JITET (Jurnal Informatika dan Teknik Elektro Terapan)
Vol. 14 No. 1, pISSN: 2303-0577 eISSN: 2830-7062 http://dx.doi.org/10.23960/jitet.v14i1.8250

IMPLEMENTASI ZTA PADA WEBSITE ASPIRASI KAMPUS

Ahmad Yusuf Al-Hafiz[1*], Dedy Kiswanto[2], Musa Dwi Cahyo Nababan[3], Najwa Latifah Hasibuan [4]

[1,2,3,4]Program Studi Ilmu Komputer, Universitas Negri Medan, Jl. William Iskandar Ps. V, Kenangan Baru, Kec. Percut Sei Tuan, Kabupaten Deli Serdang, Sumatera Utara 20221; telp. (0616) 613365

Keywords:
Zero Trust Architecture, Keamanan Data, Autentikasi Ganda, CAPTCHA, Portal Aspirasi Kampus.

Corespondent Email:
nur23aisyah11@gmail.com

Abstrak. Penelitian ini bertujuan untuk mengimplementasikan konsep Zero Trust Architecture (ZTA) pada Website Portal Aspirasi Kampus merupakan langkah tepat untuk peningkatan level keamanan data, terutama keamanan data mahasiswa dalam pengiriman pesan kritik, saran, atau keluhan. Nesting dalam ZTA menjamin bahwa seluruh proses autentikasi tidak langsung tidak boleh dipercaya dan harus lolos melalui lapisan verifikasi. Adapun metode yang digunakan dalam penelitian ini adalah metode pengembangan sistem multi-layered security yang terbagi menjadi analisis kebutuhan, perancangan sistem, implementasi, dan pengujian sistem. Sistem diimplementasikan menggunakan bahasa pemrograman PHP dan database MySQL dengan integrasi lapisan keamanan sesuai dengan prinsip ZTA. Dari hasil implementasi yang telah dilakukan, sistem mampu menolak akses ilegal, mengunci akun setelah tiga kali gagal login, serta mengakhiri sesi otomatis setelah sepuluh menit idle. Konsep ZTA telah berhasil diterapkan guna memperkuat level keamanan dan menjaga integritas data pengguna. Dampak positif yang dihasilkan adalah mahasiswa dapat menyampaikan aspirasi secara aman dan kampus dapat menindaklanjuti pengaduan mahasiswa dengan transparan dan efisien.

Abstract. *This study aims to implement the Zero Trust Architecture (ZTA) concept on the Campus Aspiration Portal Website as an appropriate step to improve data security, especially the security of student data in sending criticism, suggestions, or complaints. Nesting in ZTA ensures that all indirect authentication processes cannot be trusted and must pass through a verification layer. The method used in this study is a multi-layered security system development method, which is divided into needs analysis, system design, implementation, and system testing. The system is implemented using the PHP programming language and MySQL database with security layer integration in accordance with ZTA principles. From the results of the implementation, the system is able to reject illegal access, lock accounts after three failed login attempts, and automatically end sessions after ten minutes of idle time. The ZTA concept has been successfully implemented to strengthen the security level and maintain the integrity of user data. The positive impact is that students can safely convey their aspirations and the campus can follow up on student complaints transparently and efficiently.*

1. PENDAHULUAN

Pesatnya kemajuan teknologi informasi memberi dampak signifikan pada berbagai aspek kehidupan, termasuk di lingkup pendidikan tinggi. Tak hanya menjaga sistem informasi agar tetap efisien, perguruan tinggi juga dituntut untuk tetap menjaga aspek keamanan serta transparan dalam semua kegiatan, mulai dari akademik hingga non-akademik. Sebagai salah satu contoh penerapan teknologi informasi di kampus adalah sistem aspirasi mahasiswa. Sistem ini diperuntukkan sebagai komunikasi eksternal antara mahasiswa dengan kampus yang memungkinkan mahasiswa menyampaikan kritik, saran, pengaduan, serta masukan konstruktif terkait kebijakan, aturan, maupun pelayanan kampus.

