JITET (Jurnal Informatika dan Teknik Elektro Terapan)
Vol. 14 No. 1, pISSN: 2303-0577 eISSN: 2830-7062 http://dx.doi.org/10.23960/jitet.v14i1.8209

IMPLEMENTASI ZERO TRUST ARCHITECTURE DENGAN JUST IN TIME AUTHENTICATION TOKEN PADA WEBSITE E - WALLET

Thania Dealva Arsyad[1*], Dedy Kiswanto[2] Ali Afrrahman S.Effendi[3]

[1,2]Universitas Negeri Medan; Jl. William Iskandar Ps. V, Kenangan Baru, Kec. Percut Sei Tuan, Kabupaten Deli Serdang; 088213072463
[3]Universitas Negeri Medan; Jl. William Iskandar Ps. V, Kenangan Baru, Kec. Percut Sei Tuan, Kabupaten Deli Serdang; 085276983434

Keywords:
Zero Trust Architecture;
Just In Time;
Two Factor Authentication.

Corespondent Email:
thaniadealvaarsyad@gmail.com

Abstrak. Seiring meningkatnya popularitas e-wallet, risiko keamanan terhadap data sensitif pengguna juga semakin tinggi. Model keamanan tradisional berbasis perimeter tidak lagi memadai untuk menghadapi ancaman siber modern, sementara implementasi Zero Trust Architecture (ZTA) masih menyisakan celah pada manajemen sesi token yang berdurasi panjang. Penelitian ini bertujuan untuk merancang dan membangun sistem keamanan yang lebih kuat dengan mengintegrasikan ZTA dengan Just-in-Time (JIT) Authentication Token. Metode penelitian yang digunakan adalah Research & Development (R&D) dengan model ADDIE (Analysis, Design, Development, Implementation, Evaluation) untuk mengembangkan prototipe website e-wallet. Hasilnya adalah sebuah sistem yang berhasil menerapkan verifikasi berlapis, di mana setiap permintaan akses dan transaksi kritis divalidasi melalui autentikasi dua faktor (2FA) dan token JIT yang memiliki masa aktif sangat singkat, yakni lima menit. Pendekatan ini terbukti secara efektif meminimalkan permukaan serangan dan mengurangi risiko penyalahgunaan akses secara drastis. Berdasarkan *blackbox* yang sudah dilakukan dengan tingkat akurasi mencapai 80%, implementasi ZTA dengan token JIT menawarkan solusi keamanan yang lebih dinamis, adaptif, dan dapat diandalkan untuk melindungi ekosistem keuangan digital.

Abstract. *As e-wallets grow in popularity, the security risks to users' sensitive data also increase. Traditional perimeter-based security models are no longer adequate to deal with modern cyber threats, while the implementation of Zero Trust Architecture (ZTA) still leaves gaps in the management of long-duration token sessions. This study aims to design and build a stronger security system by integrating ZTA with Just-in-Time (JIT) Authentication Tokens. The research method used is Research & Development (R&D) with the ADDIE model (Analysis, Design, Development, Implementation, Evaluation) to develop an e-wallet website prototype. The result is a system that successfully implements layered verification, where every access request and critical transaction is validated through two-factor authentication (2FA) and JIT tokens that have a very short active period of five minutes. This approach has been proven to effectively minimize the attack surface and drastically reduce the risk of access abuse. The implementation of ZTA with JIT tokens offers a more dynamic, adaptive, and reliable security solution to protect the digital financial ecosystem.*

1. PENDAHULUAN

Perkembangan teknologi informasi yang pesat telah mendorong transformasi signifikan dalam sektor keuangan, memunculkan beragam layanan – layanan yang inovatif seperti *mobile banking*, *fintech*, dan dompet digital (*e-wallet*). Layanan *e-wallet* secara khusus telah menjadi bagian integral dari transaksi sehari-hari masyarakat karena menawarkan kemudahan dan kecepatan yang tidak dapat ditandingi oleh metode konvensional [1]. Namun, di balik efisiensi yang ditawarkan, platform ini menyimpan data pengguna yang sangat sensitif, termasuk informasi pribadi dan saldo finansial, menjadikannya target utama bagi pelaku kejahatan siber [2]. Ancaman seperti *phishing*, *malware*, dan rekayasa sosial terus berevolusi, sehingga menuntut adanya paradigma keamanan yang lebih kuat dan adaptif untuk melindungi ekosistem keuangan digital. Model keamanan tradisional, yang sering dianalogikan sebagai benteng pertahanan (*perimeter-based defense*), terbukti tidak lagi memadai untuk menghadapi lanskap ancaman modern. Dalam era digital yang semakin berkembang, keamanan jaringan menjadi salah satu aspek krusial yang harus diperhatikan. Banyaknya aktivitas pertukaran data secara online membuka celah bagi pihak tidak bertanggung jawab untuk melakukan berbagai jenis serangan siber. [3]

