JITET (Jurnal Informatika dan Teknik Elektro Terapan)
Vol. 14 No. 1, pISSN: 2303-0577 eISSN: 2830-7062 http://dx.doi.org/10.23960/jitet.v14i1.8297

RANCANG BANGUN SISTEM DOUBLE AUTHENTICATION DENGAN KONSEP ZTA (ZERO TRUST ARCHITECTURE)

Rohit Purba[1], Dedy Kiswanto[2], Cristian Sinaga[3] , Pedro Waruwu[4]

[1,2,3,4]Universitas Negeri Medan; Jalan Willem Iskandar Psr.V - Kotak Pos No.1589 - Medan 20221 Telepon (061) 6613365, 6613276, 6618754 Fax (061) 6614002 – 6613319

Keywords:
Zero Trust Architecture ;
Double Authentication;
OTP Email;
Keamanan Website.

Corespondent Email:
rohit.4233250032@mhs.unimed.ac.id

Abstrak. Perkembangan teknologi informasi yang pesat telah meningkatkan ketergantungan terhadap sistem berbasis web, namun diiringi dengan ancaman keamanan siber seperti phishing, credential theft, dan session hijacking. Penelitian ini bertujuan merancang dan mengimplementasikan sistem Double Authentication berbasis Zero Trust Architecture (ZTA) dengan menggunakan OTP Email pada website. Metode yang digunakan adalah Research and Development (R&D) dengan tahapan analisis kebutuhan, perancangan arsitektur, implementasi, dan pengujian fungsional serta keamanan. Hasil penelitian menunjukkan bahwa sistem berhasil menerapkan prinsip Never Trust, Always Verify melalui dua lapis verifikasi: login kredensial dan OTP yang dikirim via email. Sistem juga menerapkan Role-Based Access Control (RBAC) untuk membatasi akses pengguna dan admin. Pengujian keamanan membuktikan sistem mampu mencegah credential theft dan insider threat. Kesimpulannya, sistem ini secara signifikan meningkatkan keamanan akses website tanpa mengorbankan pengalaman pengguna, serta membuktikan bahwa ZTA dapat diimplementasikan secara efektif dalam lingkungan web.

1. PENDAHULUAN

Perkembangan teknologi informasi yang pesat telah mendorong transformasi digital di berbagai sektor, mulai dari bisnis, pendidikan, hingga infrastruktur kritis seperti layanan kesehatan dan energi [1], [2]. Website kini menjadi komponen utama dalam sistem informasi modern yang berfungsi sebagai sarana komunikasi, transaksi, serta pengelolaan data secara daring. Namun, seiring dengan meningkatnya ketergantungan terhadap sistem berbasis web, ancaman terhadap keamanan data dan privasi pengguna juga meningkat secara signifikan. Model keamanan tradisional yang berfokus pada perimeter jaringan kini tidak lagi

memadai untuk menghadapi kompleksitas serangan siber modern [3], [4]. Serangan seperti *phishing*, pencurian kredensial (*credential theft*), *brute force attack*, dan pembajakan sesi (*session hijacking*) telah menjadi ancaman utama bagi sistem yang tidak memiliki mekanisme autentikasi yang kuat [5]. Pelaku kejahatan siber kerap memanfaatkan berbagai alat canggih seperti Nmap untuk pemindaian port, Wireshark untuk penyadapan lalu lintas jaringan, dan Metasploit untuk eksploitasi kerentanan, yang semuanya dapat dioperasikan melalui platform seperti Kali Linux untuk mengidentifikasi dan menembus celah keamanan [6], [7].

Dalam konteks ini, muncul paradigma baru bernama *Zero Trust Architecture* (ZTA) yang menolak konsep kepercayaan implisit di dalam jaringan. Prinsip utamanya adalah *"Never Trust, Always Verify"* (Jangan Pernah Percaya, Selalu Verifikasi), yang berarti setiap permintaan akses, baik dari dalam maupun luar sistem, harus melalui proses verifikasi menyeluruh sebelum diberikan hak akses [8], [9]. ZTA mengubah paradigma dari *trust but verify* menjadi *verify everything*, dengan menerapkan kebijakan keamanan dinamis yang tidak hanya berbasis pada identitas, tetapi juga konteks lain seperti perangkat, lokasi, dan perilaku pengguna [10], [11]. Pendekatan ini terbukti lebih adaptif dalam melindungi aset digital, termasuk dalam lingkungan yang kompleks seperti *Internet of Things* (IoT) dan infrastruktur kritis lainnya [12], [13].

