerapan Zero Trust Architecture mampu meningkatkan keamanan sistem melalui validasi berlapis, pembatasan akses, serta perlindungan data pengguna. Temuan ini diharapkan dapat menjadi solusi dalam pengembangan sistem pelayanan publik yang lebih aman, andal, dan terpercaya.
Kata Kunci: Zero Trust Architecture, Sistem Pengaduan, Keamanan Sistem, OTP, RBAC

Abstract

Web-based public complaint systems play an important role in improving public service quality and transparency between citizens and government institutions. However, data security and user access control remain major challenges, particularly regarding data breaches and unauthorized access. Therefore, the implementation of Zero Trust Architecture (ZTA) is proposed as a solution to enhance system security through strict verification mechanisms. This study aims to implement and analyze the application of Zero Trust Architecture in a web-based public complaint system to improve data security and user access control. The research method used is Research and Development (R&D), consisting of requirement analysis, architecture design, system implementation, and security testing. The system is developed with key features such as user registration, login with OTP verification, complaint submission, and feedback services, supported by authentication and role-based access control mechanisms. The results show that the implementation of Zero Trust Architecture significantly improves system security through layered validation, access restriction, and data protection. These findings provide a foundation for developing more secure, reliable, and trustworthy public service systems.
Keywords: *Zero Trust Architecture, Public Complaint System, System Security, OTP, RBAC*

PENDAHULUAN

Perkembangan teknologi informasi yang semakin pesat telah mendorong transformasi digital dalam berbagai sektor, termasuk pelayanan publik berbasis website. Pemanfaatan sistem berbasis web memungkinkan instansi pemerintah dalam meningkatkan kualitas layanan kepada masyarakat secara lebih efektif, transparan, dan efisien. Website pengaduan masyarakat menjadi salah satu solusi digital yang memungkinkan masyarakat menyampaikan

keluhan, saran, maupun laporan secara langsung tanpa harus datang ke instansi terkait. Namun, meningkatnya penggunaan sistem berbasis web juga diiringi dengan meningkatnya ancaman keamanan siber yang dapat membahayakan data pengguna serta integritas sistem pelayanan publik [1]. Ancaman keamanan pada sistem berbasis web semakin kompleks dengan adanya berbagai metode serangan seperti brute force attack, session hijacking, SQL injection, serta pencurian kredensial pengguna. Serangan tersebut dapat menyebabkan kebocoran data, manipulasi informasi, hingga gangguan terhadap layanan publik. Selain itu, model keamanan tradisional yang hanya mengandalkan perimeter jaringan dinilai tidak lagi efektif dalam menghadapi ancaman keamanan modern karena sistem saat ini dapat diakses dari berbagai perangkat dan lokasi yang berbeda [2], [3]. Seiring dengan meningkatnya ancaman keamanan tersebut, diperlukan pendekatan keamanan yang lebih modern dan adaptif. Salah satu pendekatan yang saat ini banyak digunakan adalah Zero Trust Architecture (ZTA). Konsep Zero Trust Architecture menerapkan prinsip "Never Trust, Always Verify" di mana setiap pengguna, perangkat, maupun akses jaringan harus diverifikasi terlebih dahulu sebelum diberikan hak akses ke sistem. Pendekatan ini memungkinkan sistem untuk meminimalisir risiko akses tidak sah dan meningkatkan keamanan data secara menyeluruh [4], [5]

Implementasi Zero Trust Architecture juga mencakup berbagai mekanisme keamanan seperti Multi-Factor Authentication, Role-Based Access Control, session management, serta monitoring aktivitas pengguna secara berkelanjutan. Penerapan Multi-Factor Authentication memungkinkan sistem untuk melakukan verifikasi identitas pengguna melalui lebih dari satu metode autentikasi, seperti kombinasi password, kode OTP, atau autentikasi berbasis perangkat. Pendekatan ini mampu mengurangi risiko akses tidak sah akibat pencurian kredensial pengguna. Selain itu, Role-Based Access Control memungkinkan sistem untuk mengatur hak akses berdasarkan peran pengguna, seperti admin, petugas, dan masyarakat umum, sehingga setiap pengguna hanya dapat mengakses fitur yang sesuai dengan tanggung jawabnya.[6], [7], [8] Session management juga berperan penting dalam implementasi keamanan sistem, khususnya dalam mengatur masa aktif sesi pengguna serta mencegah penggunaan kembali sesi yang telah kedaluwarsa. Misalnya, sistem dapat menerapkan session timeout otomatis dalam jangka waktu tertentu serta penggunaan token unik untuk setiap sesi login. Dengan demikian, risiko serangan seperti session hijacking dan unauthorized access dapat diminimalkan. Selain itu, monitoring aktivitas pengguna secara real-time memungkinkan sistem untuk mendeteksi aktivitas mencurigakan seperti percobaan login berulang, akses dari lokasi tidak dikenal, maupun perubahan data yang tidak wajar. Jika terdeteksi aktivitas mencurigakan, sistem dapat secara otomatis memblokir akses sementara atau mengirimkan notifikasi kepada administrator untuk dilakukan tindakan lebih lanjut [9], [10].