Pendekatan ini bekerja dengan asumsi bahwa segala sesuatu di dalam jaringan dapat dipercaya, sementara ancaman hanya berasal dari luar. Kelemahan fundamental ini menjadi nyata ketika seorang penyerang berhasil menembus sebuah sistem, karena mereka dapat bergerak dengan leluasa di dalam sistem untuk mengakses data-data krusial [4]. Oleh karena itu, industri keamanan siber beralih ke pendekatan yang lebih modern, yaitu *Zero Trust Architecture* (ZTA). ZTA merupakan sebuah paradigma keamanan yang menolak konsep kepercayaan implisit berdasarkan lokasi jaringan. Fondasi utama dari ZTA adalah prinsip jangan pernah percaya, selalu verifikasi (*never trust, always verify*), yang dimana mengharuskan setiap permintaan akses untuk melalui proses pemeriksaan ketat tanpa terkecuali, baik itu berasal dari dalam maupun luar jaringan [5]. Terdapat beberapa penelitian sebelumnya telah menunjukkan efektivitas ZTA dalam meningkatkan postur keamanan jaringan dengan menerapkan JIT (*Just In Time*) sebagai tambahan keamanan agar mencegah pengguna tidak terlalu lama atau tidak selalu menggunakan sebuah website yang telah diprogram. Seperti pada penelitian yang telah dilakukan oleh Lorenza [6], penelitian ini secara spesifik mengenai metode *Just In Time* (JIT), tinjauan pustaka menjelaskan bahwa JIT adalah strategi pengelolaan yang bertujuan menghilangkan pemborosan dengan cara memproduksi sesuatu sesuai dengan apa yang dibutuhkan, kapan dibutuhkan, dan dalam jumlah yang tepat. Implementasi JIT terbukti dapat mengurangi biaya penyimpanan secara signifikan dan dapat menghindari kelebihan persediaan yang tidak terlalu perlu. Lebih lanjut, penerapan JIT juga dapat meningkatkan efisiensi – efisiensi operasional dan mengurangi pemborosan dalam proses produksi serta dapat meningkatkan keamanan.

Analisis kesenjangan (*gap analysis*) dari literatur yang ada menunjukkan bahwa meskipun ZTA adalah kerangka kerja yang superior, implementasinya seringkali masih menyisakan celah keamanan, terutama terkait manajemen sesi dan hak akses. Setelah pengguna berhasil diautentikasi, token akses yang diberikan seringkali memiliki masa berlaku yang panjang. Jika token ini berhasil dicuri, penyerang memiliki jendela waktu yang cukup luas untuk mengeksploitasi sistem [7]. Inilah letak kebaruan dan urgensi dari penelitian ini. Kami mengusulkan sebuah pendekatan keamanan yang lebih dinamis dengan mengintegrasikan ZTA dengan *Just-in-Time (JIT) Authentication Token*. Berbeda dengan token sesi tradisional, token JIT berfungsi seperti kunci akses sekali pakai yang dibuat secara spesifik saat dibutuhkan, hanya berlaku untuk satu tugas tertentu, dan memiliki masa hidup yang sangat singkat, seringkali hanya dalam hitungan menit atau bahkan detik. Pendekatan ini secara drastis meminimalkan permukaan serangan, karena bahkan jika sebuah token berhasil dicuri, kegunaannya

sangat terbatas dan akan kedaluwarsa dengan cepat. Teknologi yang mendasari token ini, seperti *JSON Web Token* (JWT), menyediakan mekanisme yang efisien untuk pertukaran informasi secara aman antara klien dan server setelah proses otentikasi [8]. Berdasarkan *gap analysis* yang ada maka tujuan penerapannya akan menggunakan token otentikasi *Just In Time* (JIT), yang berfungsi seperti kunci akses sekali pakai. Token ini dibuat hanya saat dibutuhkan, berlaku sangat singkat, dan hanya untuk satu tugas spesifik. Metode ini jauh lebih aman karena jika token dicuri, kegunaannya sangat terbatas dan cepat kedaluwarsa.

Oleh karena itu, penelitian ini bertujuan untuk menggabungkan sebuah prinsip Zero Trust dengan teknologi token JIT untuk membangun sistem keamanan *website e-wallet* yang jauh lebih kuat, adaptif, dan dapat meningkatkan kepercayaan pengguna.

2. TINJAUAN PUSTAKA

2.1. *Zero Trust Architecture*

Zero Trust Architecture adalah pendekatan keamanan jaringan yang menolak kepercayaan otomatis terhadap pengguna atau perangkat dalam dan luar jaringan organisasi. Setiap permintaan akses harus diverifikasi secara menyeluruh mengenai konteks, identitas, dan perangkat. Metode ini mengurangi akses yang berlebihan dan menerapkan segmentasi tidak percaya kepada siapapun untuk mencegah sebuah penyusupan dan kebocoran data [9].

Penerapan *Zero Trust Architecture* memiliki berbagai upaya verifikasi. Setiap upaya akses harus selalu diautentikasi dan diotorisasi secara menyeluruh. Proses verifikasi ini tidak hanya berdasarkan identitas pengguna, tetapi juga mempertimbangkan berbagai sinyal atau atribut lain. ZTA mengasumsikan bahwa ancaman dapat berasal dari mana saja, sehingga perimeter keamanan tidak lagi terbatas pada batas fisik kantor, melainkan meluas hingga mencakup setiap pengguna, perangkat, dan koneksi [10].

