Jumistik
E-ISSN: 2964-3953 P-ISSN: 2964-3988
Jurnal Manajemen Informatika, Sistem Informasi dan Teknologi Komputer

Vol.4 No.2 Desember 2025
Hal 617-623
Https://ojs.amiklps.ac.id

IMPLEMENTASI *ZERO TRUST ARCHITECTURE* DENGAN *MULTI-FACTOR AUTHENTICATION* DAN *CONTINUOUS VERIFICATION* PADA SISTEM *LOGIN* BERBASIS *WEB*

Oka Alvansyah[1*], Dedy Kiswanto[2], Afifah Naila Nasution[3], M. Fikri Zulfi[4]
[1,2,3,4]Program Studi Ilmu Komputer, Jurusan Matematika, Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Negeri Medan
E-mail: okaalv3@gmail.com[1*], dedykiswanto@unimed.ac.id[2], afifahnaila90@gmail.com[3], fikrizulfi5@gmail.com[4]

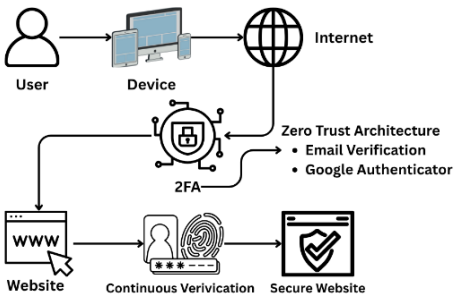
INFO ARTIKEL

Sejarah Artikel
Diterima : 21/10/2025
Direvisi : 03/11/2025
Diterbitkan : 01/12/2025

***Corresponding author**
okaalv3@gmail.com

DOI: 10.70247/jumistik.v4i2.220
Https://ojs.amiklps.ac.id

GRAPHICAL ABSTRACT



ABSTRACT

The rapid evolution of digital technology increases the demand for robust and adaptive cybersecurity frameworks. Traditional perimeter-based security models are no longer effective in addressing threats that exploit user sessions and internal network access. This study implements a Zero Trust Architecture (ZTA) model integrated with Multi-Factor Authentication (MFA) and Continuous Verification (CV) to strengthen authentication and authorization mechanisms in web-based login systems. The methodology involves five development phases, including layered authentication, least-privilege access control, continuous identity verification, and real-time activity logging based on the Assume Breach principle. The findings show that integrating MFA and CV improves resistance to credential theft and unauthorized access by enforcing continuous validation of user sessions. Moreover, the incorporation of activity logging enhances system visibility and accountability for security auditing. This research contributes a holistic framework for Zero Trust implementation that aligns with international cybersecurity standards and provides a reference model for future adaptive web security designs.

Keywords: *Zero Trust Architecture, Multi-Factor Authentication, Continuous Verification, Web Security*

ABSTRAK

Perkembangan teknologi digital yang pesat menuntut adanya kerangka keamanan siber yang adaptif dan berlapis. Model keamanan tradisional berbasis perimeter tidak lagi efektif dalam menghadapi ancaman yang mengeksploitasi sesi pengguna dan akses internal jaringan. Penelitian ini mengimplementasikan *Zero Trust Architecture* (ZTA) dengan integrasi *Multi-Factor Authentication* (MFA) dan *Continuous Verification* (CV) untuk memperkuat mekanisme autentikasi dan otorisasi pada sistem login berbasis web. Metode penelitian dilakukan melalui lima tahapan pengembangan, meliputi autentikasi berlapis, kontrol akses berbasis hak minimum, verifikasi identitas berkelanjutan, serta pencatatan aktivitas secara real-time berdasarkan prinsip *Assume Breach*. Hasil penelitian menunjukkan bahwa kombinasi *MFA* dan *CV* meningkatkan ketahanan sistem terhadap pencurian kredensial dan akses tidak sah melalui verifikasi sesi pengguna secara berkelanjutan. Selain itu, penerapan *activity logging* meningkatkan visibilitas dan kemampuan audit keamanan sistem. Penelitian ini memberikan kontribusi berupa kerangka implementasi *Zero Trust* yang komprehensif dan sesuai dengan standar keamanan global, serta dapat menjadi acuan dalam pengembangan keamanan web adaptif di masa depan.