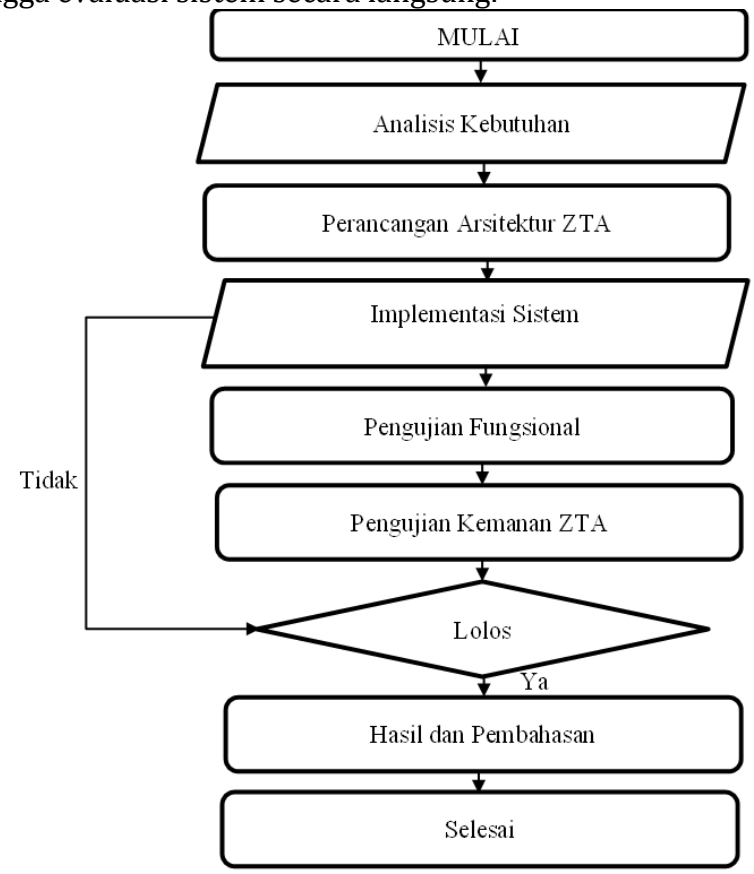
Selain itu, beberapa penelitian sebelumnya menunjukkan bahwa sistem pengaduan masyarakat berbasis web mampu meningkatkan efektivitas pelayanan publik dengan menyediakan media komunikasi yang lebih cepat, transparan, dan terstruktur antara masyarakat dan instansi pemerintah. Melalui sistem berbasis web, masyarakat dapat menyampaikan laporan secara langsung tanpa harus datang ke kantor terkait, sehingga proses pelayanan menjadi lebih efisien dan mudah diakses kapan saja. Namun demikian, sistem pengaduan berbasis web tersebut masih memiliki beberapa keterbatasan, khususnya dalam aspek keamanan data dan pengelolaan akses pengguna. Banyak sistem yang masih menggunakan metode autentikasi sederhana, kurangnya kontrol akses yang jelas, serta belum adanya monitoring aktivitas pengguna secara menyeluruh, sehingga berpotensi menimbulkan risiko kebocoran data maupun penyalahgunaan sistem [11], [12]

Selain itu, meningkatnya penggunaan layanan digital dalam pelayanan publik juga menyebabkan meningkatnya potensi ancaman keamanan siber seperti serangan phishing,

brute force attack, serta pencurian data pengguna. Oleh karena itu, diperlukan pendekatan keamanan yang lebih komprehensif dan adaptif terhadap ancaman modern. Konsep Zero Trust Architecture menjadi solusi yang relevan karena mengedepankan prinsip verifikasi berkelanjutan terhadap setiap permintaan akses tanpa menganggap bahwa pengguna dalam jaringan internal sepenuhnya aman. Dengan pendekatan ini, setiap akses pengguna akan melalui proses autentikasi dan otorisasi yang ketat sebelum diberikan izin untuk mengakses sistem.[13],[14] Berdasarkan permasalahan tersebut, penelitian ini bertujuan untuk mengembangkan sistem website pengaduan masyarakat dengan menerapkan Zero Trust Architecture guna meningkatkan keamanan sistem serta melindungi data pengguna secara menyeluruh. Pengembangan sistem ini tidak hanya berfokus pada peningkatan fitur layanan pengaduan, tetapi juga pada penerapan mekanisme keamanan berlapis yang mencakup autentikasi ganda, pengelolaan akses berbasis peran, manajemen sesi, serta pemantauan aktivitas pengguna secara real-time [15].

METODE PENELITIAN

Penelitian ini menggunakan pendekatan Research and Development (R&D) yang bertujuan untuk menghasilkan serta menguji suatu produk berupa sistem pengaduan masyarakat berbasis web dengan penerapan Zero Trust Architecture. Pendekatan ini dipilih karena tidak hanya berfokus pada analisis teori, tetapi juga pada proses perancangan, pengembangan, hingga evaluasi sistem secara langsung.



Gambar 1. Gambar Flochart Alur Kerja Sistem Pengaduan

Analisis Kebutuhan

Analisis kebutuhan dilakukan untuk mengidentifikasi persyaratan fungsional dan non-fungsional sistem. Kebutuhan fungsional mencakup: registrasi akun dengan verifikasi Mathematical CAPTCHA, login dua faktor dengan OTP via email, pembatasan percobaan login

(rate limiting), pembagian hak akses berbasis peran (user dan admin), serta fitur pengaduan dan pelacakan status aduan. Kebutuhan non-fungsional mencakup keamanan berlapis, keandalan sistem, dan kemudahan penggunaan oleh masyarakat umum.

Perancangan Arsitektur

Sistem dirancang dengan mengadopsi lima prinsip ZTA sesuai NIST SP 800-207 [8]: (1) Verify Explicitly—setiap login user memerlukan verifikasi dua faktor; (2) Use Least Privilege—role user dan admin memiliki akses berbeda melalui RBAC; (3) Assume Breach—rate limiting dengan maksimal 5 percobaan gagal sebelum lockout 15 menit; (4) Never Trust Network—setiap request API menyertakan Bearer JWT token; dan (5) Micro-segmentation—CAPTCHA memisahkan manusia dari bot pada registrasi.