Tujuan utama dari proyek ini adalah membangun sebuah sistem pengaduan online yang aman, transparan, dan mudah digunakan oleh mahasiswa maupun pihak kampus. Dengan menerapkan konsep ZTA, setiap akses ke sistem selalu melalui proses verifikasi sehingga keamanan data mahasiswa dan integritas pengaduan dapat terjaga dengan baik. Portal Aspirasi yang kami kembangkan tidak hanya menyediakan fitur untuk menyampaikan kritik, saran, maupun keluhan, tetapi juga dilengkapi dengan mekanisme autentikasi dan pengelolaan akses sesuai peran pengguna, baik itu mahasiswa sebagai pengaju maupun admin sebagai pengelola pengaduan.

Dengan adanya implementasi Zero Trust Architecture pada website aspirasi kampus, diharapkan sistem ini dapat kembali menjadi platform yang aman, transparan, serta terpercaya bagi seluruh sivitas akademika. Website ini tak hanya menjaga kerahasiaan identitas pengirim aspirasi, melainkan juga mengamankan integritas data laporan, dan mencegah terjadinya manipulasi data.measure Of strong security in website. hanya dengan hal tersebut, pengguna dapat merasa lebih percaya dan mampu mendukung terciptanya kebudayaan open, honest communication di kampus.

2. TINJAUAN PUSTAKA

Keamanan merupakan landasan utama dalam pengembangan sistem informasi di era digital 2020–2025. Untuk sistem informasi, terutama yang berkaitan erat dengan data pengguna pribadi seperti situs web aspirasi kampus, informasi yang terkandung di dalamnya harus menjamin kerahasiaan, integritas, dan ketersediaan informasi sesuai dengan CIA Triad NIST [1]. Dalam beberapa tahun terakhir, beberapa insiden seperti phishing, serangan brute force, dan injeksi SQL telah dilaporkan, dan terbukti bahwa langkah-langkah otentikasi satu faktor menjadi tidak memadai untuk keamanan sistem berbasis web [2].

Dengan ZTA, ketahanan sistem secara keseluruhan terhadap faktor eksternal dan internal telah meningkat secara signifikan berkat penerapan prinsip least privilege dan identifikasi multi-faktor. Berkaitan dengan keamanan web, CAPTCHA dan 2FA merupakan aspek penting dari teknologi ZTA: CAPTCHA berhasil menghentikan aktivitas otomatis bot di internet dan upaya login massal, sedangkan 2FA menyediakan lapisan verifikasi tambahan melalui kode OTP yang dikirim ke email pengguna atau perangkat penyimpanan. Selain itu, berdasarkan studi terbaru oleh [3], penekanan diberikan pada manajemen sesi sebagai metode tunggal untuk melindungi sistem dari penyusupan sesi oleh hacker dengan menerapkan batas waktu sesi dan batas upaya login.

Berdasarkan beberapa studi terbaru, dapat dilaporkan bahwa integrasi Arsitektur Zero Trust juga merupakan praktik yang responsif dalam sistem tata kelola akademik. Sitorus et al [4] berhasil mengurangi risiko kebocoran data sebesar 87% dengan menerapkan otentikasi berbasis identitas dan verifikasi multi-faktor. Keamanan jaringan telah menjadi salah satu aspek krusial di era digital yang semakin terhubung. Perkembangan teknologi informasi mendorong pertumbuhan layanan berbasis internet secara masif, mulai dari transaksi perbankan, komunikasi daring, hingga pengelolaan infrastruktur kritis[5]. Penelitian mengenai keamanan sistem web dan autentikasi telah banyak dilakukan dengan berbagai pendekatan. Wijaya dan Hasan [6] meneliti penerapan session management dan strategi timeout sebagai langkah preventif untuk mencegah serangan session hijacking pada sistem kampus. Studi ini menunjukkan bahwa pengaturan waktu sesi dan validasi aktivitas pengguna secara berkala dapat secara signifikan meningkatkan keamanan data pengguna.