2.2. *Just In Time* (JIT)

Sistem Produksi Just In Time atau JIT sering disebut Sistem Produksi Tepat Waktu karena istilah ini diterjemahkan langsung ke dalam bahasa Indonesia sebagai Tepat Waktu. Tepat Waktu berarti bahwa semua bahan baku yang akan diolah harus tiba dengan tepat waktu dan dalam jumlah yang tepat. Selain itu, semua barang jadi harus siap diproduksi sesuai dengan jumlah yang dibutuhkan oleh pelanggan pada waktu yang tepat. Oleh karena itu, tingkat stok atau persedian bahan baku, bahan pendukung, komponen, bahan semi-jadi (WIP atau Work In Progress), dan barang jadi akan dijaga pada tingkat yang paling rendah [11].

Sistem produksi yang dikenal sebagai sistem just in time (JIT) dapat membantu memenuhi permintaan pelanggan dalam ketepatan waktu sesuai dengan permintaan pelanggan. JIT juga dapat mengurangi waktu seperti waktu tunggu, bahan produksi yang mengendap, dan juga pemesanan jumlah - jumlah produksi yang memang tidak terlalu diperlukan.Menghindari pemborosan dan dapat terus meningkatkan produktivitas adalah tujuan utama segera [12]. Produksi adalah kemampuan setiap individu, sistem, atau perusahaan untuk menghasilkan jumlah barang - barang dan jasa setinggi mungkin dengan menggunakan sumber daya secara efisien dan efektif [13].

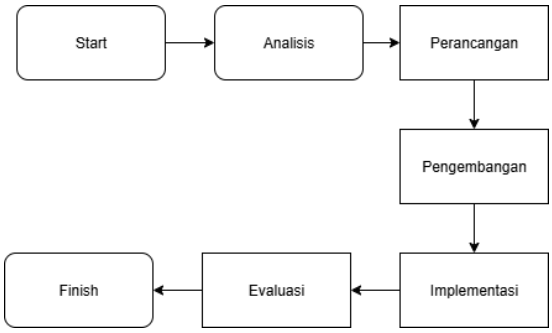
2.3. *Two Factor Authentication* (2FA)

Two-Factor Authentication merupakan fitur keamanan yang menggunakan dua metode untuk proses autentikasi, artinya pengguna harus memasukkan informasi tambahan agar dapat mengakses sumber daya pada sistem. Proses autentikasi pengguna menjadi ganda berawal dari memasukkan username dan password saat login, kemudian autentikasi dilanjutkan dengan memasukkan token yang dikirimkan ke nomor telepon atau email yang terhubung dengan akun pengguna [14].

Sistem Two-factor authentication ini dapat dirancang dengan menggunakan kombinasi username dan password serta divalidasikan kepemilikannya dengan password dinamis One-time password (OTP). One-time password adalah kata sandi yang valid dan hanya bisa digunakan satu kali login pada komputer atau alat digital lainnya. Salah satu metode untuk membangkitkan One-time password adalah algoritma Time-Based One-time password (TOTP), algoritma ini memiliki kemampuan untuk menghasilkan password sekali pemakaian [15].

3. METODE PENELITIAN

Penelitian ini menggunakan metode penelitian dengan pendekatan *Research & Development* (R&D) untuk mengembangkan sebuah aplikasi E - *wallet* berbasis *web app*. Metodologi pengembangan yang digunakan adalah model ADDIE (*Analysis, Design, Development, Implementation, Evaluation*) yang merupakan pendekatan sistematis dalam desain dan pengembangan program pendidikan. Model ADDIE merupakan kerangka kerja desain instruksional atau pengembangan sistem yang sistematis dan berurutan, sering kali digunakan untuk memandu proses penelitian pengembangan. Model ini terdiri dari lima fase utama yaitu Analisis (*Analysis*), Perancagan (*Design*), Pengembangan (*Development*), Implementasi (*Implementation*) dan Evaluasi (*Evaluation*) [16]. Tahapan penelitian akan digambarkan dalam diagram alur yang terdapat pada gambar 1.



Gambar 1. Tahapan Penelitian

3.1. Analisis

Tahapan pertama adalah tahap analisis. Yang dimana pada tahap ini berfokus pada identifikasi masalah, penentuan kebutuhan, dan studi kelayakan. Pada konteks penelitian ini, tahap analisis mencakup analisis kesenjangan celah keamanan dalam manajemen sesi ZTA, analisis kebutuhan pengguna dan analisis sumber daya atau teknologi pendukung yang akan digunakan seperti ZTA dan JIT. Hasil dari tahapan ini adalah penentuan masalah, tujuan dan kebutuhan yang harus dipenuhi oleh solusi yang diusulkan.

3.2. Perancangan

Setelah tahapan analisis kebutuhan selesai, tahapan berikutnya yang akan dilakukan pada penelitian ini membuat *design* yang akan diterapkan kedalam aplikasi yang berbentuk *web app*. Tahapan ini meliputi perancangan *Zero Trust Architecture* (ZTA), perancangan model *Just In Time Authentication Token* dan perancangan alur kerja (*workflow*) bagaimana token JIT akan diintegrasikan dengan proses autentikasi pada *website e - wallet.*

3.3. Pengembangan

Setelah tahapan perancangan dan tahapan analisis tahapan yang berikutnya adalah tahapan pengembangan. Pada tahapan ini semua komponen sistem dibangun dan diuji secara internal. Langkah - langkahnya meliputi penulisan kode program atau kode sumber (*coding*) untuk implementasi ZTA dan mekanisme token JIT, integrase semua modul dan melakukan uji coba untuk *website e - wallet*.