Tabel 1. Technology Stack Sistem

Lapisan	Teknologi
Frontend	React.js + Vite + Tailwind CSS
HTTP Client	Axios + JWT Interceptor
Backend	PHP REST API (MySQL)
Auth Token	JWT Bearer Token
Email OTP	SMTP Mailer
CAPTCHA	Client-side Math

Implementasi Sistem

Sistem dikembangkan menggunakan React.js sebagai Single Page Application (SPA) dengan Vite sebagai build tool. Backend menggunakan PHP murni berbasis REST API dengan MySQL sebagai basis data. Implementasi mencakup tiga komponen keamanan ZTA utama yang akan dijelaskan pada bagian Hasil dan Pembahasan.

Pengujian Sistem

Pengujian dilakukan dengan dua pendekatan: (1) Pengujian Fungsional menggunakan metode Black Box Testing untuk memverifikasi seluruh fitur berjalan sesuai rancangan, dan (2) Pengujian Keamanan melalui simulasi skenario serangan (credential theft, brute force, bot registration) untuk mengevaluasi ketahanan mekanisme ZTA yang diimplementasikan [2].

HASIL PENELITIAN DAN PEMBAHASAN

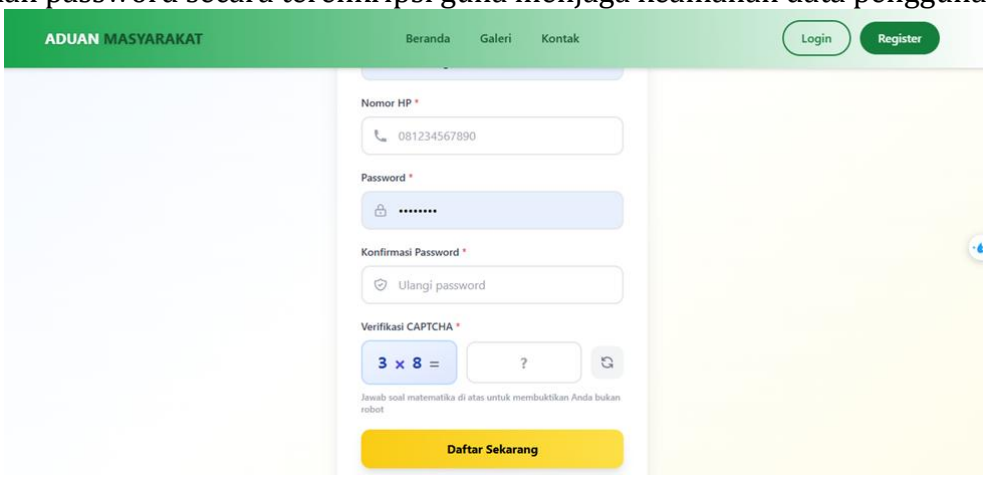
Implementasi Sistem

Implementasi sistem merupakan tahap penerapan hasil perancangan ke dalam aplikasi berbasis web. Sistem pengaduan masyarakat ini menggunakan konsep Zero Trust Architecture (ZTA) yang menekankan bahwa setiap akses harus diverifikasi terlebih dahulu tanpa adanya kepercayaan langsung, baik dari dalam maupun luar jaringan. Sistem dilengkapi dengan antarmuka yang sederhana, serta fitur autentikasi dan otorisasi untuk membatasi akses pengguna berdasarkan peran. Selain itu, keamanan sistem diterapkan melalui validasi input, enkripsi password, serta penggunaan CAPTCHA untuk mencegah akses bot. Data yang masuk disimpan dalam database secara aman sehingga dapat meningkatkan perlindungan terhadap data pengguna.

Implementasi Registrasi Akun

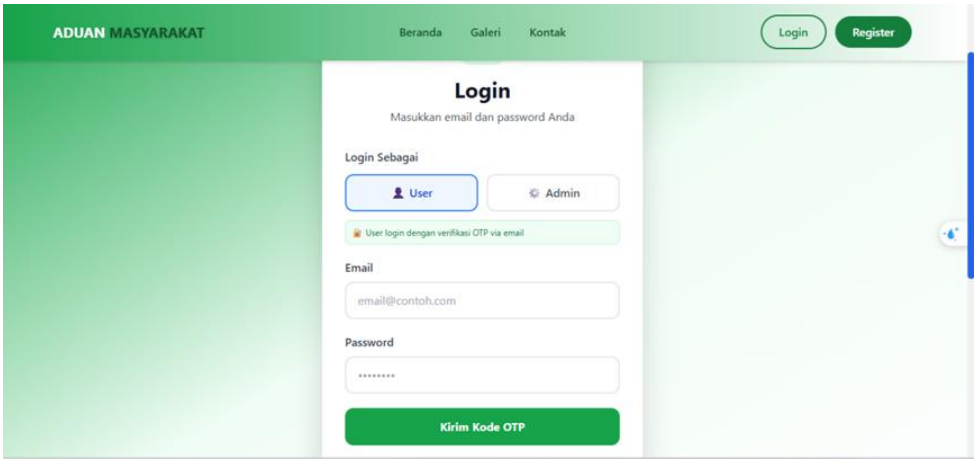
Fitur registrasi akun digunakan sebagai tahap awal bagi pengguna untuk mengakses sistem. Pengguna diminta mengisi data seperti nomor HP, password, konfirmasi password, serta CAPTCHA. Sistem akan melakukan validasi terhadap data yang diinput, termasuk kesesuaian password dan kebenaran CAPTCHA. Jika data valid, maka akun akan disimpan ke

dalam database dan pengguna dapat melakukan login. Penerapan Zero Trust pada proses ini terlihat dari adanya verifikasi ketat terhadap setiap input, penggunaan CAPTCHA, serta penyimpanan password secara terenkripsi guna menjaga keamanan data pengguna.



