# IMPLEMENTASI SISTEM LOGIN WEB BERBASIS ZTA DENGAN INTEGRASI OTP BREVO DAN CAPTCHA

**Steven Adventino Gulo*[1)], Dedy Kiswanto[2)], Muhammad Hidayatul Arifin[3)], Windy Aulia[4)]**

1. Ilmu Komputer, Universitas Negeri Medan
stevenadventinogulo@gmail.com
2. Ilmu Komputer, Universitas Negeri Medan
dedykiswanto@unimed.ac.id
3. Ilmu Komputer, Universitas Negeri Medan
arif.423325005@mhs.unimed.ac.id
4. Ilmu Komputer, Universitas Negeri Medan
windy.4231250021@mhs.unimed.ac.id

***Abstract***

*Keamanan autentikasi pada sistem web merupakan komponen penting dalam menjaga kerahasiaan dan integritas data pengguna dari berbagai ancaman siber seperti brute force, phishing, dan serangan bot. Penelitian ini mengimplementasikan sistem login web berbasis Zero Trust Architecture (ZTA) yang diintegrasikan dengan One-Time Password (OTP) Brevo serta Google reCAPTCHA untuk memperkuat proses verifikasi identitas pengguna. Prinsip dasar "never trust, always verify" diterapkan agar setiap permintaan akses divalidasi secara menyeluruh tanpa adanya asumsi kepercayaan terhadap pengguna. Sistem dikembangkan menggunakan bahasa pemrograman web dengan dukungan basis data MySQL dan diuji melalui serangkaian uji fungsional, performa, serta keamanan. Hasil pengujian menunjukkan bahwa kombinasi ZTA, OTP Brevo, dan reCAPTCHA secara signifikan meningkatkan keamanan proses login dengan membatasi percobaan akses berulang, mencegah serangan otomatis dari bot, serta menekan potensi login ilegal. Selain itu, penerapan enkripsi kata sandi dan pembatasan waktu OTP terbukti meningkatkan keandalan autentikasi berlapis. Berdasarkan hasil percobaan, sistem yang dikembangkan dinilai lebih tangguh, adaptif, dan efisien dalam menghadapi ancaman siber modern tanpa mengurangi kenyamanan pengguna.*

***Kata Kunci**: brevo, captcha, zta, otp*

## A. PENDAHULUAN

Internet memiliki peran penting dalam kehidupan pribadi maupun profesional, namun juga menimbulkan risiko karena peretas dapat mengeksploitasi kelemahan system [1]. Badan Siber dan Sandi Negara (BSSN) menegaskan pentingnya penerapan *Zero Trust Architecture* (ZTA) pada berbagai infrastruktur web [2]. Secara tradisional, keamanan jaringan mengandalkan model perimeter yang menganggap ancaman berasal dari luar dan pengguna di dalam jaringan dapat dipercaya [3]. Peningkatan ancaman siber seperti *brute force* dan *phishing*

menjadikan keamanan *login* web semakin krusial untuk diperhatikan [4]. Sistem autentikasi berbasis satu *password* kini tidak lagi memadai, sehingga diperkenalkan konsep *Zero Trust Architecture* (ZTA) dengan prinsip *"never trust, always verify"* untuk memastikan setiap akses selalu diverifikasi [5]. Banyak sistem login rentan karena hanya mengandalkan *password* lemah atau berulang. Diperlukan verifikasi tambahan agar keamanan login lebih kuat dan adaptif [6].

*One-Time Password* (OTP) adalah kata sandi unik yang hanya dapat digunakan sekali untuk sesi login atau transaksi pada komputer atau perangkat digital lainnya [7]. OTP dibuat untuk mencegah akses tidak sah oleh pihak yang tidak berwenang terhadap data rahasia [8].