Inti dari penerapan ZTA adalah proses verifikasi berkelanjutan yang kuat. Salah satu metode paling efektif untuk mencapai hal ini adalah dengan mengimplementasikan *Multi-Factor Authentication* (MFA), sebuah sistem keamanan yang mewajibkan pengguna untuk menyediakan dua atau lebih bukti verifikasi (kredensial) untuk mendapatkan akses [14]. Mekanisme MFA umumnya didasarkan pada tiga kategori faktor yang independen: sesuatu yang pengguna ketahui (*knowledge factor*) seperti kata sandi atau PIN; sesuatu yang pengguna miliki (*possession factor*) seperti token OTP pada ponsel atau *smart card*; dan sesuatu yang melekat pada diri pengguna (*biometric factor*) seperti sidik jari atau pengenalan wajah. Dengan mengharuskan verifikasi dari beberapa kategori, MFA secara signifikan meningkatkan keamanan dan mempersulit akses tidak sah bahkan jika salah satu faktor, seperti kata sandi, berhasil dicuri [15].

Mengingat pentingnya keseimbangan antara keamanan dan kemudahan penggunaan, implementasi autentikasi dua faktor (*Double Authentication*) menjadi solusi yang praktis dan efektif. Sistem ini memerlukan dua tahap verifikasi identitas, yang pada penelitian ini terdiri dari tahap pertama berupa *credential-based login* (faktor pengetahuan) dan tahap kedua berupa autentikasi tambahan seperti *One-Time Password* (OTP) yang dikirimkan ke email pengguna (faktor kepemilikan). Penggunaan OTP berbasis waktu (*Time-based One-Time Password* atau TOTP) memastikan bahwa kode verifikasi hanya valid untuk periode singkat, sehingga mampu menangkal serangan seperti *replay attack* dan *phishing* secara efektif.

Dengan demikian, penelitian ini berfokus pada perancangan dan implementasi sistem autentikasi ganda (*Double Authentication*) berbasis *Zero Trust Architecture* (ZTA) menggunakan OTP Email pada website. Tujuan utama penelitian ini adalah menciptakan sistem yang lebih aman, adaptif, dan sesuai dengan paradigma keamanan modern, yang menuntut verifikasi berkelanjutan dan pengendalian akses secara dinamis untuk setiap entitas pengguna guna melindungi data sensitif dari ancaman siber yang terus berevolusi.

2. TINJAUAN PUSTAKA

2.1. Zero Trust Architecture (ZTA)

ZTA adalah model keamanan yang menolak kepercayaan implisit terhadap entitas internal. Semua permintaan akses diverifikasi secara menyeluruh, tanpa terkecuali [1]. ZTA berfokus pada autentikasi berkelanjutan (continuous verification), pembatasan hak akses (least privilege access), dan segmentasi jaringan (micro-segmentation). Model ini memastikan hanya pengguna yang telah diverifikasi berlapis yang dapat mengakses sumber daya sistem.

2.2. Double Authentication

Double Authentication menggabungkan dua tahap verifikasi pengguna. Tahap pertama adalah login kredensial, di mana *username* dan *password* diverifikasi terhadap *database*. Tahap kedua adalah verifikasi OTP, di mana sistem mengirimkan kode acak ke email pengguna yang harus dimasukkan sebelum *login* berhasil. Pendekatan ini meningkatkan keyakinan bahwa pengguna benar-benar pemilik akun yang sah. OTP bersifat sementara, sehingga mencegah penyalahgunaan kredensial hasil pencurian.