Gambar 1. Tampilan Halaman Registrasi

Login dan Verifikasi OTP



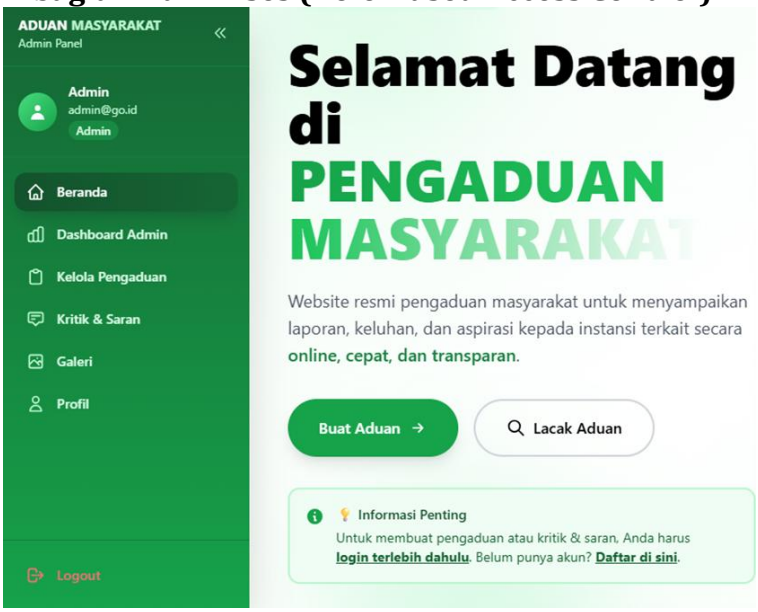
Gambar 2. Tampilan Halaman Login

Fitur login digunakan sebagai mekanisme autentikasi untuk memastikan bahwa hanya pengguna yang terdaftar yang dapat mengakses sistem. Pada halaman login, pengguna diminta memasukkan email dan password serta memilih peran sebagai user atau admin. Setelah data dimasukkan, sistem tidak langsung memberikan akses, melainkan mengirimkan kode One Time Password (OTP) ke email pengguna sebagai lapisan keamanan tambahan. Kode OTP ini bersifat sementara dan memiliki batas waktu penggunaan, sehingga dapat mencegah akses tidak sah.

Gambar 3. Tampilan Kode OTP Gmail

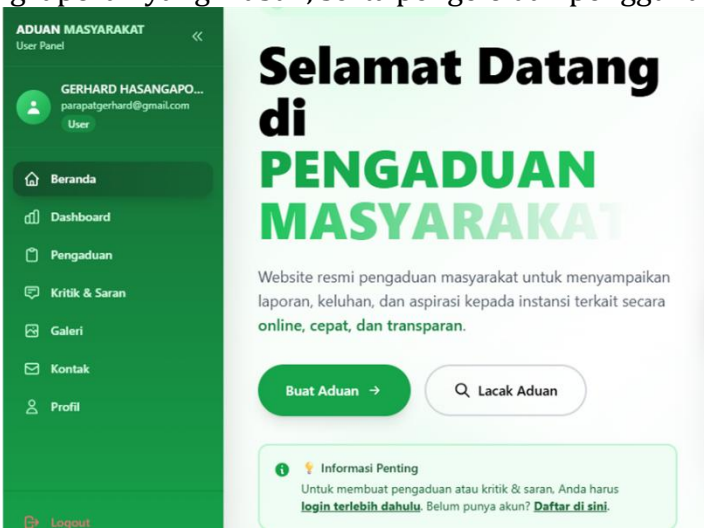
Berdasarkan Gambar 3, pengguna harus memasukkan kode OTP yang diterima melalui email untuk melanjutkan proses login. Jika kode yang dimasukkan sesuai, maka sistem akan memverifikasi identitas pengguna dan memberikan akses ke dalam sistem. Sebaliknya, jika kode salah atau telah kedaluwarsa, maka proses login akan ditolak. Penerapan OTP ini merupakan bagian dari konsep Zero Trust yang menekankan verifikasi berlapis untuk meningkatkan keamanan, sehingga meskipun password diketahui pihak lain, akses tetap tidak dapat dilakukan tanpa kode OTP yang valid.

Dashboard dan Pembagian Hak Akses (Role-Based Access Control)