CAPTCHA (*Completely Automated Public Turing test to tell Computers and Humans Apart*) adalah teknik yang digunakan untuk membedakan antara manusia dan program komputer (bot) [9]. CAPTCHA sebagai kode keamanan berupa deretan karakter atau simbol acak yang ditampilkan dalam bentuk gambar pada halaman *form* [10]. Pengguna harus memasukkan karakter tersebut ke dalam kolom yang disediakan agar dapat mengirimkan atau melanjutkan pengisian data [11]. Kita dapat mengatur tingkat kesulitan captcha agar menantang dan menyulitkan akses dari yang bukan semestinya. Namun perlu juga menyesuaikan agar penggunaan captcha tidak menyulitkan interaksi dan mengganggu pengalaman dari *user* atau pengguna [12].

Penelitian terdahulu hanya mengkombinasikan sistem login web berbasis ZTA yang memadukan OTP. Namun belum sepenuhnya menerapkan prinsip *Zero Trust*. Karena itu, penelitian ini menutup celah tersebut dengan menggabungkan ZTA, OTP, dan CAPTCHA dalam satu sistem login terintegrasi. Maka daripada itu penelitian ini membangun sistem login web berbasis *Zero Trust Architecture* dengan integrasi OTP *Brevo* dan CAPTCHA guna meningkatkan keamanan autentikasi pengguna.

## B. METODE PENELITIAN

### 1. Analisis Kebutuhan

Tahap ini mencakup identifikasi kebutuhan sistem autentikasi berbasis ZTA, analisis ancaman terhadap proses login web (seperti *brute force*, *credential stuffing*, dan *bot attack*), serta penentuan kebutuhan integrasi OTP dan CAPTCHA.

### 2. Perancangan Sistem

Perancangan dilakukan dengan pendekatan arsitektur *Zero Trust*, di mana setiap proses autentikasi dan permintaan akses harus diverifikasi tanpa asumsi kepercayaan. Diagram arsitektur sistem disusun untuk menunjukkan interaksi antara pengguna, server aplikasi, API Brevo, dan layanan CAPTCHA.

#### a. Implementasi

Sistem dikembangkan menggunakan bahasa pemrograman web (PHP atau Python) dengan basis data MySQL/PostgreSQL. Integrasi OTP dilakukan melalui API Brevo, sedangkan CAPTCHA diimplementasikan menggunakan layanan reCAPTCHA. Prinsip *Zero Trust* diterapkan melalui validasi identitas berlapis, pemantauan sesi, dan pembatasan akses berdasarkan konteks (*context-aware access*).

#### b. Pengujian dan Evaluasi

Pengujian dilakukan secara fungsional, performa, dan keamanan:

- Uji fungsional: memastikan seluruh fitur *login*, OTP, dan CAPTCHA berjalan sesuai desain.
- Uji performa: mengukur waktu rata-rata pengiriman OTP dan durasi autentikasi pengguna.

- Uji keamanan: menguji ketahanan terhadap serangan *brute-force*, *bot*, serta simulasi login tidak sah.

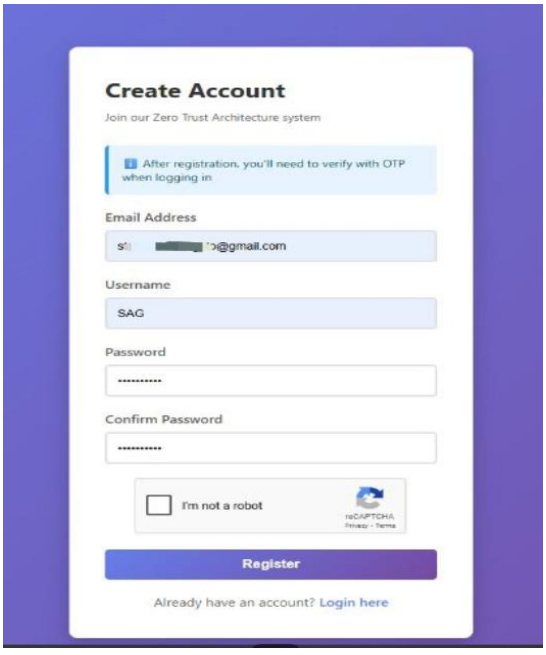
Selain itu, dilakukan pengukuran *usability* menggunakan kuesioner sederhana (skala Likert) untuk menilai kenyamanan pengguna terhadap proses autentikasi.