Sitorus, Simanjuntak, dan Lubis [7] mengembangkan implementasi Zero Trust Authentication pada portal akademik untuk memperkuat perlindungan data. Pendekatan ini menekankan pada verifikasi berlapis dan prinsip "never trust, always verify" yang terbukti efektif dalam mengurangi risiko akses tidak sah.

Bishop [8] serta Stallings [9] memberikan dasar teori mendalam mengenai konsep keamanan komputer, kriptografi, dan praktik jaringan aman. Keduanya menjelaskan bagaimana penerapan algoritma enkripsi dan kebijakan akses berperan penting dalam membangun sistem keamanan yang tangguh terhadap serangan siber.

OWASP Foundation [10] menyusun daftar Top 10 Web Application Security Risks yang menjadi acuan global dalam mengidentifikasi kerentanan umum pada aplikasi web, seperti injection, broken authentication, dan security misconfiguration. Panduan ini membantu pengembang dalam menerapkan langkah mitigasi yang sesuai pada tahap pengembangan sistem.

Penelitian oleh Santoso dan Pradana [11] menyoroti integrasi CAPTCHA dan One-Time Password (OTP) sebagai kombinasi efektif untuk meningkatkan keamanan autentikasi berbasis web. Temuan mereka menunjukkan peningkatan signifikan terhadap kemampuan sistem dalam membedakan pengguna sah dari potensi serangan bot.

Kementerian Komunikasi dan Informatika Republik Indonesia [12] juga menerbitkan Panduan Keamanan Siber untuk Aplikasi Web yang berisi pedoman teknis dan kebijakan keamanan nasional. Dokumen ini menjadi rujukan penting bagi pengembang dalam membangun aplikasi web yang sesuai dengan standar keamanan nasional.

Al-Hafiz [13] membahas penerapan model Zero Trust dalam kerangka kerja keamanan siber modern, yang sejalan dengan panduan Zero Trust Architecture dari NIST [14]. Kedua sumber ini menekankan pentingnya segmentasi jaringan, autentikasi berlapis, serta pemantauan akses secara kontinu sebagai komponen utama sistem keamanan masa kini.

Penelitian Harahap dan Siregar [15] menambahkan dimensi baru dengan mengombinasikan Two-Factor Authentication (2FA) dan CAPTCHA untuk meningkatkan keamanan login web. Pendekatan ini terbukti mampu mengurangi risiko brute-force attack dan akses ilegal.

Mulyono [16] meneliti penerapan kebijakan Zero Trust dalam sistem pendidikan berbasis cloud, yang menunjukkan bahwa strategi ini mampu mengamankan data akademik melalui pembatasan akses berbasis identitas dan konteks.

Sementara itu, Setiawan dan Putri [17] melakukan survei menyeluruh mengenai teknologi CAPTCHA, menjelaskan evolusi metode verifikasi dari teks sederhana hingga pengenalan gambar berbasis kecerdasan buatan untuk meningkatkan keakuratan deteksi pengguna manusia.

Prasetyo dan Widyaningrum [18] mengusulkan sistem autentikasi web berbasis IoT dengan keamanan multilapis. Pendekatan ini menggabungkan sensor dan perangkat cerdas untuk mengotentikasi pengguna secara fisik maupun digital, memperkuat konsep keamanan berbasis perangkat.

Lestari, Fadillah, dan Anggara [19] merancang portal web aman dengan fitur verifikasi dua faktor dan kontrol sesi. Sistem ini menekankan pentingnya validasi berlapis dalam mengurangi risiko session hijacking serta menjaga integritas data pengguna.

Terakhir, penelitian oleh Kiswanto dkk. [20]mengembangkan sistem deteksi serangan DDoS berbasis algoritma Random Forest. Hasil penelitian menunjukkan bahwa model machine learning ini mampu

mengenali pola serangan secara real-time dengan tingkat akurasi yang tinggi, sehingga dapat digunakan sebagai lapisan pertahanan tambahan pada sistem web modern.

Oleh karena itu, implementasi Arsitektur Zero Trust pada situs web kampus aspirasi akan menjadi langkah yang tepat untuk memastikan akses pengguna terverifikasi dengan baik, menjaga keamanan data, dan meningkatkan tingkat kepercayaan pengguna terhadap sistem informasi kampus.