Gambar 4. Tampilan Dashboard Admin

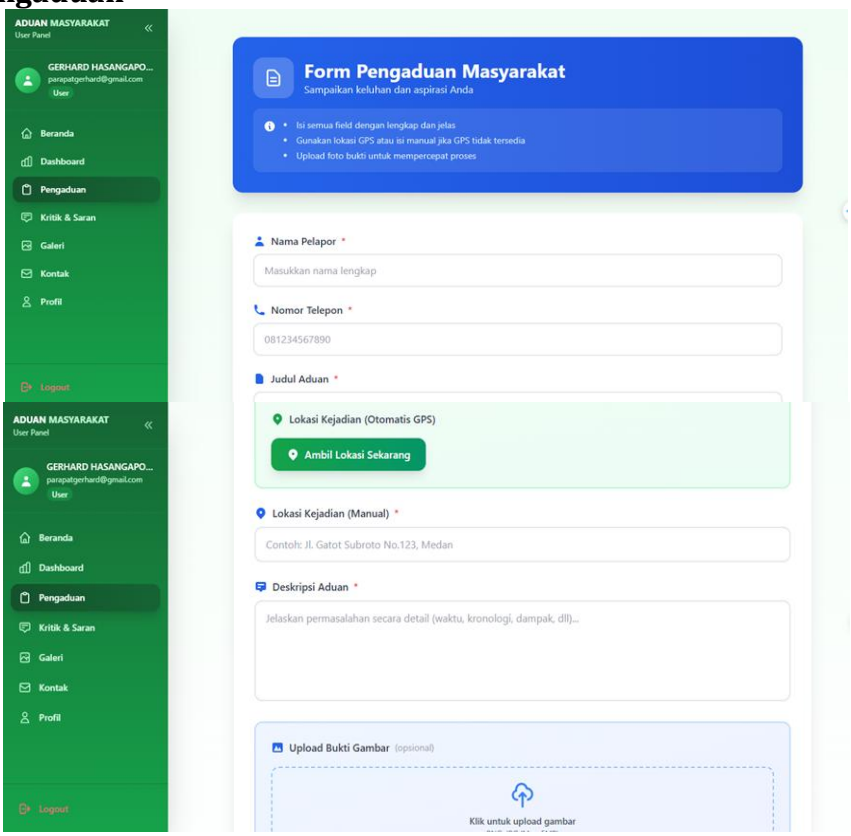
Dashboard merupakan halaman utama yang ditampilkan setelah pengguna berhasil login ke dalam sistem. Berdasarkan implementasi yang ditunjukkan pada gambar, terdapat perbedaan tampilan dashboard antara pengguna (user) dan admin sebagai bentuk penerapan Role-Based Access Control (RBAC). Pada dashboard user, fitur yang tersedia meliputi pembuatan pengaduan, melihat status laporan, mengakses kritik dan saran, serta melihat profil. Sementara itu, pada dashboard admin terdapat fitur tambahan seperti pengelolaan data pengaduan, monitoring laporan yang masuk, serta pengelolaan pengguna.



Gambar 5. Tampilan Dashboard User

Pembagian hak akses ini bertujuan untuk membatasi setiap pengguna agar hanya dapat mengakses fitur sesuai dengan perannya. Admin memiliki hak akses yang lebih luas untuk mengelola sistem, sedangkan user hanya dapat menggunakan fitur yang berkaitan dengan pengaduan. Dengan adanya RBAC, sistem dapat mencegah penyalahgunaan akses serta meningkatkan keamanan data. Konsep ini juga sejalan dengan Zero Trust Architecture, di mana setiap akses dikontrol dan diverifikasi berdasarkan identitas serta peran pengguna sebelum diberikan izin ke dalam sistem.

Mekanisme Pengaduan



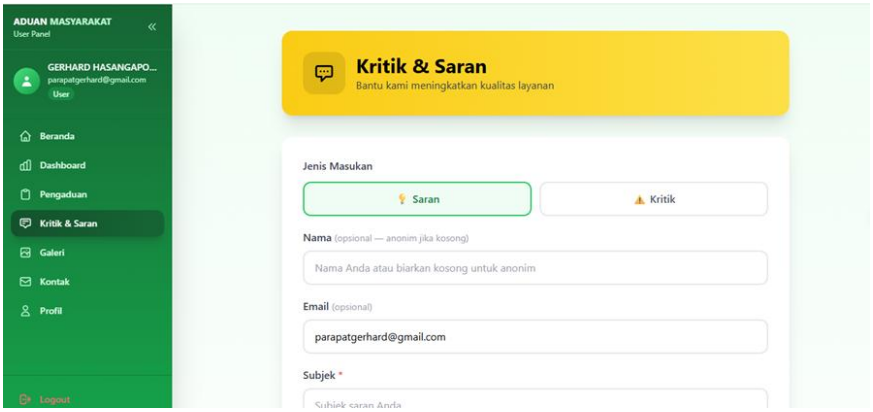
Gambar 6. Halaman Form Pengaduan User

Mekanisme pengaduan dalam sistem ini dirancang dengan menerapkan prinsip keamanan berbasis Zero Trust, di mana setiap pengguna harus melalui proses verifikasi sebelum dapat mengakses fitur pengaduan. Berdasarkan implementasi pada gambar tersebut, sistem pertama-tama melakukan pengecekan apakah pengguna sudah login atau belum. Jika pengguna belum login, maka sistem akan menolak akses dan mengarahkan pengguna untuk melakukan login terlebih dahulu. Selain itu, sistem juga membatasi akses berdasarkan peran pengguna, di mana admin tidak diperbolehkan membuat pengaduan karena fungsi tersebut hanya diperuntukkan bagi user sebagai masyarakat. Setelah pengguna lolos dari proses verifikasi, sistem akan menampilkan form pengaduan yang harus diisi secara lengkap. Form tersebut meliputi data seperti nama pelapor, nomor telepon, judul pengaduan, kategori, serta lokasi kejadian yang dapat diambil secara otomatis menggunakan GPS. Pengguna juga dapat menambahkan informasi pendukung seperti deskripsi dan bukti foto untuk memperkuat laporan yang disampaikan. Sistem memberikan panduan pengisian agar data yang dimasukkan lebih jelas dan valid. Setelah form diisi, pengguna dapat mengirimkan pengaduan dan sistem akan memproses serta menyimpan data ke dalam database. Jika pengaduan berhasil dikirim,

sistem akan menampilkan notifikasi keberhasilan beserta nomor pengaduan yang dapat digunakan untuk pelacakan. Sebaliknya, jika terjadi kesalahan, sistem akan menampilkan pesan error kepada pengguna. Seluruh proses ini menunjukkan bahwa setiap akses dan data yang masuk telah melalui validasi dan kontrol yang ketat, sehingga dapat meningkatkan keamanan serta keakuratan data dalam sistem pengaduan masyarakat.