**c. Analisis Hasil**

Data hasil pengujian dianalisis secara kuantitatif dan kualitatif. Analisis kuantitatif mencakup penghitungan rata-rata waktu autentikasi, tingkat keberhasilan OTP, dan efektivitas CAPTCHA terhadap *bot*. Analisis kualitatif dilakukan terhadap pengalaman pengguna dan tingkat persepsi keamanan sistem.

## C. HASIL DAN PEMBAHASAN

Dalam penelitian ini, penulis menggunakan ZTA dengan Brevo yang berfungsi sebagai OTP *sender* yang kemudian akan dikirim ke *email user*, serta menggunakan Google reCAPTCHA v2.

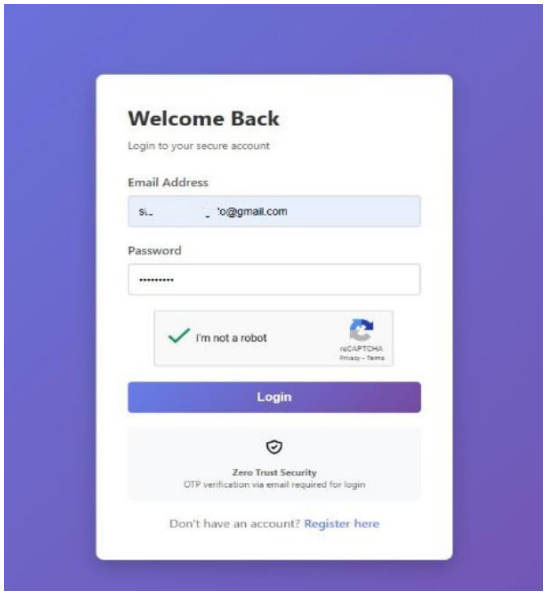



**Gambar 1.** Halaman registrasi

Gambar 1 adalah halaman registrasi, *user* akan menggunakan *email user* untuk registrasi, *username*, serta *password* yang diinginkan *user*. Setelah itu, CAPTCHA wajib dilakukan untuk mengetahui apakah *user* tersebut asli atau robot

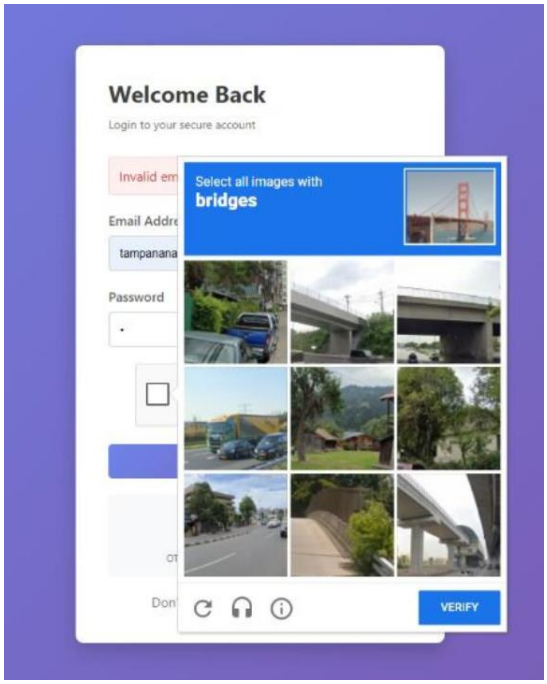
**Gambar 2.** Tabel *users* di phpMyAdmin

Setelah registrasi, maka *username*, *email*, dan *password* yang sudah didaftar akan dimasukkan ke dalam tabel *users*. Terlihat pada kolom *password* terdapat beberapa karakter acak, padahal di Gambar 1, *password*-nya cuma beberapa karakter. Ini karena *password* yang sudah teregistrasi akan dienkripsi supaya penyerang akan lebih kesusahan untuk menyerang web.