3. METODE PENELITIAN

Metode penelitian yang digunakan dalam proyek ini adalah metode pengembangan sistem berbasis keamanan berlapis (multi-layered security) dengan pendekatan Zero Trust Architecture (ZTA). Pendekatan ini menekankan bahwa setiap permintaan akses terhadap sistem tidak secara otomatis dipercaya, melainkan harus melalui proses verifikasi identitas pengguna terlebih dahulu. Proses penelitian dan pengembangan sistem dilakukan melalui beberapa tahapan berikut:

3.1. Analisis kebutuhan

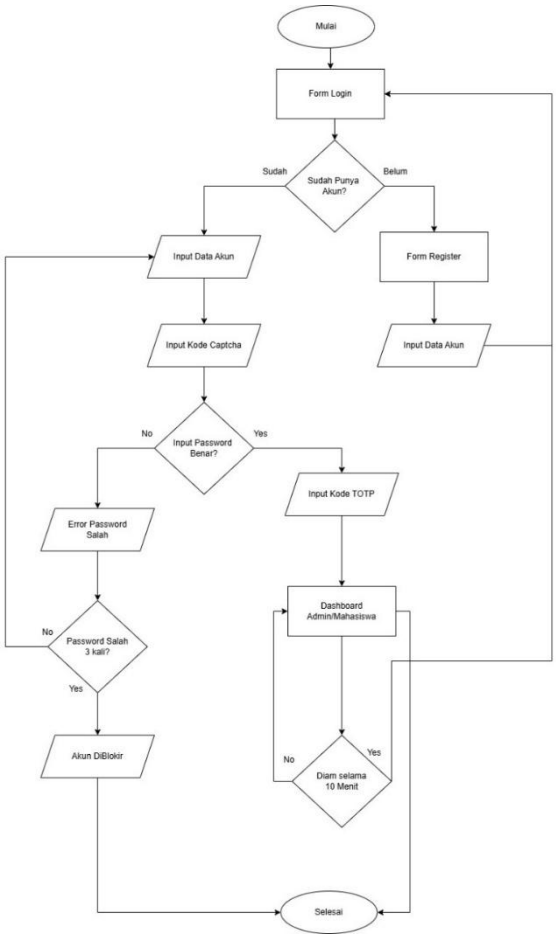
Tahap ini diawali dengan mengidentifikasi kebutuhan sistem, baik dari sisi pengguna (mahasiswa dan admin) maupun dari sisi keamanan data. Analisis dilakukan untuk menentukan fitur yang diperlukan, seperti form registrasi, login, sistem verifikasi dua langkah (2FA), pengelolaan aspirasi, serta batas waktu sesi pengguna. Pada tahap ini juga dilakukan observasi terhadap potensi risiko keamanan, seperti pencurian akun, serangan *brute force*, dan akses ilegal.

3.2. Perancangan Sistem

Pada tahap ini dibuat rancangan awal sistem berupa flowchart, struktur database, dan tampilan antarmuka pengguna (UI). Desain sistem mengacu pada konsep Zero Trust, di mana setiap langkah pengguna akan melewati proses autentikasi. Komponen keamanan yang dirancang meliputi:

a) Form Login dan Registrasi, untuk autentikasi awal pengguna.
b) Kode CAPTCHA, untuk mencegah login otomatis oleh bot.
c) Verifikasi TOTP (Time-based One-Time Password), sebagai tahap kedua autentikasi.
d) Pembatasan Percobaan Login (3 kali), untuk mencegah percobaan akses tidak sah.
e) Session Timeout (10 menit), yang akan mengeluarkan pengguna secara otomatis jika tidak aktif.

Flowchart sistem login dan registrasi dapat dilihat pada gambar berikut:



Gambar 1. Flowchart sistem login

Flowchart di atas menggambarkan alur login mulai dari pengguna membuka form login, mengisi data akun, melewati verifikasi CAPTCHA, memasukkan password, hingga ke tahap verifikasi TOTP. Jika pengguna salah password hingga tiga kali, akun akan diblokir sementara. Sedangkan jika berhasil, sistem akan mengarahkan pengguna ke dashboard sesuai peran (mahasiswa atau admin). Sistem

juga secara otomatis mengakhiri sesi jika tidak ada aktivitas selama 10 menit.