Kata kunci: *Arsitektur Zero Trust, Multi-Factor Authentication, Continuous Verification, Assume Breach,* Keamanan Web

PENDAHULUAN

Keamanan sistem informasi menjadi pilar utama dalam pengembangan aplikasi berbasis web di era digital. Peningkatan interkoneksi antarperangkat, sistem cloud, serta mobilitas pengguna menimbulkan potensi risiko yang semakin besar terhadap keamanan data dan privasi pengguna [1]. Serangan siber seperti *phishing*, *brute-force*, dan *credential stuffing* menunjukkan bahwa model keamanan tradisional yang berfokus pada perimeter tidak lagi memadai dalam melindungi sistem dari ancaman internal maupun eksternal [1],[2]. Sebagai contoh konkret, penelitian mengenai simulasi serangan siber menunjukkan kerentanan jaringan terhadap serangan Man-in-the-Middle (MitM) melalui teknik ARP Spoofing [3]. Oleh karena itu, paradigma keamanan modern seperti *Zero Trust Architecture* (ZTA) menjadi solusi yang semakin relevan [4].

Zero Trust Architecture berprinsip pada "*Never Trust, Always Verify*", yang berarti setiap entitas baik pengguna, perangkat, maupun aplikasi harus diverifikasi secara terus-menerus sebelum diberikan akses ke sumber daya sistem [2],[3]. Tidak ada lagi zona aman internal, setiap permintaan akses dianggap berpotensi berbahaya hingga terbukti sah [5]. Dalam konteks sistem login berbasis web, pendekatan ini memerlukan penerapan autentikasi berlapis serta verifikasi berkelanjutan untuk mencegah eksploitasi sesi dan eskalasi hak akses.

Salah satu komponen penting dalam arsitektur Zero Trust adalah *Multi-Factor Authentication (MFA)*. *MFA* memastikan bahwa proses autentikasi tidak bergantung hanya pada satu faktor seperti kata sandi, tetapi menggunakan kombinasi faktor misalnya sesuatu yang diketahui (password), dimiliki (OTP token), dan melekat (biometrik) [8],[9],[10]. Penelitian terbaru menunjukkan bahwa penerapan *MFA* dapat menurunkan risiko kompromi akun hingga 80% dibandingkan metode autentikasi tunggal [8]. Namun, penerapan *MFA* saja belum cukup jika sistem tidak melakukan evaluasi berkelanjutan terhadap identitas pengguna selama sesi berlangsung.

Framework Laravel adalah sebuah framework PHP yang dirilis dibawah lisensi MIT, dibangun dengan konsep MVC (model view controller) [12].

Untuk itu, konsep *Continuous Verification (CV)* hadir sebagai pelengkap logis bagi *MFA* dalam kerangka *Zero Trust* [5]. *CV* bertujuan memastikan bahwa verifikasi identitas pengguna tidak berhenti setelah proses login, tetapi terus dilakukan sepanjang sesi aktif berdasarkan perilaku, konteks akses, serta parameter risiko seperti lokasi, perangkat, dan waktu aktivitas [5]. Dengan demikian, *CV* memungkinkan sistem untuk mendeteksi anomali perilaku secara real-time dan segera membatasi akses jika terdapat indikasi pelanggaran[7].

Implementasi Zero Trust dengan *MFA* dan *CV* pada sistem login berbasis web menjadi langkah strategis dalam memperkuat ketahanan keamanan. Kombinasi keduanya memberikan lapisan proteksi ganda: *MFA* sebagai gerbang autentikasi awal dan *CV* sebagai mekanisme pengawasan berkelanjutan selama sesi berjalan. Selain itu, sistem dapat diintegrasikan dengan mekanisme *activity logging* untuk mendukung prinsip *Assume Breach* yakni menganggap setiap aktivitas dapat berpotensi berbahaya dan perlu diawasi [14].

Penelitian mengenai kombinasi penerapan *MFA* dan *Continuous Verification* secara spesifik pada sistem login berbasis web masih terbatas, sehingga menjadi celah riset yang penting untuk dikembangkan.

Berdasarkan kondisi tersebut, penelitian ini berfokus pada implementasi *Zero Trust Architecture* menggunakan *Multi-Factor Authentication (MFA)* dan *Continuous Verification (CV)* pada sistem login berbasis web. Tujuan utama penelitian ini adalah:

Menerapkan arsitektur Zero Trust pada sistem login berbasis web untuk memastikan verifikasi identitas dan otorisasi akses yang aman, mengintegrasikan *Multi-Factor Authentication* sebagai lapisan autentikasi awal untuk mencegah akses tidak sah, menerapkan *Continuous Verification* untuk memastikan validitas identitas pengguna secara dinamis selama sesi aktif dan melakukan pemantauan dan pencatatan aktivitas autentikasi untuk mendukung prinsip *Assume Breach* dan audit keamanan sistem.

Penelitian ini diharapkan mampu memberikan kontribusi praktis dan akademik dalam pengembangan sistem keamanan web modern yang lebih tangguh, responsif terhadap ancaman, serta selaras dengan standar keamanan global berbasis *Zero Trust Architecture*.