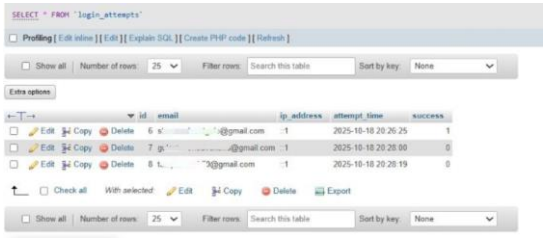

**Gambar 3.** Halaman login

Setelah registrasi, *user* akan melalukan login sesuai dengan *email* dan *password* yang telah teregistrasi ke database.



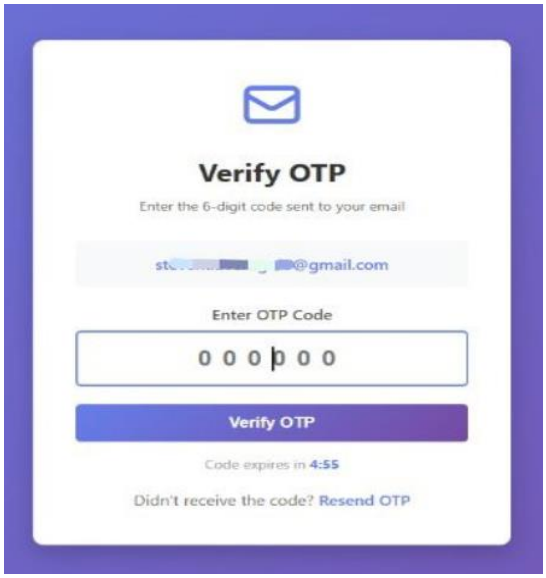

**Gambar 4.** CAPTCHA jika user login berkali-kali

Jika *user* melakukan *login* berulang, maka CAPTCHA akan melakukan keamanan tingkat lanjut, seperti CAPTCHA gambar atau pun suara seperti gambar di atas.



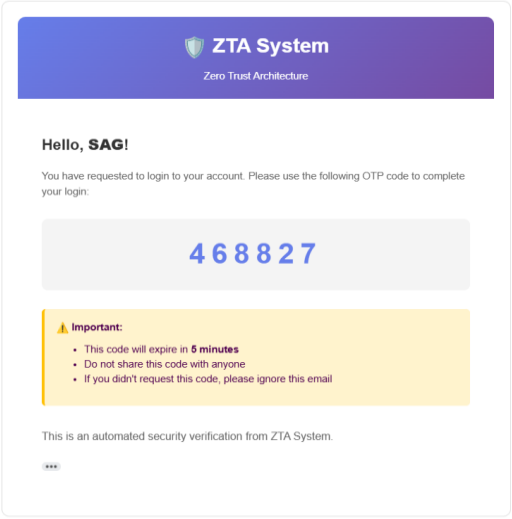
**Gambar 5.** Tabel login_attempts

Untuk tabel pada gambar 5 di atas adalah tabel jika ada satu *user* atau lebih yang mencoba *login*, maka setiap *login* akan terekam ke tabel data ini. Ini berguna untuk mengetahui serangan-serangan atau pun aktivitas yang mencurigakan.