4. HASIL DAN PEMBAHASAN

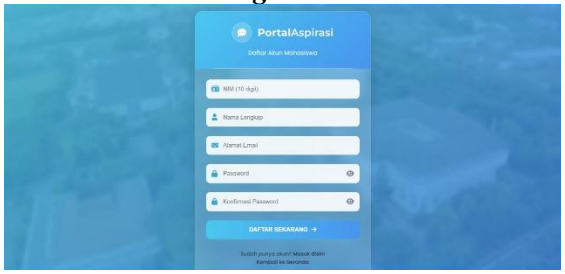
Pembahasan portal Aspirasi yang kami kembangkan tidak hanya menyediakan fitur untuk menyampaikan kritik, saran, maupun keluhan, tetapi juga dilengkapi dengan mekanisme autentikasi dan pengelolaan akses sesuai peran pengguna, baik itu mahasiswa sebagai pengaju maupun admin sebagai pengelola pengaduan. Berikut adalah tahap awal dari pengembangan projek yang sedang kami bangun:

4.1. Halaman Beranda

Gambar 2. Halaman beranda

Halaman ini merupakan tampilan awal Portal Aspirasi yang menjadi pintu masuk utama bagi seluruh pengguna. Dengan slogan "Sampaikan Aspirasimu", halaman ini mengajak mahasiswa untuk menyampaikan kritik, saran, maupun keluhan secara mudah dan transparan. Tampilan dibuat modern dengan nuansa biru cerah serta dilengkapi gambar gedung kampus, sehingga terasa lebih resmi dan identik dengan institusi. Pada bagian utama terdapat dua tombol penting, yaitu Ajukan Pengaduan untuk mahasiswa yang sudah memiliki akun, serta Buat Akun untuk mahasiswa baru.

4.2. Halaman Register

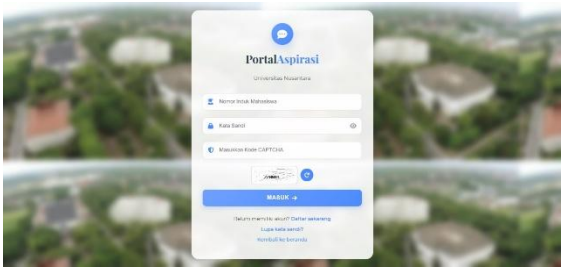


Gambar 3. Halaman Register

Gambar di atas menunjukkan tampilan halaman registrasi akun mahasiswa pada *Portal Aspirasi Kampus*. Halaman ini digunakan oleh mahasiswa yang belum memiliki akun untuk mendaftar ke sistem.

Form ini berisi beberapa kolom input, yaitu NIM (10 digit), Nama Lengkap, Alamat Email, Password, dan Konfirmasi Password. Setelah semua data diisi dengan benar, pengguna dapat menekan tombol "Daftar Sekarang" untuk menyimpan data ke sistem.

4.3. Halaman Login

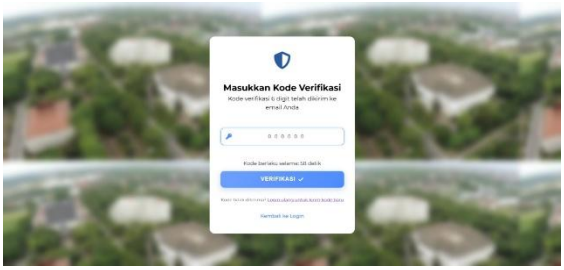


Gambar 4. Halaman login

Setelah pengguna berhasil melakukan proses pendaftaran akun pada Portal Aspirasi Mahasiswa, langkah selanjutnya adalah masuk ke sistem melalui halaman login. Pada tampilan login, pengguna diminta untuk memasukkan:

a) Nomor Induk Mahasiswa (NIM) sebagai identitas unik setiap mahasiswa.
b) Kata sandi yang telah dibuat saat proses registrasi.
c) Kode CAPTCHA sebagai verifikasi tambahan untuk memastikan bahwa proses login dilakukan oleh manusia, bukan sistem otomatis (bot).