TINJAUAN PUSTAKA

Penelitian-penelitian terdahulu telah menunjukkan bahwa penerapan *Zero Trust Architecture (ZTA)* menjadi paradigma penting dalam keamanan sistem informasi modern karena kemampuannya dalam mengatasi keterbatasan model keamanan tradisional berbasis perimeter. Menurut [5], pendekatan *Zero Trust* mampu meningkatkan ketahanan sistem terhadap serangan siber dengan menerapkan prinsip *Never Trust, Always Verify* dan *Assume Breach*. Meskipun demikian, implementasi menyeluruh dari prinsip tersebut masih menghadapi tantangan besar, terutama pada tahap integrasi dan verifikasi berkelanjutan.

Dakić [13] melakukan analisis penerapan arsitektur *Zero Trust* berbasis platform *Microsoft Azure* untuk organisasi menengah dan menemukan bahwa tantangan terbesar terletak pada tahap integrasi *MFA* dengan sistem manajemen identitas yang sudah ada. Penelitian tersebut menyoroti perlunya continuous verification agar autentikasi tidak berhenti setelah login awal, melainkan berlanjut sepanjang sesi.

Temuan ini diperkuat oleh Liu [6], yang dalam studinya tentang *Multi-Factor Authentication (MFA)* dalam *Zero Trust Architecture* menekankan pentingnya kombinasi *MFA* dengan *continuous session re-validation* untuk menurunkan risiko pencurian kredensial dan serangan session hijacking.

Reddy [14] menegaskan bahwa *Zero Trust* yang efektif harus mencakup proses continuous monitoring dan *activity logging* untuk mendukung prinsip *Assume Breach*, yakni menganggap setiap aktivitas berpotensi berbahaya dan perlu diawasi. Di sisi lain, Dalal [15] menambahkan bahwa salah satu tantangan utama dalam implementasi *ZTA* adalah bagaimana mengelola *logging* dan monitoring tanpa mengorbankan kinerja sistem. Ia menyarankan desain log adaptif yang hanya merekam aktivitas berisiko tinggi untuk efisiensi penyimpanan dan analisis.

Berdasarkan telaah pustaka tersebut, dapat disimpulkan bahwa terdapat celah riset (*research gap*) dalam integrasi holistik antara MFA, *Continuous Verification, dan activity logging* di dalam kerangka Zero Trust Architecture. Sebagian besar penelitian terdahulu hanya berfokus pada aspek tunggal seperti *MFA* atau *CV* tanpa mempertimbangkan penerapan keduanya secara simultan dan berkelanjutan pada sistem login berbasis web. Oleh karena itu, penelitian ini dilakukan untuk mengisi gap tersebut dengan merancang dan mengimplementasikan sistem keamanan login berbasis web yang menggabungkan *Multi-Factor Authentication, Continuous Verification,* dan *activity logging* untuk mendukung prinsip *Assume Breach* secara menyeluruh.

METODOLOGI PENELITIAN

Penelitian ini menerapkan metodologi pengembangan sistem yang berfokus pada implementasi keamanan berlapis secara iteratif. Pendekatan ini memastikan bahwa setiap komponen fungsionalitas dibangun di atas fondasi keamanan yang telah divalidasi terlebih dahulu, sejalan dengan prinsip-prinsip arsitektur *Zero Trust (ZTA)*. Alih-alih menganggap keamanan sebagai fitur tambahan, metodologi ini menjadikannya sebagai kerangka dasar dari keseluruhan arsitektur aplikasi.

Tahapan Penelitian

Proses penelitian dan pengembangan sistem dilaksanakan secara sekuensial melalui lima tahapan utama yang terstruktur, di mana setiap tahap memiliki tujuan spesifik yang berkontribusi pada arsitektur keamanan sistem secara keseluruhan.

Terdapat 5 fase dalam tahapan penelitian ini. Penelitian diawali dengan

Fase 1 Fondasi & Autentikasi Dasar

Fase ini bertujuan untuk membangun kerangka aplikasi dasar yang kokoh dan aman. Pada tahap ini, dilakukan serangkaian aksi fundamental seperti inisialisasi proyek menggunakan *Laravel Jetstream*, konfigurasi lingkungan dan database, implementasi fitur autentikasi standar, serta pengaktifan *Login Throttling* untuk mitigasi serangan *brute-force*.

Fase 2 Implementasi Prinsip Least Privilege

Fase ini bertujuan untuk memisahkan hak akses antar jenis pengguna dengan mengintegrasikan paket *spatie/laravel-permission* untuk menciptakan peran *Admin* dan *Customer* , serta membangun area khusus Admin yang dilindungi oleh middleware berbasis peran untuk membatasi akses.