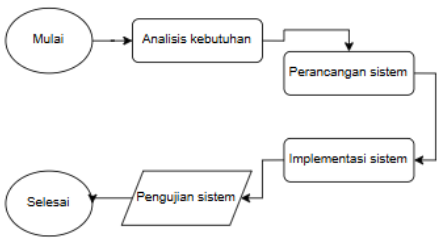
2.3. Penerapan OTP pada Arsitektur ZTA

Dalam konteks Zero Trust, OTP berperan sebagai bagian dari prinsip *Continuous Authentication* sistem tidak mempercayai autentikasi tunggal, melainkan menambahkan lapisan validasi kedua untuk memastikan keaslian pengguna di setiap sesi. Setiap OTP dihasilkan secara acak dan dikirim melalui kanal terenkripsi (email via SMTP TLS), memastikan keamanan selama transmisi.

2.4. Relevansi Penerapan

Model ZTA dapat diadaptasi ke berbagai konteks, termasuk lingkungan kolaboratif seperti website, cloud, hingga metaverse. Pendekatan yang sama dapat diterapkan pada autentikasi berbasis web untuk meningkatkan integritas sistem dan perlindungan data pengguna.

3. METODE PENELITIAN



Gambar 1. Flowchard alur penelitian

Penelitian ini menggunakan pendekatan Research and Development (R&D) dengan tahapan perancangan, implementasi, dan evaluasi sistem. Metode yang digunakan meliputi analisis kebutuhan, perancangan arsitektur sistem, implementasi komponen keamanan, dan pengujian fungsional serta keamanan.

3.1. Analisis Kebutuhan

Analisis dilakukan untuk mengidentifikasi kebutuhan fungsional dan non-fungsional sistem. Adapun Kebutuhan fungsional meliputi registrasi pengguna dengan verifikasi email, login dengan username dan password, pengiriman dan verifikasi OTP via email, serta pembagian hak akses berdasarkan peran (user dan admin). Sementara itu, kebutuhan non-fungsional meliputi keamanan, keandalan, dan kemudahan penggunaan.

3.2. Perancangan Sistem

Sistem dirancang dengan mengadopsi prinsip Zero Trust Architecture (ZTA). Prinsip ini menerapkan *Never Trust, Always Verify*, di mana setiap akses harus melalui dua lapis verifikasi. Selain itu, diterapkan pula *Least Privilege Access* yang memastikan pengguna hanya mendapatkan akses sesuai perannya, dan *Continuous Authentication* di mana OTP digunakan sebagai bagian dari verifikasi berkelanjutan. Arsitektur sistem terdiri dari modul registrasi dan login, modul pengiriman OTP via email (menggunakan SMTP dengan enkripsi TLS), serta modul manajemen sesi dan hak akses berbasis peran (RBAC).

3.3. Implementasi Sistem

Sistem dikembangkan menggunakan teknologi frontend berupa HTML, CSS, dan JavaScript, serta backend menggunakan PHP dengan framework CodeIgniter. Untuk database, sistem ini menggunakan MySQL guna menyimpan data pengguna, OTP, dan log aktivitas. Layanan email untuk pengiriman OTP memanfaatkan SMTP dengan TLS. Tahapan implementasi meliputi pembuatan form registrasi dan login, diikuti dengan integrasi sistem pengiriman OTP via email. Setelah itu, dilakukan penerapan mekanisme RBAC pada dashboard dan pengembangan log aktivitas untuk monitoring.

3.4. Pengujian Sistem

Pengujian dilakukan dengan dua pendekatan utama. Pendekatan pertama adalah Pengujian Fungsional untuk memastikan semua fitur berjalan sesuai rancangan. Pendekatan kedua adalah Pengujian Keamanan, yang melibatkan

simulasi serangan seperti *credential theft* dan *insider threat* untuk mengevaluasi ketahanan sistem. Pengujian ini juga mencakup evaluasi terhadap kecepatan pengiriman OTP, ketepatan verifikasi kode, dan efektivitas keterbatasan akses berdasarkan peran.