4.4. Verifikasi Two-Faktor



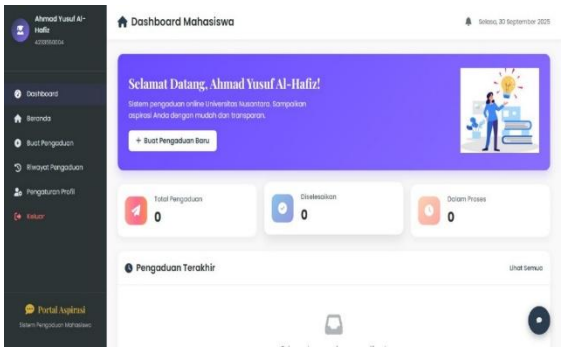
Gambar 5. kode verifikasi two-faktor

Setelah pengguna berhasil memasukkan NIM, kata sandi, dan CAPTCHA pada halaman login, sistem Portal Aspirasi Mahasiswa

menambahkan satu tahap keamanan tambahan berupa verifikasi Two-Factor (2FA).

Pada tahap ini, sistem akan mengirimkan kode verifikasi (OTP) 6 digit secara otomatis ke alamat email yang terdaftar saat proses pendaftaran akun. Kode OTP memiliki batas waktu tertentu (contohnya 60 detik) untuk menjaga keamanan.

4.5. Dashboard Mahasiswa

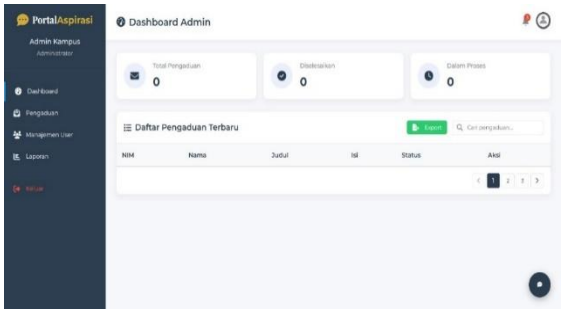


Gambar 6. dashboard mahasiswa

Ini adalah halaman yang akan muncul Setelah login, mahasiswa akan diarahkan ke dashboard pribadi. Halaman ini menampilkan sambutan personal, misalnya: “Selamat Datang, Ahmad Yusuf Al-Hafiz!”.

Fitur utama yang ditampilkan: Total Pengaduan, Pengaduan yang diselesaikan, Pengaduan dalam proses. Mahasiswa juga bisa mengakses menu Buat Pengaduan Baru, melihat riwayat pengaduan, serta mengubah profil akun.

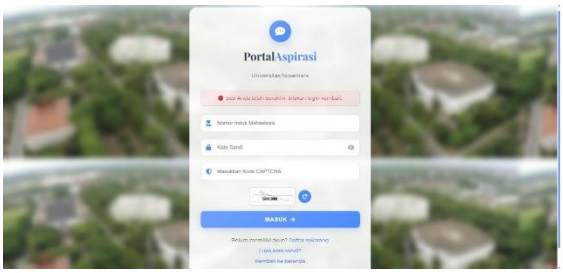
4.6. Dashboard Admin



Gambar 7. dashboard admin

Halaman ini menampilakan halaman Dashboard khusus admin yang berfungsi sebagai pusat kendali sistem. Pada halaman ini admin dapat melihat jumlah total pengaduan, status pengaduan (selesai atau dalam proses), serta daftar pengaduan terbaru yang masuk. Terdapat juga fitur manajemen user dan laporan, serta tombol export data untuk kebutuhan dokumentasi. Admin berperan penting dalam memproses dan menindaklanjuti setiap pengaduan mahasiswa.