Fase 3 Penguatan Verifikasi Identitas

Penguatan verifikasi identitas dilaksanakan dengan tujuan untuk memastikan identitas pengguna divalidasi melalui berbagai metode. Aksi yang dilakukan meliputi penerapan kewajiban Verifikasi Email saat pendaftaran, pengaktifan fitur opsional *2FA (TOTP)*, dan implementasi Pertanyaan Keamanan *(KBA)* sebagai faktor verifikasi sekunder yang wajib diatur saat registrasi.

Fase 4 Otorisasi Aksi Sensitif *(Step-up Authentication)*

Fase ini bertujuan menerapkan lapisan verifikasi tambahan untuk tindakan-tindakan berisiko tinggi di dalam aplikasi. Implementasi pada fase ini mencakup pembuatan sistem PIN Transaksi 6 digit , integrasi alur konfirmasi PIN sebelum setiap transfer dana, dan penggantian verifikasi password dengan verifikasi *KBA* untuk aksi-aksi sensitif di halaman profil.

Fase 5 Pengawasan & Monitoring

Pada fase ini didasari oleh prinsip *ZTA Assume Breach*. Tujuannya adalah untuk mencatat semua aktivitas penting untuk keperluan audit dan investigasi di kemudian hari. Hal ini dicapai dengan mengintegrasikan paket *spatie/laravel-activitylog*, mengkonfigurasi *logging* otomatis untuk semua event autentikasi dan transaksi, serta membangun antarmuka khusus bagi Admin untuk memantau log aktivitas secara global maupun per pengguna. Rincian setiap tahapan disajikan pada Tabel 1.

Tabel 1. Tahapan Penelitian dan Pengembangan Sistem

Tahap	Nama Tahapan	Deskripsi Aktivitas
1	Fondasi & Autentikasi Dasar	Membangun kerangka aplikasi dasar yang aman, termasuk inisialisasi proyek, konfigurasi, autentikasi standar, dan login throttling.
2	Implementasi Prinsip Least Privilege	Memisahkan hak akses dengan menciptakan peran Admin dan Customer, serta melindungi area khusus Admin menggunakan middleware.
3	Penguatan	Memastikan validitas identitas

	Verifikasi Identitas	pengguna melalui Verifikasi Email wajib, 2FA opsional, dan pengaturan KBA saat registrasi.
4	Otorisasi Aksi Sensitif	Menerapkan verifikasi tambahan (PIN dan KBA) untuk tindakan-tindakan berisiko tinggi seperti transfer dana dan perubahan data profil.
5	Pengawasan & Monitoring	Mencatat semua aktivitas penting (autentikasi dan transaksi) untuk keperluan audit dan membangun antarmuka monitoring bagi Admin.

Diagram Alir dan Perancangan Sistem

Gambar 1 menunjukkan diagram alir tahapan penelitian yang menggambarkan alur proses dari perancangan hingga analisis hasil. Diagram ini memberikan gambaran umum mengenai langkah-langkah utama yang dilakukan dalam penerapan dan evaluasi sistem berbasis Zero Trust Architecture (ZTA).

Gambar 1. Diagram Alir Tahapan Penelitian
Sumber: Proses Tahapan Penelitian

Langkah-langkah penelitian serta perancangan sistem divisualisasikan dalam bentuk diagram alir. Gambar 1 menunjukkan alur kerja penelitian secara menyeluruh, yang menggambarkan urutan logis dari setiap fase, mulai dari tahap awal hingga penyelesaian. Proses dimulai dengan studi literatur dan perancangan arsitektur, dilanjutkan dengan pengembangan sistem, serta pembangunan fondasi dan autentikasi. Tahap berikutnya mencakup implementasi *RBAC (Role-Based Access Control)* yang diikuti dengan penguatan verifikasi identitas dan otorisasi aksi sensitif untuk memastikan kontrol akses yang ketat. Setelah itu dilakukan implementasi monitoring guna memantau aktivitas sistem secara berkelanjutan. Selanjutnya, dilakukan pengujian fungsional dan keamanan untuk menilai kinerja sistem, kemudian hasilnya dianalisis dalam tahap analisis hasil dan validasi efektivitas *Zero Trust Architecture (ZTA)*. Seluruh rangkaian kegiatan diakhiri dengan tahap selesai setelah sistem dinyatakan efektif dan sesuai dengan tujuan penelitian.