3.4. Implementasi

Tahapan yang berikutnya adalah tahapan implementasi, yang dimana pada tahapan ini mencakup installasi sistem ZTA yang terintegrasi JIT token pada server simulasi *e - wallet*, serta pengumpulan data melalui uji coba fungsional dan peforma. Pada tahap implementasi memastikan bahwa sistem berfungsi sesuai dengan hasil yang diharapkan, terutama dalam meminimalkan permukaan serangan dengan token yang memiliki masa berlaku sangat singkat.

3.5. Evaluasi

Tahapan yang terakhir adalah tahapan evaluasi. Pada tahapan ini mencakup uji coba sistem (pengujian fungsionalitas dan juga keamanan), analisis data - data dari hasil implementasi, dan perbandingan dengan sistem konvensional. Pada tahapan ini memastikan bahwa hasil penelitian yaitu menggabungkan ZTA dengan token JIT dapat meningkatkan keamanan jaringan.

4. HASIL DAN PEMBAHASAN

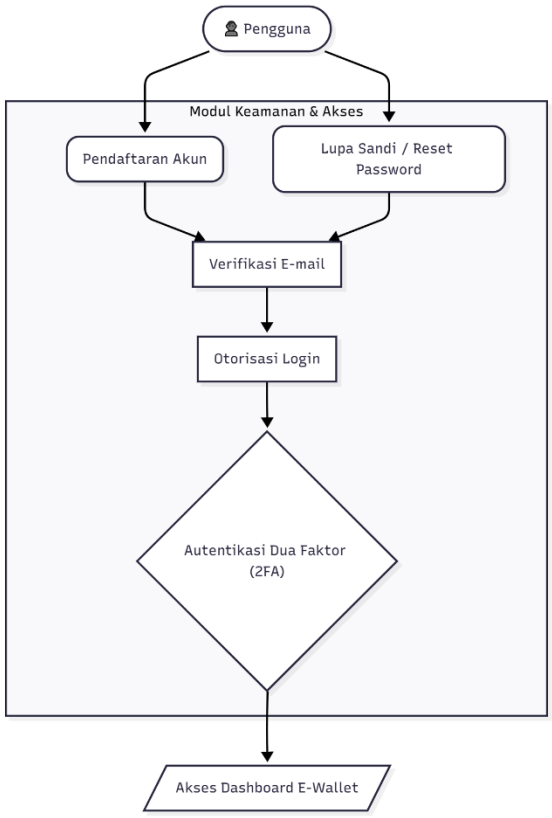
4.1. Analisis

Pada tahapan ini merupakan fondasi awal yang krusial, berfokus pada identifikasi mendalam terhadap permasalahan keamanan pada *website e-wallet* dan penentuan kebutuhan solusi yang inovatif. Penelitian ini berangkat dari sebuah analisis kesenjangan (*gap analysis*) yang menunjukkan bahwa model keamanan tradisional (*perimeter-based defense*) telah

terbukti tidak lagi memadai untuk menghadapi lanskap ancaman siber modern. Model lama tersebut memiliki kelemahan fundamental, yakni asumsi kepercayaan implisit terhadap entitas di dalam jaringan , yang memungkinkan penyerang bergerak leluasa setelah berhasil menembus sistem. analisis mengidentifikasi bahwa meskipun *Zero Trust Architecture* (ZTA) adalah pendekatan yang superior, implementasi ZTA yang ada masih menyisakan celah keamanan, terutama terkait manajemen sesi dan hak akses. Secara spesifik, token akses tradisional seringkali memiliki masa berlaku yang panjang, sehingga jika dicuri, penyerang memiliki jendela waktu yang luas untuk mengeksploitasi sistem. Oleh karena itu, kebutuhan mendesak yang teridentifikasi adalah pergeseran paradigma keamanan dari token sesi berjangka panjang menuju mekanisme yang lebih dinamis dan terikat waktu. Berdasarkan hasil analisis inilah, penelitian ini bertujuan untuk mengusulkan dan mengimplementasikan solusi yang lebih kuat, yaitu integrasi ZTA dengan *Just-in-Time* (JIT) *Authentication Token*.

4.2. Perancangan

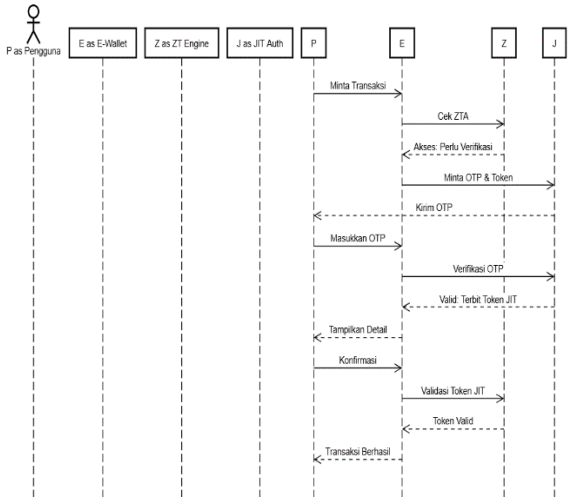
Pada perancangan dibuat sebuah diagram alur untuk menjelaskan bagaimana rancangan dari sistem yang akan dikembangkan oleh peneliti akan dibuat. Untuk menjelaskan alur kerja sistem keamanan yang diusulkan, berikut disajikan dua diagram utama, yaitu diagram alur pengguna untuk proses login dan diagram urutan untuk penerapan token JIT-OTP dalam arsitektur ZTA.