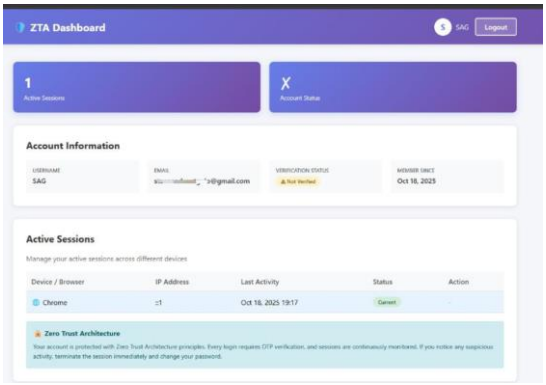

**Gambar 6.** Halaman kode OTP

Setelah *login* berhasil, web akan meminta kode OTP yang sebelumnya dikirim ke dalam *email user* yang sudah teregistrasi. Batas yang diberikan adalah 5 menit, selebih dari waktu yang ditentukan maka kode OTP tersebut akan kadaluarsa dan *user* harus men-generate kode OTP yang baru.




**Gambar 7.** OTP yang sudah terkirim

OTP kemudian akan dikirim ke email pengguna yang sudah terdaftar. Kode ini lebih baik dirahasiakan untuk *user* itu sendiri.




**Gambar 8.** Halaman Dashboard

Setelah *login* berhasil, *user* akan dibawa ke halaman *dashboard* web. *Active Session* bertujuan untuk web-web yang digunakan oleh *user* untuk login. *Account Information* berisi informasi username, email, status verifikasi, dan tanggal pendaftaran *user*. *Active Session* bagian bawah akan memberitahu user web apa saja yang digunakan untuk login email tersebut.

Setelah semua penjelasan di atas maka dapat mengkoreksi tabel pengujian.

**Tabel 1.** Tabel pengujian websites

| No | Skenario | Hasil yang Diharapkan | Hasil Aktual | Status |
|---|---|---|---|---|
| 1 | Login valid | Akses diterima | Akses diterima | Ya |
| 2 | Login salah | Akses ditolak | Akses ditolak | Ya |
| 3 | OTP benar | Verifikasi berhasil | Verifikasi berhasil | Ya |
| 4 | OTP salah | Akses ditolak | Akses ditolak | Ya |
| 5 | OTP kadaluarsa | Akses ditolak | Akses ditolak | Ya |
| 6 | CAPTCHA tidak diisi | Akses ditolak | Akses ditolak | Ya |
| 7 | CAPTCHA salah | Akses ditolak | Akses ditolak | Ya |
| 8 | Akses tanpa login | Ditolak | Ditolak | Ya |
| 9 | Akses setelah logout | Ditolak | Ditolak | Ya |
| 10 | Brute-force login | Diblokir sementara | Diblokir sementara | Ya |

## D. KESIMPULAN DAN SARAN

### 1. Kesimpulan

Penelitian ini mengembangkan sistem *login* web berbasis *Zero Trust Architecture* (ZTA) yang terintegrasi dengan *One-Time Password* (OTP) Brevo dan Google reCAPTCHA untuk meningkatkan keamanan autentikasi pengguna. Dengan prinsip "*never trust, always verify*", setiap proses *login* divalidasi secara berlapis melalui identifikasi pengguna, verifikasi OTP, dan CAPTCHA guna mencegah akses otomatis oleh *bot*. Hasil pengujian menunjukkan bahwa sistem ini efektif mengurangi serangan *brute force* dan *login* ilegal, berkat penerapan enkripsi password serta pembatasan waktu OTP. Secara keseluruhan, kombinasi ZTA, OTP, dan CAPTCHA mampu

menciptakan sistem *login* yang lebih aman dan adaptif terhadap ancaman siber.

**2. Saran**

Kedepannya, pengembangan sistem akan menambahkan lapisan keamanan tambahan seperti *multi-factor authentication (MFA)* berbasis biometrik atau perangkat fisik guna meningkatkan keandalan autentikasi. Pengujian pada jumlah pengguna yang lebih luas juga diperlukan untuk menilai kinerja sistem secara menyeluruh. Selain itu, integrasi dengan deteksi ancaman berbasis kecerdasan buatan (*AI-based threat detection*) akan dipertimbangkan agar sistem mampu mengenali pola serangan secara *real-time*. Dari sisi pengguna, peningkatan edukasi terkait kerahasiaan kode OTP dan penggunaan kata sandi yang kuat menjadi aspek penting untuk menjaga keamanan sistem secara berkelanjutan.