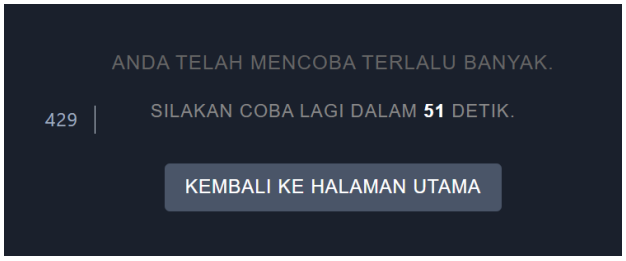
HASIL DAN PEMBAHASAN

Pada bagian ini, akan dipaparkan hasil dari setiap tahapan pengembangan sistem serta pembahasan mengenai bagaimana implementasi tersebut selaras dengan prinsip-prinsip arsitektur *Zero Trust (ZTA)*. Alur pembahasan mengikuti kerangka kerja penelitian yang telah disajikan pada diagram alir di bab metodologi.

Diagram alir pada Gambar 1 menggambarkan tahapan sistematis dalam proses penelitian yang dilakukan. Penelitian diawali dengan tahap Studi Literatur dan Perancangan Arsitektur, yang bertujuan untuk memperoleh dasar teoretis serta merancang kerangka kerja sistem yang akan dikembangkan. Selanjutnya dilakukan Pengembangan Sistem sebagai implementasi rancangan awal. Tahap berikutnya adalah Fondasi dan Autentikasi, yang menjadi dasar pengamanan sistem, kemudian dilanjutkan dengan Implementasi RBAC (Role-Based Access Control) untuk pengaturan hak akses pengguna. Setelah itu dilakukan Penguatan Verifikasi Identitas guna memastikan validitas autentikasi pengguna.

Fase 1: Implementasi Fondasi & Autentikasi

Sebagai fondasi awal, sistem dibangun menggunakan Laravel Jetstream yang secara inheren menyediakan mekanisme autentikasi dasar. Hasil dari tahap ini adalah sebuah sistem yang fungsional dengan fitur registrasi, login, dan logout. Lebih lanjut, untuk menerapkan pilar pertama ZTA yaitu Autentikasi Kuat, fitur *Login Throttling* diaktifkan. Pengujian menunjukkan bahwa sistem berhasil membatasi percobaan login sebanyak tiga kali; pada percobaan keempat, akses pengguna diblokir sementara selama 60 detik.



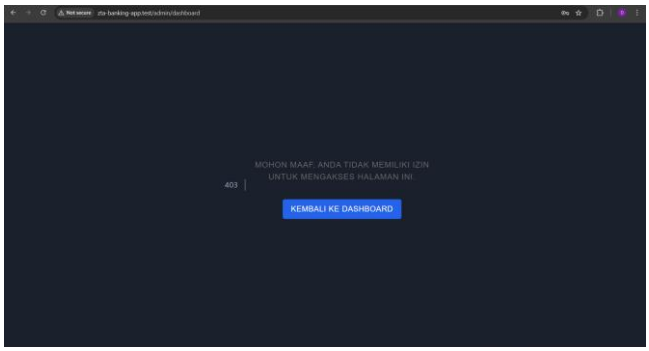
Gambar 2. Halaman Peringatan Akibat Percobaan Login Berlebih
Sumber: Hasil Pengujian

Pembahasan dari implementasi ini adalah bahwa sistem tidak serta-merta mempercayai permintaan login yang masuk. Dengan adanya throttling, sistem secara aktif memitigasi risiko serangan *brute-force*, yang merupakan langkah fundamental dalam memastikan bahwa hanya identitas yang sah yang dapat memulai sesi.

Fase 2: Implementasi Role-Based Access Control (RBAC)

Pada tahap ini, prinsip *ZTA* Hak Akses Minimum *(Least Privilege)* diimplementasikan. Hasil yang dicapai adalah terciptanya dua peran pengguna yang

berbeda, yaitu *Admin* dan *Customer*, menggunakan paket *spatie/laravel-permission*. Sebagai bukti implementasi, telah dibuat serangkaian rute dan halaman khusus Admin (seperti Dashboard Admin dan Manajemen User) yang dilindungi oleh *middleware* berbasis peran. Pengujian memvalidasi bahwa pengguna dengan peran *Customer* akan menerima respons *"403 Forbidden"* saat mencoba mengakses URL admin, membuktikan bahwa segmentasi akses telah berhasil diterapkan. Pembahasan dari fitur ini adalah bahwa sistem secara eksplisit membatasi ruang gerak setiap pengguna sesuai dengan kebutuhan mereka. Seorang pengguna biasa *(Customer)* tidak memiliki akses apa pun ke area administratif, sehingga jika akun mereka berhasil diretas, potensi kerusakan dapat diminimalisir secara signifikan karena penyerang tidak dapat mengakses fungsi-fungsi vital sistem.