Gambar 2. Use Case Diagram

Dapat dilihat pada gambar 2, terdapat *use case diagram* yang memaparkan secara sistematis tahapan yang dilalui pengguna untuk mendapatkan akses kedalam web *e - wallet*. Proses dimulai ketika pengguna berinteraksi dengan web. Terdapat dua pilihan dapat dipilih oleh pengguna, yang pertama ada pendaftaran untuk pengguna baru atau lupa sandi bagi pengguna yang sudah memiliki akun tapi lupa kata sandinya. Setelah memilih salah satu pilihan tersebut proses berikutnya akan dilanjutkan ketahap verifikasi *E- Mail* yang dimana pada tahap verifikasi *e - mail* pengguna untuk memvalidasi identitas pengguna. Kemudian verifikasi ini akan mengarah pada otorisasi login. Otorisasi login merupakan tahap yang penting dikarenakan otorisasi login adalah penentuan apakah kredensial yang diberikan pengguna sah untuk mengakses sistem. Setelah itu pengguna akan diarahkan ke dashboard verifikasi 2 tahap. Pada tahapan ini pengguna harus memasukkan kode OTP yang telah dikirim melalui *e-mail*. Jika *two step - verification* berhasil atau tidak diaktifkan/tidak

diperlukan, alur akan berakhir pada hasil akhir, yaitu Akses Dashboard *E-Wallet*.



Gambar 3. Sequence Diagram

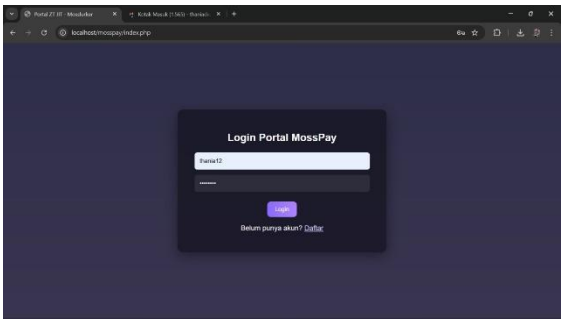
Pada gambar 3 terdapat *sequence diagram* yang dimana pada diagram ini menjelaskan proses otentikasi transaksi yang dilakukan pada program. *sequence diagram* ini akan membantu menggambarkan ZTA dengan token JIT dan OTP yang akan mengilustrasikan interaksi komponen utama dalam proses otentikasi transaksi yang mengintegrasikan ZTA, JIT Token, dan OTP. Proses ini menekankan bahwa setiap permintaan akses (dalam hal ini, transaksi) memerlukan verifikasi ulang.

4.3. Pengembangan

Pada tahap pengembangan berfokus pada mekanisme JIT Token untuk mengamankan transaksi kritis seperti *top up* saldo. Mekanisme ini melibatkan integrasi teknologi seperti JSON Web Token (JWT) untuk menghasilkan token yang memiliki karakteristik kunci akses sekali pakai (*single-use access key*), yang dibuat secara spesifik saat dibutuhkan dan hanya berlaku untuk satu tugas tertentu. Aspek krusial dari pengembangan JIT Token adalah penetapan *Time-to-Live* (TTL) yang sangat singkat (misalnya 5 menit) pada token transaksi, yang secara drastis membatasi jendela waktu eksploitasi (*window of exploitation*) bahkan jika token berhasil dicuri oleh penyerang.

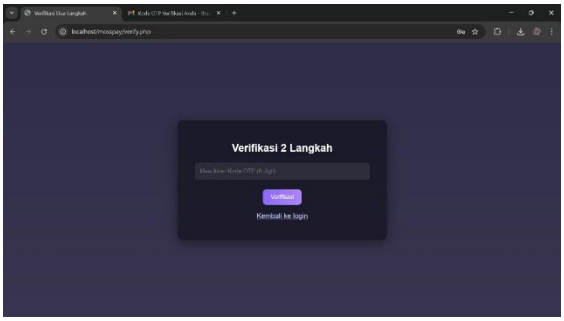
4.4. Implementasi

Implementasi dimulai dengan antarmuka Login Portal MossPay . Antarmuka ini dirancang sederhana untuk memfasilitasi otentikasi awal pengguna. Setelah pengguna memasukkan nama pengguna dan kata sandi yang valid, sistem tidak langsung memberikan akses penuh ke dashboard website, melainkan menerapkan prinsip *never trust, always verify* dari ZTA melalui proses Verifikasi 2 Langkah. Tampilan login *form* dapat dilihat pada gambar 4.



Gambar 4. Login Form

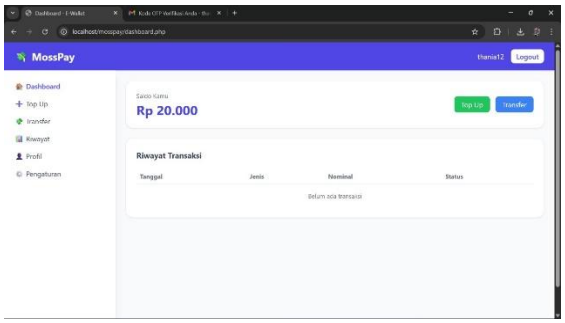
Berikutnya diimplementasikan *Two Factor Authentication* guna menerapkan ZTA pada program yang telah dikembangkan. *Two Factor Authentication* yang digunakan pada penelitian ini menggunakan kode OTP. Yang dimana kode OTP akan diberikan kepada *e-mail* pengguna. Form OTP dapat dilihat pada gambar 5.