## E. REFERENSI


[1] Walidin, A. P., Putri, F. P., & Kiswanto, D. (2025). Kali Linux sebagai alat analisis keamanan jaringan melalui penggunaan Nmap, Wireshark, dan Metasploit. JATI (Jurnal Mahasiswa Teknik Informatika), 9(1), 1188–1196. https://doi.org/10.36040/jati.v9i1.12661

[2] Zuhriyanto, I., & Astari, S. R. A. (2025). Penerapan Zero Trust Architecture untuk mitigasi ancaman pembajakan akun WhatsApp. JITU: Journal Informatic Technology and Communication, 9(1), 50–58. https://doi.org/10.36596/jitu.v9i1.1815

[3] Muakhori, I., & Syamsiah, N. (2025). Pengamanan arsitektur microservices pada aplikasi perusahaan: Strategi dan implementasi. Info Kripto, 19(1), 29–37. https://doi.org/10.56706/ik.v19i1.116

[4] Mukhlisin, M., & Firmansyah, R. A. (2025). Zero Trust Architecture: Solusi keamanan dan privasi untuk institusi pendidikan, systematic literature review. JATI (Jurnal Mahasiswa Teknik Informatika), 9(4), 6926–6935. https://doi.org/10.36040/jati.v9i4.14344

[5] Hose, F., Censaka, F., Wijaya, R. A., Jennifer, Tanuwijaya, C., & Ng, J. (2025). Analisis peran blockchain dalam zero-trust architecture untuk penguatan identitas digital dan privasi data. JIMU: Jurnal Ilmiah Multidisipliner, 4(1), 568–577. https://doi.org/10.70294/jimu.v4i01.1330

[6] Nabillah, J. L., Satriawan, N., & Saputra, F. (2025). Strategi manajemen sekuriti dalam menghadapi ancaman siber di era digital. Orbit: Jurnal Ilmu Multidisiplin Nusantara, 1(3), 136–141. https://doi.org/10.63217/orbit.v1i3.151

[7] Wibawa, S., Suryanto, & Ningsih, R. (2024). Perlindungan data digital dengan Time-Based One-Time Password (TOTP). INSANtek – Jurnal Inovasi dan Sains Teknik Elektro, 5(1), 30–36.

https://doi.org/10.31294/insantek.v5i1.3495

[8] Christian, C., Sitorus, S. H., & Nirmala, I. (2023). Implementasi algoritma RSA dan One Time Password (OTP) untuk pengamanan data pengguna dan proses transaksi pada website e-commerce. Coding: Jurnal Komputer dan Aplikasi, 11(1), 62–72. https://doi.org/10.26418/coding.v11i1.58684

[9] Rayza, M., Usman, A., & Budiman, A. (2023). Keamanan jaringan hotspot mikrotik menggunakan metode otentikasi pengguna dengan captcha dan IP-binding untuk filtering user. Jurnal Ilmu Komputer dan Sistem Informasi (JIRSI), 2(3), 206–215. https://doi.org/10.70340/jirsi.v2i3.76

[10] Najwa, H. (2024). Analisis penerapan Trust Network Access (ZTNA) dengan penggunaan CAPTCHA pada website umum. Technology Sciences Insights Journal, 1, 76–80.

[11] Putra A, R., Kurniawan, R., & Aviani, T. H. B. (2025). Optimalisasi model jaringan syaraf untuk pengenalan CAPTCHA dengan metode LeNet-5. Journal of Informatics Management and Information Technology, 5(3), 250–259. https://doi.org/10.47065/jimat.v5i3.476

[12] Hansen, J., & Sutabri, T. (2023). Mendesain cyber security untuk mencegah serangan DDoS pada website menggunakan metode captcha. Digital Transformation Technology, 3(1), 289–298. https://doi.org/10.47709/digitech.v3i1.2764