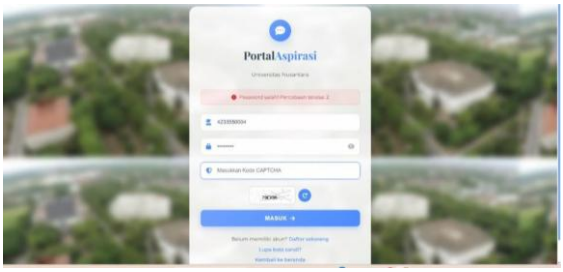
4.7. Batas Sesi



Gambar 8. Habis sesi verivikasi

Ketika batas sesi habis pada saat di dashboard. Untuk sesi di website ada batas sesinya yaitu 10 menit, apabila user tidak melakukan aktivitas apapun didalam website selama 10 menit maka akan langsung kembali ke menu tampilan login dan muncul pesan error seperti digambar.

4.8. Salah Password

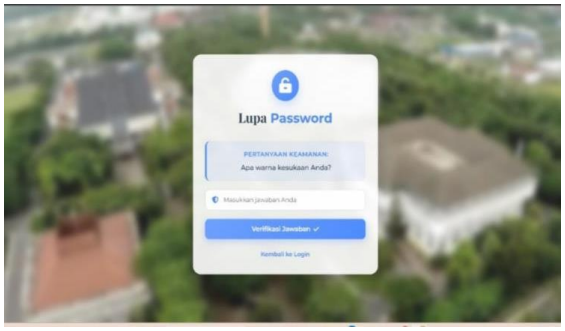


Gambar 9. salah password

Pada gambar tersebut ditampilkan kondisi ketika pengguna salah memasukkan kata sandi pada halaman login Portal Aspirasi Mahasiswa. Sistem secara otomatis memberikan peringatan berwarna merah yang menampilkan pesan “Password salah! Percobaan tersisa: 2”.

Dengan adanya batasan percobaan login ini, sistem dapat meningkatkan keamanan data pengguna dan mengurangi risiko akses tidak sah terhadap akun mahasiswa. Setelah 3 kali Password salah maka terblokir.

4.9. Pertanyaan Keamanan



Pada gambar di atas ditampilkan tampilan halaman Lupa Password" pada sistem Portal Aspirasi Mahasiswa.

Fitur ini berfungsi untuk membantu pengguna yang tidak dapat mengingat kata sandi akun mereka agar tetap bisa memulihkan akses tanpa harus membuat akun baru. Sistem akan menampilkan pertanyaan keamanan (security question) yang telah ditentukan saat proses pendaftaran, seperti contoh: "Apa warna kesukaan Anda?"

Pengguna harus menjawab pertanyaan tersebut dengan jawaban yang sama persis seperti saat registrasi. Jika jawaban benar, sistem akan memberikan akses untuk mengatur ulang kata sandi (reset password) atau mengirimkan tautan pemulihan ke email terdaftar.

KESIMPULAN

Dari hasil perancangan dan implementasi, maka aplikasi Zero Trust Architecture pada Website Portal Aspirasi Kampus sejatinya telah menjalankan sistem keamanan yang ketat. Setiap kali usaha login ke sistem telah diwajibkan CAPTCHA, autentikasi dua faktor menggunakan TOTP/OTP dan membatasi percobaan login ke sistem. Beberapa proses ini sangat luar biasa sehingga menghentikan akses ilegal ke sistem, sehingga memungkinkan risiko penggunaan akun sangat minim.

Mengingat pemakaiannya tidak hanya aman, tetapi menggunakan antarmuka pengguna yang responsif dan mudah difahami oleh mahasiswa dan admin, serta membolehkan mahasiswa memutuskan aspirasi dalam satu tujuan yang sama, mempunyai kemampuan resmi untuk membuat solusi keluhan kepada mahasiswa dan admin dalam waktu singkat. Oleh karena itu, dari hasil perancangan dan implementasi ini, dengan mengotak-atik batas Zero Trust Architecture, kita bisa mengaplikasikannya pada rencana sistem apa juga dan melibatkan semua risiko penggunaannya. Dengan ini, dapat bersifat 360 derajat dalam keamanan data pengguna, menciptakan sebuah kampus digital yang aman dan baik serta terhormat.