Gambar 3. Halaman Penolakan Akses untuk Peran yang Tidak Sah
Sumber: Hasil Pengujian

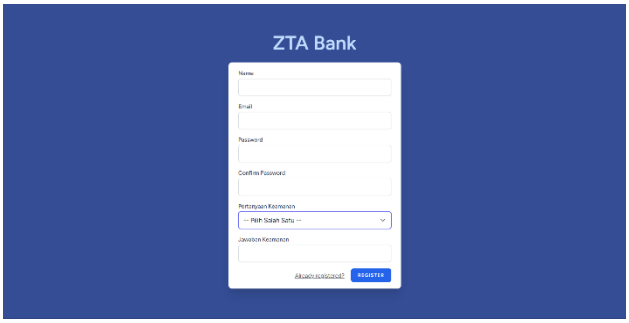
Fase 3: Penguatan Verifikasi Identitas

Untuk lebih memperkuat proses verifikasi identitas, beberapa lapisan keamanan tambahan diimplementasikan.

Hasil dari fase ini adalah tiga fitur keamanan baru:

1) Verifikasi Email Wajib: Setiap akun baru wajib melakukan verifikasi melalui link yang dikirim ke email sebelum dapat mengakses fitur-fitur utama.
2) *Knowledge-Based Authentication (KBA):* Pengguna diwajibkan untuk memilih dan menjawab Pertanyaan Keamanan saat proses registrasi.
3) *Two-Factor Authentication (2FA)*: Fitur *2FA* berbasis *TOTP* (menggunakan aplikasi seperti *Google Authenticator*) telah diaktifkan dan tersedia sebagai opsi keamanan tambahan di halaman profil pengguna[11].

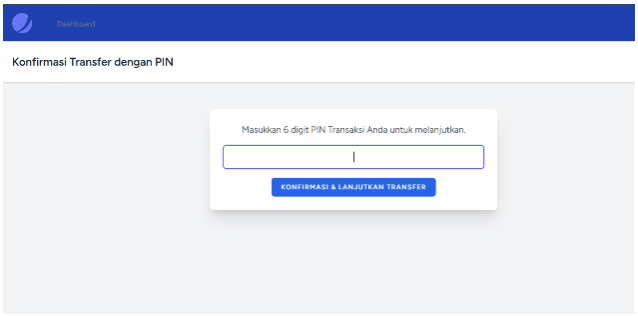
Pembahasan dari ketiga fitur ini adalah diversifikasi faktor autentikasi. Sistem tidak lagi hanya bergantung pada satu faktor "sesuatu yang Anda tahu" (*password*). Dengan verifikasi email, sistem memastikan kepemilikan aset digital (email). Dengan KBA, sistem menambahkan faktor pengetahuan kedua yang berbeda. Dengan *2FA*, sistem menambahkan faktor kepemilikan "sesuatu yang Anda miliki" (ponsel). Ini secara drastis meningkatkan kepercayaan sistem terhadap identitas pengguna yang mencoba masuk.



Gambar 4. *Formulir Pertanyaan Keamanan (KBA) pada Halaman Registrasi*
Sumber: Tampilan Web Register Page

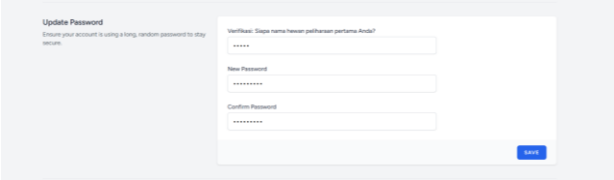
Fase 4: Implementasi Otorisasi Aksi Sensitif

Tahap ini adalah inti dari implementasi ZTA di dalam sesi yang sudah terautentikasi, menerapkan prinsip "Jangan Pernah Percaya, Selalu Verifikasi" secara berkelanjutan. Hasil dari tahap ini adalah implementasi PIN Transaksi 6 digit dan integrasi verifikasi KBA pada fitur-fitur krusial. Pengujian menunjukkan bahwa setiap upaya transfer dana akan selalu diinterupsi oleh halaman konfirmasi PIN.