Mekanisme Kritik dan Saran

Mekanisme kritik dan saran pada sistem ini dirancang untuk memberikan ruang bagi pengguna dalam menyampaikan masukan terhadap layanan yang tersedia. Berdasarkan implementasi pada kode program, sistem menyediakan form yang dapat digunakan untuk mengirimkan dua jenis masukan, yaitu kritik dan saran. Pengguna dapat memilih jenis masukan yang diinginkan, kemudian mengisi data seperti nama, email, subjek, dan isi pesan. Beberapa data seperti nama, email, dan nomor telepon dapat terisi otomatis dari penyimpanan lokal (localStorage) jika pengguna telah login sebelumnya, sehingga memudahkan proses pengisian form.



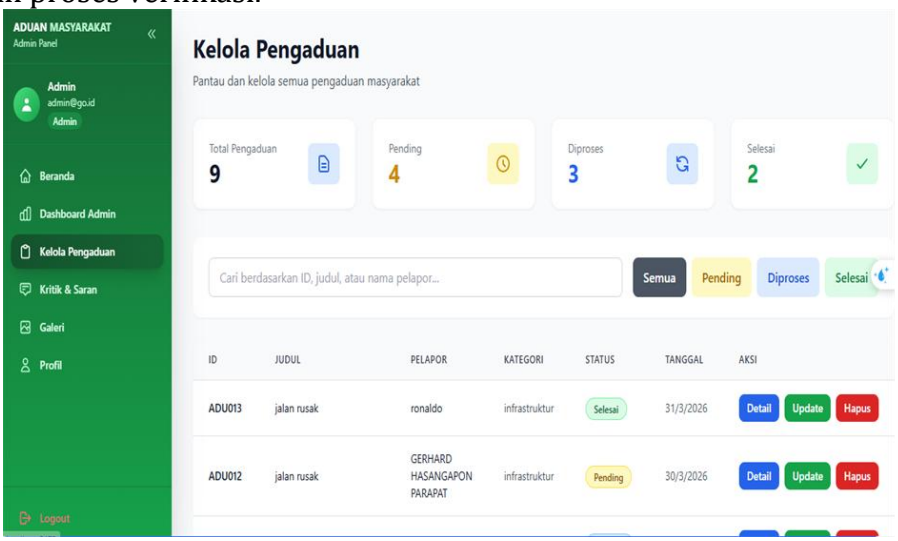
Gambar 7. Halaman Form Kritik & Saran User

Sistem juga mendukung pengiriman masukan secara anonim, di mana pengguna tidak wajib mengisi identitas pribadi. Saat form dikirim, sistem akan melakukan proses pengiriman data ke server melalui API, kemudian menampilkan notifikasi keberhasilan atau kegagalan berdasarkan hasil proses tersebut. Jika pengiriman berhasil, sistem akan menampilkan pesan sukses dan mengosongkan sebagian field untuk input berikutnya. Sebaliknya, jika terjadi kesalahan, sistem akan menampilkan pesan error kepada pengguna. Penerapan mekanisme ini juga mendukung prinsip Zero Trust, di mana setiap input tetap divalidasi sebelum diproses dan tidak langsung dipercaya. Dengan adanya fitur kritik dan saran ini, sistem tidak hanya berfungsi sebagai media pengaduan, tetapi juga sebagai sarana evaluasi untuk meningkatkan kualitas layanan secara berkelanjutan.

Pengelolaan Pengaduan oleh Admin

Pengelolaan pengaduan oleh admin merupakan tahap lanjutan setelah pengguna berhasil mengirimkan laporan melalui sistem. Berdasarkan implementasi yang ada, setiap data pengaduan yang dikirim oleh user akan disimpan ke dalam database melalui API dalam bentuk data terstruktur, termasuk informasi pelapor, judul, kategori, deskripsi, lokasi (GPS atau manual), serta bukti gambar jika tersedia. Setelah data tersimpan, admin dapat mengakses seluruh laporan melalui dashboard admin untuk dilakukan monitoring dan pengelolaan. Admin memiliki hak akses penuh dalam mengelola pengaduan, seperti melihat detail laporan, memverifikasi kebenaran informasi, serta memproses tindak lanjut dari setiap pengaduan yang masuk. Data lokasi yang dikirimkan, baik dalam bentuk koordinat GPS maupun alamat manual,

membantu admin dalam mengidentifikasi lokasi kejadian secara lebih akurat. Selain itu, adanya bukti gambar yang diunggah oleh pengguna dapat memperkuat validitas laporan sehingga mempermudah proses verifikasi.

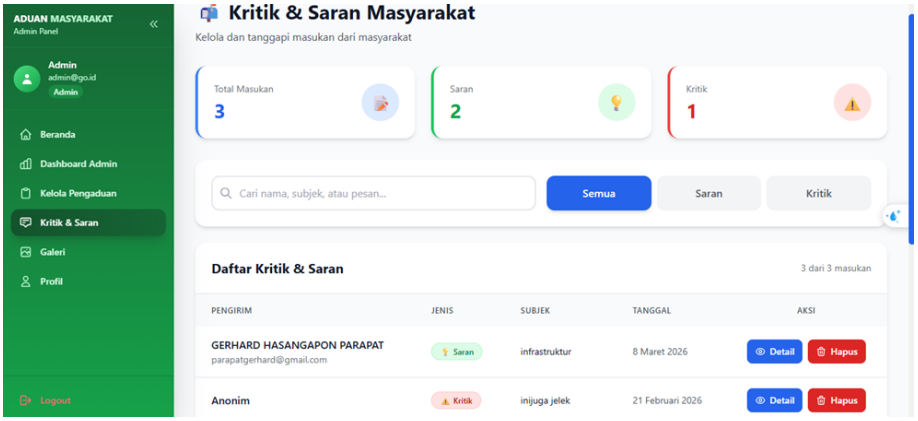


Gambar 8. Halaman Kelola Pengaduan Admin

Dalam proses pengelolaan, admin juga dapat menentukan status pengaduan, seperti diproses, selesai, atau ditolak sesuai dengan hasil verifikasi. Setiap perubahan status akan tersimpan dalam sistem sehingga dapat dipantau oleh pengguna melalui dashboard mereka. Mekanisme ini mendukung transparansi dan akuntabilitas dalam penanganan pengaduan masyarakat.Penerapan konsep Zero Trust pada sisi admin terlihat dari pembatasan akses yang hanya diberikan kepada pengguna dengan peran admin serta adanya kontrol terhadap setiap data yang masuk sebelum diproses lebih lanjut. Dengan demikian, sistem tidak hanya memastikan keamanan pada saat pengiriman pengaduan oleh user, tetapi juga pada tahap pengelolaan oleh admin, sehingga keseluruhan proses tetap terjaga keamanannya.