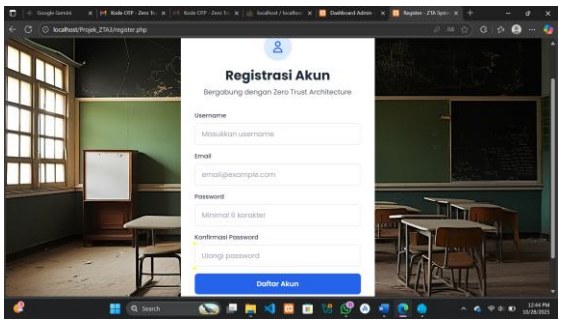
4. HASIL DAN PEMBAHASAN

4.1 Implementasi Sistem

Proyek ini menghasilkan sebuah sistem Double Authentication pada website dengan menerapkan konsep Zero Trust Architecture (ZTA). Sistem dibangun untuk memastikan setiap proses login pengguna melalui verifikasi berlapis, sehingga tidak ada entitas yang langsung dipercaya tanpa proses validasi tambahan. Proses utama sistem terdiri dari beberapa tahapan:

4.1.1 Registrasi Akun

Pengguna melakukan registrasi dengan mengisi data berupa username, password, dan alamat email. Email digunakan sebagai sarana pengiriman kode OTP (One-Time Password) yang akan dipakai untuk verifikasi saat login. Proses registrasi ini memastikan bahwa setiap akun yang dibuat memiliki alamat email valid dan unik, sehingga sistem dapat mengenali identitas pengguna dengan benar.

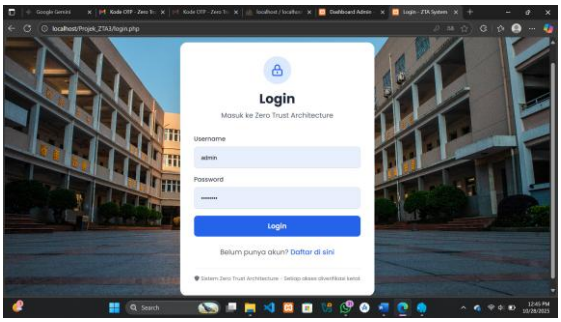


Gambar 2. Tampilan Registrasi Akun

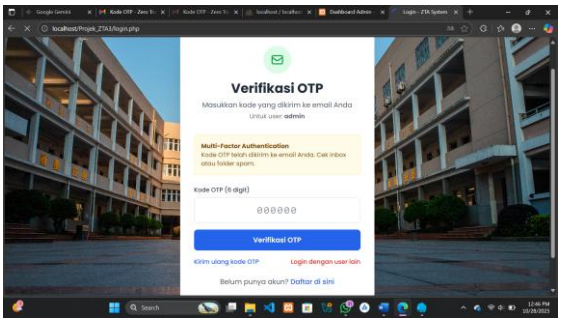
4.1.2 Login dan Verifikasi OTP

Setelah akun berhasil dibuat, pengguna dapat melakukan login dengan username dan password yang telah didaftarkan. Namun, sistem tidak langsung memberikan akses meskipun kredensial benar. Website akan mengirimkan kode OTP ke email pengguna untuk diverifikasi terlebih dahulu.

Kode OTP bersifat acak dan hanya berlaku satu kali. Jika kode yang dimasukkan tidak sesuai, maka pengguna tidak dapat melanjutkan ke tahap berikutnya. Langkah ini menjadi inti dari prinsip *Never Trust, Always Verify* pada model ZTA, di mana setiap akses harus diverifikasi lebih dari satu kali.



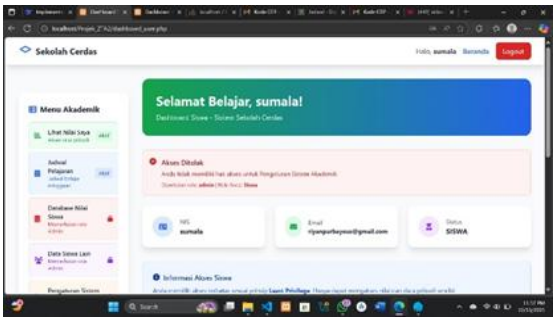
gambar 3. Tampilan Login



Gambar 4.Tampilan verifikasi kode OTP

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

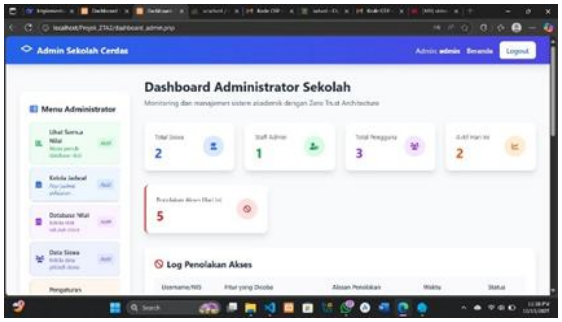
Setelah proses autentikasi ganda berhasil, pengguna akan diarahkan ke halaman dashboard. Dalam sistem ini terdapat dua peran utama, yaitu **user** dan **admin**.