Gambar 5. *Halaman Konfirmasi PIN Sebelum Eksekusi Transfer*
Sumber: Hasil Pengujian

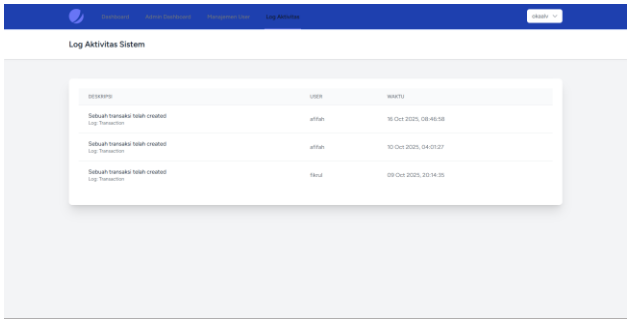
Demikian pula, upaya untuk mengubah data sensitif seperti password atau PIN di halaman profil akan gagal jika pengguna tidak dapat memberikan jawaban KBA yang benar. Pembahasan dari mekanisme ini adalah penerapan step-up authentication. Sistem tidak mempercayai sesi login yang sedang aktif untuk melakukan tindakan berisiko tinggi. Dengan meminta verifikasi kedua (PIN atau KBA), sistem memastikan bahwa orang yang sedang melakukan aksi tersebut benar-benar pemilik akun yang sah, melindungi dari skenario di mana perangkat pengguna ditinggalkan dalam keadaan login.



Gambar 6. Verifikasi KBA untuk Mengubah Password
Sumber: Hasil Percobaan

Fase 5: Implementasi Monitoring

Mengacu pada prinsip *ZTA* Asumsikan Adanya Pelanggaran *(Assume Breach)*, sistem monitoring dan pencatatan log diimplementasikan. Hasil dari fase ini adalah integrasi *spatie/laravel-activitylog* yang secara otomatis mencatat semua event autentikasi (berhasil, gagal, logout) dan setiap transaksi yang dibuat. Selain itu, telah dibangun antarmuka khusus bagi Admin untuk melihat seluruh log aktivitas sistem dan melakukan filter untuk melihat riwayat aktivitas dari satu pengguna spesifik.



Gambar 7. Halaman Log Aktivitas Spesifik per Pengguna di Dasbor Admin
Sumber: Hasil percobaan

Pembahasan dari implementasi ini adalah peningkatan visibilitas dan kemampuan investigasi. Dengan adanya audit trail yang lengkap, admin dapat dengan cepat mendeteksi pola aktivitas yang mencurigakan dan melakukan analisis forensik jika terjadi insiden keamanan, yang merupakan komponen vital dalam arsitektur ZTA.

KESIMPULAN DAN SARAN

Penelitian ini berhasil mengimplementasikan *Zero Trust Architecture (ZTA)* dengan integrasi *Multi-Factor Authentication (MFA)* dan *Continuous Verification (CV)* pada sistem login berbasis web untuk memperkuat mekanisme autentikasi dan otorisasi pengguna. Hasil pengujian menunjukkan bahwa penerapan *MFA* mampu meningkatkan keamanan autentikasi awal melalui kombinasi beberapa faktor verifikasi, sementara *CV* memastikan validitas identitas pengguna secara berkelanjutan selama sesi aktif. Integrasi activity logging juga menambah kemampuan sistem dalam mendeteksi aktivitas mencurigakan serta mendukung proses audit keamanan. Keunggulan sistem ini terletak pada penerapan prinsip *Never Trust, Always Verify* secara menyeluruh dan kemampuan pemantauan *real-time* yang meningkatkan ketahanan terhadap pencurian kredensial serta akses tidak sah. Namun demikian, kelemahan masih terdapat pada kebutuhan sumber daya sistem yang lebih tinggi serta potensi keterlambatan respon akibat proses verifikasi berlapis. Secara keseluruhan, implementasi ini terbukti efektif dalam menjawab tujuan penelitian untuk membangun sistem login yang aman, adaptif, dan sesuai dengan standar keamanan global berbasis *Zero Trust*.

Penelitian selanjutnya disarankan untuk mengoptimalkan efisiensi sistem dengan melakukan integrasi teknologi machine learning guna mendeteksi anomali perilaku pengguna secara otomatis, sehingga proses verifikasi dapat berjalan lebih cepat dan cerdas. Selain itu, sistem dapat dikembangkan lebih lanjut untuk mendukung lingkungan *multi-platform* seperti aplikasi *mobile* dan *cloud-based authentication*. Pengujian juga perlu diperluas menggunakan skenario pengguna yang lebih beragam untuk mengevaluasi skalabilitas dan ketahanan sistem terhadap ancaman siber yang lebih kompleks.

UCAPAN TERIMA KASIH

Kami mengucapkan terima kasih kepada dosen pembimbing yang telah memberikan arahan dan bimbingan selama proses penyusunan tugas ini. Kami berharap dukungan dan masukan dari semua pihak akan menjadi landasan bagi pengembangan penelitian lebih lanjut di masa yang akan datang.

DAFTAR PUSTAKA

[1] M. S. Rakhmadi Rahman1*, Muhammad Faiz Ilyaz1, "IMPLEMENTASI ZERO TRUST ARSITEKTUR PADA JARINGAN HYBRID WORK," *J. Syst. Technol.*, vol. 1, no. 1, pp. 14–19, 2025.