Pengelolaan Kritik dan Saran oleh Admin

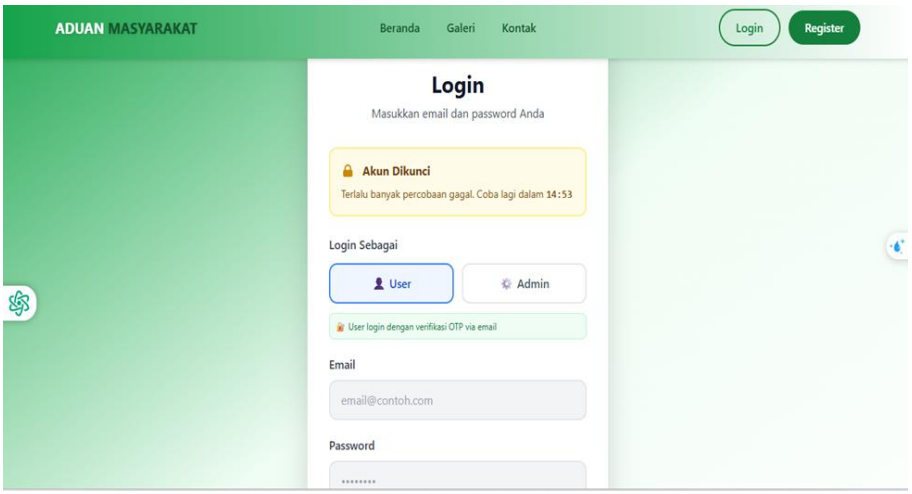
Pengelolaan kritik dan saran oleh admin merupakan tahap lanjutan setelah pengguna mengirimkan masukan melalui form yang tersedia. Berdasarkan implementasi sistem, data kritik dan saran yang dikirim oleh pengguna akan diteruskan ke server melalui API dan disimpan dalam database dengan informasi seperti nama (opsional), email, nomor telepon, jenis masukan (kritik atau saran), subjek, dan isi pesan. Sistem juga mendukung pengiriman secara anonim, sehingga admin tetap dapat menerima masukan tanpa identitas pengguna. Melalui dashboard admin, seluruh data kritik dan saran dapat ditampilkan dan dikelola secara terpusat. Admin dapat membaca isi masukan, mengelompokkan berdasarkan jenisnya, serta melakukan evaluasi terhadap kualitas layanan berdasarkan feedback yang diterima. Informasi yang telah terisi otomatis dari localStorage membantu meningkatkan kelengkapan data tanpa membebani pengguna, sehingga masukan yang diterima menjadi lebih informatif. Dalam proses pengelolaan, admin berperan dalam menganalisis, menindaklanjuti, serta menjadikan kritik dan saran sebagai bahan evaluasi untuk pengembangan sistem. Penerapan konsep Zero Trust tetap digunakan dengan memastikan bahwa hanya admin yang memiliki hak akses dapat melihat dan mengelola data tersebut. Selain itu, setiap data yang masuk tetap melalui proses validasi sebelum disimpan, sehingga keamanan dan integritas data tetap terjaga. Dengan adanya mekanisme ini, sistem tidak hanya berfungsi sebagai media pengaduan, tetapi juga sebagai sarana peningkatan kualitas layanan secara berkelanjutan.



Gambar 9. Halaman Kritik&Saran Admin

Implementasi Rate Limiting dan Account Lockout

Rate limiting diimplementasikan di sisi frontend menggunakan localStorage sebagai penyimpanan persisten. Pemilihan localStorage memastikan status lockout tetap aktif meskipun halaman di-refresh atau browser ditutup dan dibuka kembali—berbeda dengan pendekatan berbasis session yang hilang saat sesi berakhir. Hal ini mengimplementasikan prinsip ZTA Assume Breach secara lebih ketat.



Gambar 10. Halaman Dikunci dan Disertai Limit Waktu

Setiap kegagalan autentikasi menambah counter loginAttempts yang disimpan dalam format { attempts, lockoutUntil } di localStorage. Ketika jumlah percobaan mencapai MAX_ATTEMPTS (5 kali), sistem menerapkan lockout selama LOCKOUT_DURATION (900 detik / 15 menit) dengan menampilkan countdown timer real-time dan menonaktifkan seluruh form login. Sistem ini melengkapi fitur autoban yang diterapkan Purba dkk. [2] dengan pendekatan yang lebih ringan namun persisten

Tabel 2. Parameter Rate Limiting

Parameter	Nilai
Batas Percobaan	5 kali (MAX_ATTEMPTS)
Durasi Lockout	900 detik (15 menit)
Storage	localStorage browser
Persistensi	Bertahan saat refresh
Reset	Saat login berhasil
Cakupan	User & Admin