Gambar 5. Tampilan Dashboard User

Role User hanya memiliki akses terbatas pada beberapa fitur. Beberapa menu ditampilkan dengan tanda kunci, menandakan bahwa fitur

tersebut tidak dapat digunakan oleh pengguna biasa.

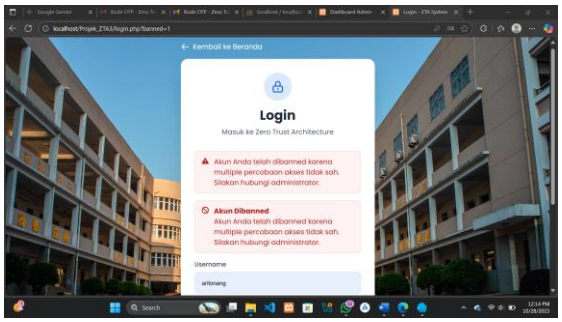


Gambar 6. Tampilan Dashboard Admin

Role Admin memiliki hak akses yang lebih luas. Admin dapat melihat daftar seluruh pengguna, memantau aktivitas login seperti status berhasil, menunggu OTP, maupun logout dari sistem. Pembagian hak akses ini bertujuan untuk membatasi wewenang setiap pengguna agar sesuai dengan tanggung jawab dan kebutuhan masing-masing.

4.1.4 Pemberian Sanksi Pada Pelanggaran Sistem

Sistem tentunya memiliki pertahanan tersendiri yang dapat dikatakan tidak sepenuhnya bergantung pada kontrol admin, contohnya semisal admin tidak dalam status online dalam monitoring. Pada penelitian ini sistem yang dikembangkan mempunyai fitur *autoban* yang akan diberikan pada para user yang melakukan pelanggaran hak akses lebih dari batas wajar.

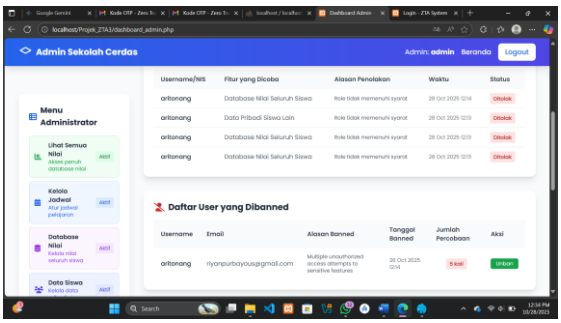


Gambar 7. Akun user yang terkena autoban setelah pelanggaran akses lebih dari batas wajar

Pada bagian diatas dapat dilihat bahwa user yang melakukan pelanggaran hak akses lebih dari batas wajar, maka sistem akan langsung melakukan ban pada akun user secara otomatis sehingga user tidak akan bisa mengakses sistem kembali. Untuk membuka ban yang diberikan sistem, diharuskan untuk melalui perantara admin sistem.

4.1.5 Monitoring Dashboard Admin

Dari bagian sebelumnya dapat diketahui user yang melakukan pelanggaran hak akses melebihi batas wajar, maka sistem akan secara otomatis memberikan ban yang bertujuan untuk "mengusir" user dari sistem. Disini admin juga memiliki wewenang untuk membuka *ban* pada akun user jika semisal user sudah menghubungi administrator.



Gambar 8. Tampilan dashboard admin ketika terdapat user yang terkena ban

Aktivitas user yang terkena ban akan tercatat pada log sistem, sebelumnya sistem mencatat percobaan yang dilakukan user dalam melakukan pelanggaran akses, lalu sistem akan melakukan autoban dan menampilkan user yang terkena ban. Sehingga admin dapat secara real-time melakukan monitoring dan mengambil keputusan yang tepat seperti halnya melakukan "unban" pada akun user yang terkena ban sebelumnya.