Gambar 5. Form OTP

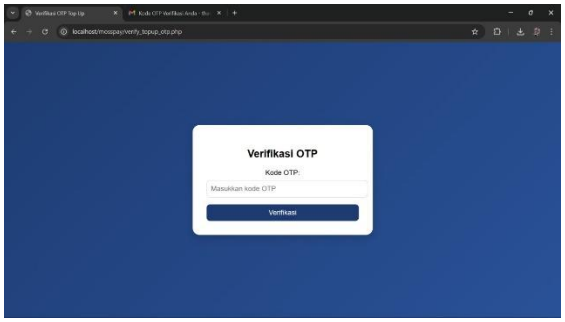
Setelah memasukkan kode OTP pada *website* pengguna akan diarahkan kedalam *dashboard*. Pada tampilan *dashboard* terdapat Navigasi menu di sisi kiri memuat opsi seperti *Dashboard*, *Top Up*, *Transfer*, riwayat, profil,

dan pengaturan. pada panel utama, tertera Saldo Kamu sebesar Rp 20.000. Pengguna dapat segera melakukan *Top Up* atau *Transfer* melalui tombol di samping nominal saldo. Bagian bawah menyajikan tabel Riwayat Transaksi, yang saat ini menunjukkan keterangan Belum ada transaksi. Dashboard *website* dapat dilihat pada gambar 6.



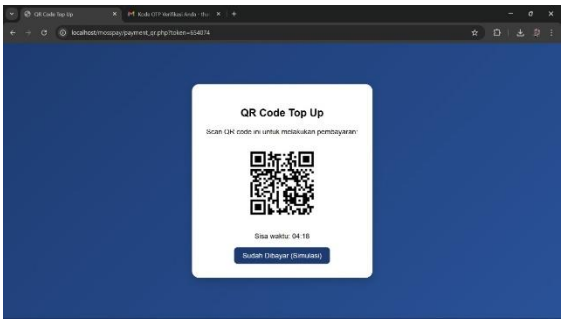
Gambar 6. Dashboard *e-wallet*

Berikutnya diimplementasikan juga OTP pada menu transaksi guna menerapkan ZTA pada program yang telah dikembangkan. *Two Factor Authentication* yang digunakan pada penelitian ini menggunakan kode OTP. Yang dimana kode OTP akan diberikan kepada *e-mail* pengguna sama seperti saat ketika pengguna mencoba melakukan login. OTP transaksi dapat dilihat pada gambar 7.



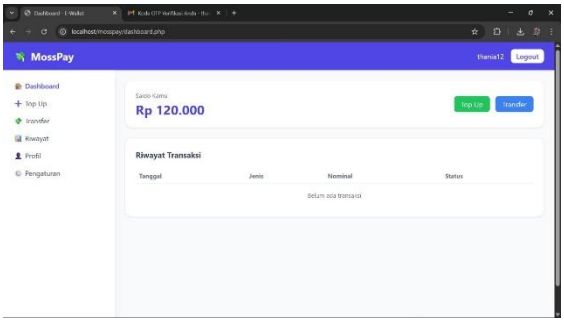
Gambar 7. Form OTP Transaksi

Setelah itu, ketika pengguna telah memasukkan kode OTP untuk melakukan transaksi, maka pengguna akan diarahkan ke sebuah QR *code.* QR *code* ini menerapkan konsep JIT Token, yang dimana token yang diberikan memiliki waktu terbatas sehingga pengguna harus melakukan scan pada QR *code* yang telah ditampilkan pada program. Implementasi JIT pada penelitian ini dapat dilihat pada gambar 8.



Gambar 8. Implementasi Token JIT

Kemudian ketika pengguna telah berhasil melakukan *scanning* kode QR maka pengguna akan diarahkan kedalam sebuah platform untuk menunjukkan bahwa *Top Up* telah berhasil dilakukan. Bukti berhasil dilakukan *top up* dapat dilihat pada *dashboard* dari *website e-wallet*. Bukti *Top Up* telah berhasil dilakukan dapat dilihat pada gambar 9.



Gambar 9. *Top Up* Berhasil

4.5. Evaluasi

Tahap evaluasi harus dilakukan untuk mengukur fungsionalitas dan keamanan sistem yang telah dikembangkan, dengan fokus utama pada pemenuhan serta persyaratan sistem (fungsionalitas) dan efektivitas penerapan prinsip JIT dan ZTA.

4.5.1 Uji *Blackbox*

Pengujian *black box* dilakukan untuk memverifikasi apakah setiap fitur dalam aplikasi *e-wallet* MossPay, terutama yang

terkait dengan mekanisme keamanan ZTA dan JIT, berfungsi sesuai dengan spesifikasi yang dirancang. Uji *blackbox* dapat dilihat pada tabel 1.