KESIMPULAN

Berdasarkan hasil penelitian dan implementasi sistem yang telah dilakukan, dapat disimpulkan bahwa penerapan Zero Trust Architecture (ZTA) pada sistem pengaduan masyarakat berbasis web mampu meningkatkan keamanan data dan kontrol akses pengguna secara lebih optimal. Sistem yang dikembangkan telah berhasil mengimplementasikan mekanisme autentikasi berlapis melalui login dan verifikasi OTP, serta pembagian hak akses menggunakan Role-Based Access Control (RBAC) antara user dan admin.Fitur utama seperti registrasi akun, pengajuan pengaduan, serta kritik dan saran telah berjalan dengan baik dan terintegrasi dengan sistem backend melalui API. Penggunaan validasi input, enkripsi password, serta pembatasan akses berdasarkan peran menunjukkan bahwa prinsip Zero Trust telah diterapkan secara efektif, di mana setiap akses tidak langsung dipercaya dan harus melalui proses verifikasi.Selain itu, sistem juga mampu memberikan kemudahan bagi pengguna dalam menyampaikan laporan dengan dukungan fitur seperti lokasi GPS, upload bukti gambar, serta notifikasi hasil pengaduan. Dari sisi admin, sistem mempermudah proses monitoring dan pengelolaan laporan sehingga meningkatkan efisiensi pelayanan. Dengan demikian, sistem yang dibangun tidak hanya berfungsi sebagai media pengaduan, tetapi juga sebagai solusi yang aman dan terpercaya dalam pengelolaan data masyarakat.

DAFTAR PUSTAKA

(1) Ramadhan, M. Fery Afrizal, and Asri Samsiar Ilmananda. "Analisis ancaman keamanan pada sistem informasi akademik kampus menggunakan metode OWASP ZAP." *vol* 8 (2024): 7985-7991

(2) Mukhlisin, Muhamad, and Rico Agung Firmansyah. "Zero Trust Architecture: Solusi Keamanan Dan Privasi Untuk Institusi Pendidikan, Systematic Literature Review." *JATI (Jurnal Mahasiswa Teknik Informatika)* 9.4 (2025): 6926-6935.

(3) Ananta, Wanda Vebya Ayu. "Keamanan Siber Pemerintah Dan Aspek Hukum Administrasi Negara: Tanggung Jawab Administratif Dalam Perlindungan Sistem Informasi Publik Di Era Digital." *Jurnal Atribusi Hukum* 1.1 (2025): 1-15.

(4) Darmawan, R. Wahyudi, Irawan Irawan, and Septa Petriansyah. "Analisis Adaptif Zero Trust Architecture (ZTA) Berbasis Machine Learning untuk Deteksi Intrusi pada Jaringan IoT dalam Infrastruktur Kritis." *RIGGS: Journal of Artificial Intelligence and Digital Business* 3.4 (2025): 36-45.

(5) Kusnanto, Y., Nugroho, M. A., & Kartadie, R. (2024). Implementasi Zero Trust Architecture untuk Meningkatkan Keamanan Jaringan: Pendekatan Berbasis Simulasi. *JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)*, *9*(4), 2357-2364.

(6) Ulah, Rizatul Mas, and I. Made Suartana. "Implementasi Session Management Pada Website Magang Menggunakan Teknologi MERN." *Journal of Informatics and Computer Science (JINACS)* 6.03 (2025): 765-777.

(7) Nabil, Muhammad, and Rakhmadi Rahman. "Analisis Keamanan Sistem Autentikasi Pengguna terhadap Serangan Session Hijacking." *International Journal Of Social Issues and Multidisiplinary Studies* 2.1 (2026): 111-115.

(8) Ramalinda, Dola, and A. R. Raharja. "Strategi Perlindungan Data Menggunakan Sistem Kriptografi Dalam Keamanan Informasi." *Journal of International Multidisciplinary Research. https://doi. org/10.62504/jimr679* (2024).

(9) Farahdiva, A. T., Mulyana, S. L., & Asri, T. P. (2025). Implementasi Cyber Security Pada Sistem Transaksi Keuangan Digital. *Jurnal Ilmiah Ekonomi, Manajemen, Bisnis Dan Akuntansi*, *2*(4), 276-289.

(10) Ramalinda, Dola, and A. R. Raharja. "Strategi Perlindungan Data Menggunakan Sistem Kriptografi Dalam Keamanan Informasi." *Journal of International Multidisciplinary Research. https://doi. org/10.62504/jimr679* (2024).
(11) Budiyanto, Deny, and Muhammad Mabruri. "Pentingnya Keamanan Siber Dalam Era Digital:: Tinjauan Global Dan Kondisi Di Indonesia." *Prosiding Seminar Nasional Sains dan Teknologi" SainTek"*. Vol. 2. No. 1. 2025.
(12) Alfi, Muhammad, Ni Putu Yundari, and Ahnaf Tsaqif. "Analisis risiko keamanan siber dalam transformasi digital pelayanan publik di Indonesia." *Jurnal Kajian Stratejik Ketahanan Nasional* 6.2 (2023): 5.
(13) Al-Hafiz, A. H. M. A. D. "Implementasi Zta Pada Website Aspirasi Kampus." *Jurnal Informatika dan Teknik Elektro Terapan* 14.1 (2026).
(14) Shabrina, A. N., Naila, G. S., Nuryansyah, G. P., & Amanda, R. (2025). Studi Kasus: Implementasi Sekuriti di Perusahaan. *Fibonacci: Jurnal Ilmu Ekonomi, Manajemen dan Keuangan*, *2*(1), 8-22.
(15) Ananta, Wanda Vebya Ayu. "Keamanan Siber Pemerintah Dan Aspek Hukum Administrasi Negara: Tanggung Jawab Administratif Dalam Perlindungan Sistem Informasi Publik Di Era Digital." *Jurnal Atribusi Hukum* 1.1 (2025): 1-15.