4.2 Evaluasi Keamanan Sistem

Beberapa skenario pengujian dilakukan untuk memastikan ketahanan sistem terhadap ancaman umum. Skenario pertama adalah Pencurian Akun (*Credential Theft*), di mana diuji apabila *username* dan *password* diketahui pihak lain. Hasilnya, pelaku tetap tidak bisa *login* karena sistem akan meminta OTP yang hanya dikirim ke email pengguna asli. Skenario kedua adalah Ancaman dari Dalam Sistem (*Insider Threats*). Dalam skenario ini, hak akses admin dibatasi hanya untuk melihat log aktivitas dan daftar pengguna, tanpa kemampuan mengubah data *login* pengguna

lain. Hasil pengujian secara keseluruhan menunjukkan bahwa sistem mampu menangani berbagai kemungkinan serangan tersebut dengan efektif.

4.3 Pembahasan Umum

Secara keseluruhan, hasil implementasi dan pengujian menunjukkan bahwa sistem Double Authentication menggunakan OTP Email dengan model Zero Trust Architecture berhasil meningkatkan keamanan website secara signifikan. Sistem ini memastikan setiap permintaan akses diverifikasi lebih dari satu kali, dan setiap pengguna hanya dapat mengakses fitur sesuai perannya. Pendekatan ini juga membuktikan bahwa prinsip Zero Trust dapat diterapkan secara sederhana dan efisien pada sistem berbasis web tanpa memerlukan perangkat keras tambahan. Selain meningkatkan keamanan terhadap serangan berbasis kredensial, sistem ini juga memperkuat kepercayaan pengguna terhadap perlindungan data pribadi mereka.

5. KESIMPULAN

Dari hasil perancangan dan implementasi yang telah dilakukan, dapat disimpulkan bahwa sistem *Double Authentication* menggunakan OTP Email berbasis *Zero Trust Architecture* (ZTA) mampu meningkatkan tingkat keamanan akses pada website secara signifikan. Sistem ini berhasil menerapkan konsep *Never Trust, Always Verify* di mana setiap pengguna, meskipun sudah memiliki kredensial yang valid, tetap harus melewati proses autentikasi tambahan melalui OTP yang dikirim ke email pribadi.

Beberapa poin penting yang dapat disimpulkan. Pertama, proses autentikasi ganda mampu mencegah akses tidak sah akibat pencurian *username* dan *password*. Kedua, penggunaan OTP yang dikirim melalui email terbukti efektif sebagai lapisan verifikasi tambahan, karena bersifat unik, hanya berlaku satu kali, dan memiliki batas waktu tertentu. Selanjutnya, penerapan prinsip *Zero Trust* seperti *least privilege access*, *continuous verification*, dan *audit monitoring* membuat sistem lebih tangguh terhadap ancaman dari luar maupun dalam jaringan. Terakhir, pembagian hak akses antara pengguna dan admin berhasil diterapkan dengan baik, sehingga peran masing-masing pengguna dapat dibatasi sesuai kebutuhan.

Secara keseluruhan, sistem ini berhasil menunjukkan bahwa penerapan ZTA dengan mekanisme *Double Authentication* berbasis OTP email dapat diimplementasikan secara efektif pada website untuk meningkatkan keamanan data dan validitas identitas pengguna tanpa mengorbankan kenyamanan dalam penggunaan.

Berkaitan dengan pengembangan sistem, agar nantinya sistem yang dirancang dapat dikembangkan lebih baik dimasa yang akan datang, kami memberikan beberapa saran yang mungkin berguna untuk pengembangan selanjutnya. Pertama, karena perkembangan teknologi sudah sangat pesat, maka integrasi kecerdasan buatan (AI) bukanlah pilihan yang buruk. Dengan AI sistem dapat melakukan deteksi anomali berbasis perilaku pengguna untuk mengenali aktivitas *login* yang tidak wajar.