[2] H. Najwa, "Analisis penerapan Trust Network Access (ZTNA) dengan penggunaan CAPTCHA pada website umum," *Technol. Sci. Insights J.*, vol. 1, no. 2, pp. 77–80, 2024.

[3] M. Rizki *et al.*, "SIMULASI SERANGAN SIBER MAC ADDRESS DAN IP ADDRESS SPOOFING PADA JARINGAN HTTP DI KALI LINUX," *JUTIK J. Teknol. Inf. dan Komput.*, vol. 11, no. 2, pp. 139–149, 2025.

[4] R. W. Darmawan, I. Irawan, and S. Petriansyah, "Analisis Adaptif Zero Trust Architecture (ZTA) Berbasis Machine Learning untuk Deteksi Intrusi pada Jaringan IoT dalam Infrastruktur Kritis," *RIGGS J. Artif. Intell. Digit. Bus.*, vol. 3, no. 4, pp. 36–45, 2025, doi: 10.31004/riggs.v3i4.460.

[5] S. Mushtaq, M. Mohsin, and M. M. Mushtaq, "A Systematic Literature Review on the Implementation and Challenges of Zero Trust

Architecture Across Domains," *Sensors*, vol. 25, no. 19, p. 6118, 2025, doi: 10.3390/s25196118.

[6] I. Cahyanto, H. Madihah, I. Budiarso, A. Sutrisno, and T. Hidayat, "Effectiveness of Multifactor Authentication Technology for Protecting Student Privacy : a Systematic Literature Review," *Edum J.*, vol. 7, no. 2, pp. 253–269, 2025, doi: 10.31943/edumjournal.v7i2.286.

[7] W. Badeges and M. N. Fauzi, "Implementasi Multi Factor Authentication Pada PHPMyAdmin," *TRIPLE A J. Pendidik. Teknol. Inf.*, vol. 2, no. 1, pp. 35–39, 2023.

[8] H. Haeruddin, S. E. Prasetyo, and A. Mindy, "Implementasi Multi-Factor Authentication Untuk Optimalisasi Keamanan Akses Data Di PT.ABC," *J. Manaj. Inform.*, vol. 15, no. 1, p. 85096, 2025, doi: 10.34010/5rdjmw37.

[9] H. Hasrul, A. Amriadi, and N. F. Suprayitno, "Perancangan Sistem Informasi Pengarsipan Surat Pada Kantor Kejaksaan Kabupaten Mamuju Utara," *J. Manaj. Inform. Sist. Inf. dan Teknol. Komput.*, vol. 1, no. 1, pp. 21–31, 2022, doi: 10.70247/jumistik.v1i1.6.

[10] A. Yousseef, S. Satam, B. S. Latibari, M. Abdel-Malek, S. Salehi, and P. Satam, "Zero Trust-based Decentralized Identity Management System for Autonomous Vehicles," *Veh. Tehcnology*, vol. 00, pp. 1–14, 2025, [Online]. Available: http://arxiv.org/abs/2509.25566

[11] V. Dakić, Z. Morić, A. Kapulica, and D. Regvart, "Analysis of Azure Zero Trust Architecture Implementation for Mid-Size Organizations," *J. Cybersecurity Priv.*, vol. 5, no. 1, 2025, doi: 10.3390/jcp5010002.

[12] Y. Liu, "Analysis of Multi-factor Authentication (MFA) Schemes in Zero Trust Architecture (ZTA): Current State, Challenges, and Future Trends," *Int. J. Comput. Appl.*, vol. 186, no. 57, pp. 30–36, 2024, doi: 10.5120/ijca2024924310.

[13] R. P. Reddy, "Zero Trust Architectures in Modern Enterprises: Principles, Implementation Challenges, and Best Practices," *Int. J. Comput. Trends Technol.*, vol. 73, no. 6, pp. 48–57, 2025, doi: 10.14445/22312803/ijctt-v73i6p107.

[14] A. Dalal, "Designing Zero Trust Security Models to Protect Distributed Networks and Minimize Cyber Risks," *SSRN Electron. J.*, vol. XI, no. 142, pp. 142–164, 2025, doi: 10.2139/ssrn.5422314.

[15] A. Marsehan, S. Ardilla, and A. Novia Putri, "Pengembangan Sistem Absensi Mahasiswa berbasis QR-Code di Prodi Teknologi Informasi," *J. Manaj. Inform. Sist. Inf. dan Teknol. Komput.*, vol. 4, no. 1, pp. 332–339, 2025, doi: 10.70247/jumistik.v4i1.138.