Tabel 1. Uji Blackbox

No	Modul Uji	Skenario Pengujian	Hasil Yang Diharapkan	Hasil Pengujian	Keterangan
1	Otentikasi Awal	Pengguna login dengan *username* dan *password* valid.	Sistem menampilkan halaman Verifikasi 2 Langkah (OTP) dan mengirim OTP.	Sesuai	Implementasi ZTA (verifikasi lanjutan) berhasil.
2	Verifikasi Login OTP	Memasukkan kode OTP yang benar.	Pengguna berhasil masuk ke *Dashboard* utama.	Sesuai	Akses disetujui setelah verifikasi berlapis.
3	*Top Up* Saldo	Memasukkan nominal *top up* yang valid.	Sistem meminta Verifikasi OTP Transaksi.	Sesuai	Implementasi ZTA (verifikasi per akses/transaksi) berhasil.
4	Verifikasi JIT - OTP	Memasukkan kode OTP transaksi yang benar.	Sistem menampilkan *QR Code* dengan *countdown* 5 menit	Sesuai	Pembentukan Token JIT dengan *Time-to-Live* (TTL) berhasil.
5	Kadaluwarsa Token JIT	Mencoba menggunakan QR Code setelah *countdown* 5 menit berakhir.	Transaksi ditolak /token dinyatakan tidak valid.	Sesuai	Prinsip Just-in-Time Token berhasil diterapkan.
6	Transaksi Berhasil	Melakukan simulasi pembayaran dalam batas waktu 5 menit.	Saldo pengguna diperbarui.	Sesuai	Fungsi inti sistem berjalan dengan aman.

4.5.2 Analisis Efektivitas Keamanan JIT

Selain pengujian fungsionalitas, evaluasi juga harus mempertimbangkan efektivitas peningkatan keamanan yang ditawarkan oleh Token JIT dibandingkan dengan *session token* tradisional. Token JIT, dengan masa aktif yang sangat singkat (misalnya 5 menit untuk dapat melakukan transaksi), secara signifikan dapat mengurangi risiko penyalahgunaan. Analisis Efektivitas keamanan JIT dapat dilihat pada tabel 2.

Tabel 2. Efektivitas Keamanan JIT

Parameter Keamanan	Token Sesi Tradisional	Token *Just In Time*	Peningkatan Keamanan

Masa Aktif (TTL)	Jam hingga hari	Hitungan menit/detik	Menurunkan jendela eksploitasi (*window of exploitation*) secara drastic.
Jangkauan Otorisasi	Akses penuh ke seluruh sistem	Akses spesifik untuk satu tugas	Mencegah pergerakan lateral penyerang (*lateral movement*).
Resiko Pencurian	Tinggi (masa aktif panjang)	Sangat rendah (masa aktif sangat singkat)	Memperkuat keamanan manajemen sesi.

5. KESIMPULAN

Berdasarkan penelitian dan pengembangan yang telah dilakukan, dapat ditarik beberapa kesimpulan sebagai berikut:

a. Hasil yang Diperoleh : Penelitian ini berhasil untuk mengimplementasikan arsitektur keamanan *Zero Trust Architecture* (ZTA) yang terintegrasi dengan menggunakan *Just-in-Time* (JIT) *Authentication Token* pada prototipe *website e-wallet*. Hasil pengujian *black box* yang memiliki persentase 80% dalam keamanan dalam melakukan transaksi menunjukkan bahwa semua fungsionalitas keamanan, mulai dari autentikasi dua faktor (2FA) saat login hingga verifikasi OTP dan penggunaan token JIT berbatas waktu (5 menit) untuk transaksi, berjalan sesuai dengan yang diharapkan. Implementasi ini secara efektif menerapkan prinsip *never trust, always verify* pada setiap akses dan transaksi kritis.

b. Kelebihan dan Kekurangan: Kelebihan utama dari model yang diusulkan adalah peningkatan keamanan secara signifikan dengan mempersempit jendela eksploitasi (*window of exploitation*) berkat masa aktif token yang sangat singkat. Pendekatan ini memitigasi risiko pencurian token sesi dan pergerakan lateral penyerang di dalam sistem. Namun, kekurangannya adalah implementasi saat ini masih dalam skala simulasi dan belum diuji pada lingkungan produksi dengan beban lalu lintas yang tinggi. Selain itu, penambahan langkah - langkah verifikasi yang akan berpotensi sedikit memengaruhi kenyamanan pengguna.

c. Pengembangan Selanjutnya: Untuk pengembangan selanjutnya, penelitian dapat difokuskan pada analisis performa dan skalabilitas sistem di bawah beban pengguna yang masif. Selain itu, dapat dieksplorasi integrasi metode autentikasi yang lainnya seperti biometrik mampu untuk meningkatkan kenyamanan tanpa adanya sedikitpun mengorbankan keamanan. Penerapan token JIT juga dapat diperluas untuk mengamankan aksi-aksi yang sensitif lainnya di luar transaksi finansial, seperti perubahan data profil pengguna.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada pihak-pihak terkait yang telah memberi dukungan terhadap penelitian ini.

DAFTAR PUSTAKA

[1] A. T. Rahmah and M. I. Fasa, “Pengaruh Transformasi Digital dan Pengembangan Financial Technology (Fintech) Terhadap Inovasi Layanan Perbankan Syariah,” *J. Manajemen, Akunt. dan Logistik*, vol. II, no. 3, pp. 300–313, 2024.