DAFTAR PUSTAKA

[1]Gupta, A., Khan, H. U., Nazir, S., Shafiq, M., & Shabaz, M. (2023). *Metaverse security: Issues, challenges and a viable ZTA model.* Electronics,12(391).https://doi.org/10.3390/electronics12020391

[2]Khan, M. J. (2023). *Zero trust architecture: Redefining network security paradigms in the digital age.* World Journal of Advanced Research and Reviews, 19(3), 105–116. https://doi.org/10.30574/wjarr.2023.19.3.1785

[3]Ojo, A. O. (2025). *Adoption of zero trust architecture (ZTA) in the protection of critical infrastructure.* Path of Science, 11(1), 5001–5009. https://doi.org/10.22178/pos.113-2

[4]Phanireddy, S. (2023). *AI-powered zero trust architecture for web app security.* International Journal of Innovative Research in Management, Physics & Sciences, 11(4), 1–6.

[5]Sasada, T., Taenaka, Y., Kadobayashi, Y., & Fall, D. (2024). *Web-biometrics for user authenticity verification in zero trust access control.* IEEE Access, 12, 129611–129623. https://doi.org/10.1109/ACCESS.2024.3413696

[6] M. A. Fauzi, A. I. Hadiana, and F. R. Umbara, "Penambahan Fitur Multi-Factor Authentication dalam Studi Kasus Sistem Informasi Rekam Medis Rumah Sakit," *JATI (Jurnal Mahasiswa Teknik Informatika)*, vol. 7, no. 4, Agu. 2023.

[8] M. Rusdan and M. Sabar, "Analisis dan Perancangan Jaringan Wireless Dengan Wireless Distribution System Menggunakan User Authentication Berbasis Multi-Factor Authentication," *JOINT (Journal of Information Technology)*, vol. 2, no. 1, Feb. 2020.

[9] D. Aribowo, J. Damayanti, M. Sadewa, S. R. Nabila, and Sarnata, "Risiko Keamanan dan Kerentanan Jaringan Transmisi Listrik Terhadap Serangan Siber pada Infrastruktur

[7] R. W. Darmawan, Irawan, and S. Petriansyah, "Analisis Adaptif Zero Trust Architecture (ZTA) Berbasis Machine Learning untuk Deteksi Intrusi pada Jaringan IoT dalam Infrastruktur Kritis," *Journal of Artificial Intelligence and Digital Business (RIGGS)*, vol. 3, no. 4, 2025.

[10] M. Akbar et al., "Perancangan Sistem Informasi Manajemen Magang Mahasiswa Manajemen Informatика Universitas Sriwijaya Berbasis Website," *JITET (Jurnal Informatika dan Teknik Elektro Terapan)*, vol. 13, no. 3, 2025.

[11] I. P. A. E. D. Udayana et al., "Pelatihan dan Penerapan Sistem Single Sign-On untuk Meningkatkan Efisiensi dan Keamanan Layanan Digital," *KOMET: Kolaborasi Masyarakat Berbasis Teknologi*, vol. 2, no. 2, Okt. 2025.

[12] A. Nuryasa and I. Suharjo, "Implementasi Traefik sebagai Reverse Proxy dengan Prinsip Zero Trust," *Jutisi: Jurnal Ilmiah Teknik Informatika dan Sistem Informasi*, vol. 13, no. 1, Apr. 2024.

[13] R. Atmawijaya and U. Radiyah, "Perancangan Autentikasi Multi Faktor dengan Pengenalan Wajah dan FIDO (Fast Identity Online)," *INTI NUSA MANDIRI*, vol. 19, no. 1, Agu. 2024.

[14] R. Rahman and A. F. Rahman, "Penerapan Zero Trust Network Access (ZTNA) dengan penggunaan CAPTCHA pada website umum," *Technology Sciences Insights Journal*, vol. 1, no. 2, Nov. 2024.
Energi Terdistribusi," *SURYA TEKNIKA*, vol. 11, no. 2, Des. 2024.

[15] A. P. Walidin, F. P. Putri, and D. Kiswanto, "Kali Linux sebagai Alat Analisis Keamanan Jaringan Melalui Penggunaan Nmap, Wireshark, dan Metasploit," *JATI (Jurnal Mahasiswa Teknik Informatika)*, vol. 9, no. 1, Feb. 2025.