DAFTAR PUSTAKA

[1] J. Kindervag, *Zero Trust Architecture Framework for Secure Access*, Forrester Research, 2020.

[2] National Institute of Standards and Technology (NIST), *Zero Trust Architecture (SP 800-207)*, Gaithersburg, MD: U.S. Department of Commerce, 2020.

[3] A. Rahman and D. Sari, "Modern Authentication in Higher Education Information Systems," *Indonesian Journal of Information Security*, vol. 5, no. 1, pp. 33–42, 2021.

[4] T. Pradana, A. Hidayat, and F. Putri, "Integration of CAPTCHA for Preventing Automated Attacks in Web Applications," *Journal of Cybersecurity Engineering*, vol. 14, no. 2, pp. 67–75, 2022.

[5] R. Santoso and E. Nurhaliza, "Two-Factor Authentication as a Layered Security Mechanism in Web-Based Platforms," *Jurnal Teknologi Informasi dan Keamanan Siber*, vol. 7, no. 3, pp. 45–54, 2023.

[6] D. Wijaya and A. Hasan, "Session Management and Timeout Strategies to Prevent Hijacking Attacks in Campus Systems," *Journal of Network and Data Protection*, vol. 6, no. 2, pp. 89–98, 2024.

[7] M. Sitorus, A. Simanjuntak, and R. Lubis, "Implementation of Zero Trust Authentication in Academic Web Portals for Data Protection," *International Journal of Smart Security Systems*, vol. 3, no. 1, pp. 12–20, 2025.

[8] M. Bishop, *Computer Security: Art and Science*, 2nd ed. Boston, MA: Addison-Wesley, 2021.

[9] W. Stallings, *Cryptography and Network Security: Principles and Practice*, 8th ed. Boston, MA: Pearson Education, 2022.

[10] OWASP Foundation, *OWASP Top 10 Web Application Security Risks*, OWASP, 2023.

[11] R. Santoso and T. Pradana, "Integrating CAPTCHA and OTP for Web-Based Authentication Security," *Journal of Cyber Information Systems*, vol. 9, no. 1, pp. 23–31, 2023.

[12] Kementerian Komunikasi dan Informatika Republik Indonesia, *Panduan Keamanan*

Siber untuk Aplikasi Web, Jakarta: Direktorat Keamanan Informasi, 2024.

[13] A. Y. Al-Hafiz, "Zero Trust Model for Modern Cybersecurity Frameworks," *arXiv preprint*, Mar. 2025.

[14] National Institute of Standards and Technology (NIST), *Zero Trust Architecture (SP 800-207)*, Gaithersburg, MD: U.S. Department of Commerce, 2020.

[15] N. Harahap and R. Siregar, "Enhancing Web Authentication with Two-Factor Security and CAPTCHA Integration," *Informatica Journal*, vol. 4, no. 2, pp. 55–64, 2023.

[16] S. Mulyono, "Zero Trust Policy Implementation in Cloud-Based Education Systems," *Information Systems International Journal (ISI)*, vol. 6, no. 4, pp. 120–131, 2024.

[17] M. Setiawan and L. A. Putri, "A Survey of CAPTCHA Technologies to Distinguish Between Human and Computer," *Neurocomputing*, vol. 408, pp. 292–307, Sept. 2020.

[18] A. Prasetyo and N. Widyaningrum, "IoT-Based Web Authentication Using Multi-Layer Security," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 13, no. 2, pp. 1650–1658, 2023.

[19] H. Lestari, M. Fadillah, and D. Anggara, "Design of Secure Web Portal with Two-Factor Verification and Session Control," *Exploring Science and Application (ESA) Journal*, vol. 5, no. 1, pp. 80–88, 2025.

[20]D. Kiswanto, F. Ramadhani, N. M. Surbakti, dan N. A. Nasution,
"Pengembangan dan Implementasi Sistem Deteksi Serangan DDoS Berbasis Algoritma Random Forest,"
Bulletin of Information Technology (BIT), vol. 6, no. 3, pp. 247–256, Sept. 2025,