[2] A. T. Farahdiva, S. L. Mulyana, and T. P. Asri, “IMPLEMENTASI CYBER SECURITY DALAM SISTEM TRANSAKSI KEUANGAN DIGITAL,” *J. Ilm. Ekon. Manaj. Bisnis dan Akunt.*, vol. 2, no. 4, pp. 276–289, 2025.

[3] M. R. A. Fitra, N. T. Jehian, L. Elisabet, and D. Kiswanto, “SIMULASI SERANGAN SIBER

MAC ADDRESS DAN IP ADDRESS SPOOFING PADA JARINGAN HTTP DI KALI LINUX," *J. Teknol. Inf. dan Komput.*, vol. 11, no. 2, pp. 139–149, 2025, doi: 10.36002/jutik.v11i2.3766.

[4] Y. Kusnanto, M. A. Nugroho, and R. Kartadie, "Implementasi Zero Trust Architecture untuk Meningkatkan Keamanan Jaringan: Pendekatan Berbasis Simulasi," *JIPI (Jurnal Ilm. Penelit. dan Pembelajaran Inform.*, vol. 9, no. 4, pp. 2357–2364, 2024, doi: 10.29100/jipi.v9i4.6943.

[5] 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.

[6] U. Lorenza, R. Angelisa Soedira, M. Ayu Ramadiani, and F. Zona Rizal, "Implementasi Metode Just In Time (JIT) dalam Pengelolaan Persediaan Bahan Baku pada Sweet Donuts di Kota Depok," *Sanskara Manaj. Dan Bisnis*, vol. 2, no. 03, pp. 133–145, 2024, doi: 10.58812/smb.v2i03.408.

[7] G. Y. Gustiegan and Painem, "Implementasi Web Service Restful Dengan Autentikasi Json Web Token Dan Algoritma Kriptografi Aes-256 Untuk Aplikasi Peminjaman Laboratorium Berbasis Mobile Pada Universitas Budi Luhur," *Bit (Fakultas Teknol. Inf. Univ. Budi Luhur)*, vol. 19, no. 1, pp. 9–16, 2022.

[8] U. B. Astowo and A. Sujarwo, "Penerapan JSON Web Token sebagai Strategi Pengamanan Data pada Aplikasi MultiMasjid," *Innov. J. Soc. Sci. Res.*, vol. 3, no. 6, pp. 5279–5292, 2023.

[9] R. Rahman, M. F. Ilyaz, and M. Syawal, "IMPLEMENTASI ZERO TRUST ARSITEKTUR PADA JARINGAN HYBRID WORK," *Systec J. Syst. Technol.*, vol. 1, no. 1, pp. 14–19, 2025.

[10] M. Mukhlisin and R. Agung Firmansyah, "Zero Trust Architecture: Solusi Keamanan Dan Privasi Untuk Institusi Pendidikan, Systematic Literature Review," *JATI (Jurnal Mhs. Tek. Inform.*, vol. 9, no. 4, pp. 6926–6935, 2025, doi: 10.36040/jati.v9i4.14344.

[11] J. B. Lase, K. S. Zai, and N. K. Lase, "Penerapan Sistem Just In Time (JIT) dalam Perencanaan dan Pengendalian Manajemen Persediaan Bahan Baku Material di CV Utama," *J. EMBA*, vol. 10, no. 4, pp. 1234–1238, 2022.

[12] L. Okstiana and Purwanti, "Penerapan Metode Just In Time (JIT) dalam Pengelolaan Persediaan UMKM Kripik Singkong Balado di Kabupaten Bekasi," *Junral Ekon. dan Bisnis Digit.*, vol. 12, no. 01, pp. 1676–1686, 2025.

[13] N. Qomariyah and N. I. Mauliyah, "Implementasi Sistem Just in Time (JIT) dalam Meningkatkan Produktivitas Perusahaan pada PT. Langgeng Makmur Utama Bangsalsari Jember," *J. Akunt. dan Audit Syariah*, vol. 4, no. 1, pp. 94–106, 2023, doi: 10.28918/jaais.v4i01.947.

[14] M. N. Annaisaburi, A. Kusyanti, and F. A. Bakhtiar, "IMPLEMENTASI ALGORITMA CLEFIA 128DAN TIME-BASED ONE TIMEPASSWORDSEBAGAI TWO-FACTOR AUTHENTICATIONUNTUKMENINGKATKAN KEAMANANPADA PROSES AUTENTIKASI," *J. Teknol. Inf. dan Ilmu Komput.*, vol. 11, no. 3, pp. 539–548, 2025.

[15] L. Qadriah, S. Achmady, and Husaini, "Sistem Pengamanan Dokumen dengan Algoritma Time-Based One Time Password (TOTP) pada Two-Factor Authentation (2FA)," *J. Sains dan Inform.*, vol. 9, no. November 2022, pp. 29–35, 2023, doi: 10.34128/jsi.v9i1.519.

[16] T. Q. Hanifah, D. Kuswoyo, and E. D. Asgawanti, "RANCANG BANGUN APLIKASI 'K3POIN' BERBASIS PROGRESSIVE WEB APPSDAN METODE ANALYSIS DESIGN DEVELOPMENT IMPLEMENTATION EVALUATION," *JITET (Jurnal Inform. dan Tek. Elektro Ter.*, vol. 13, no. 3, pp. 2270–2282, 2025, doi: 10.23960/jitet.v13i3.7358.