IMPLEMENTASI MULTI-FACTOR AUTHENTICATION (MFA) DENGAN METODE HASHING (SHA-256) UNTUK MENINGKATKAN KEAMANAN PENGGUNA E-COMMERCE

R.Z.Nafiah[1], Ramadhan Renaldy[2] dan R.Ardiansyah[3]

[1,2,3]*Jurusan Informatika, Fakultas Teknik dan Informatika, Universitas PGRI Semarang*

Gedung Pusat Lantai 3, Kampus 1 Jl. Sidodadi Timur 24, Semarang

E-mail : rizqazahrotun@gmail.com[1], ramadhanrenaldy@upgris.ac.id[2], riffkiardiansyah32@gmail.com[3]

Abstrak

Perkembangan teknologi informasi telah menjadikan e-commerce bagian penting dalam kehidupan modern, namun ancaman keamanan data pengguna, seperti peretasan akun, terus meningkat. Multi-Factor Authentication (MFA) menjadi solusi efektif untuk melindungi akun pengguna dengan menambahkan lapisan keamanan. Penelitian ini mengembangkan mekanisme MFA berbasis hashing SHA-256 dan pengiriman One Time Password (OTP) melalui e-mail sebagai alternatif dari metode berbasis SMS yang memiliki berbagai kelemahan. Hasil pengujian menunjukkan bahwa mekanisme ini dapat meningkatkan keamanan data pengguna e-commerce, terutama dalam menjaga confidentiality, integrity, dan availability (CIA) dari ancaman peretasan.

Kata Kunci*: *E-Commerce, Multi-Factor Authentication, Hashing

I. PENDAHULUAN

Perkembangan pesat teknologi informasi dan digitalisasi telah membawa perubahan signifikan dalam berbagai aspek kehidupan, termasuk dalam aktivitas jual beli. E-commerce sebagai salah satu bentuk transaksi online semakin populer dan menjadi bagian integral dari kehidupan masyarakat modern. Namun, seiring dengan pertumbuhan *e-commerce*, ancaman terhadap keamanan data pengguna juga semakin meningkat.

Salah satu masalah utama yang dihadapi oleh platform *e-commerce* adalah tingginya angka peretasan akun pengguna. Kasus kebocoran data yang dialami oleh platform *e-commerce* Tokopedia pada April 2020 menjadi salah satu contoh nyata risiko keamanan dalam sistem digital. Hacker dengan nama samaran "Why So Dank" berhasil mencuri data pribadi hingga 91 juta pengguna dan 7 juta merchant, yang mencakup informasi sensitif seperti email, password, dan nama pengguna. Kebocoran ini tidak hanya memberikan potensi kerugian finansial bagi pengguna, seperti penyalahgunaan akun atau pencurian identitas, tetapi juga berdampak buruk pada reputasi Tokopedia sebagai platform yang seharusnya dapat dipercaya [1].

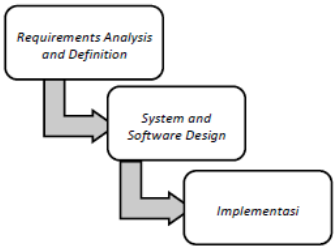
Untuk mengatasi permasalahan tersebut, diperlukan suatu mekanisme keamanan yang lebih kuat untuk melindungi akun pengguna. Salah satu solusi yang dapat diimplementasikan adalah Multi-Factor Authentication (MFA). MFA adalah metode autentikasi elektronik yang mengharuskan pengguna memasukkan dua atau lebih faktor keamanan untuk mengakses aplikasi atau situs web [2]. Dengan demikian, meskipun kata sandi pengguna berhasil dicuri, pihak yang tidak berwenang akan kesulitan untuk mengakses akun tersebut karena memerlukan faktor verifikasi tambahan.

E-ISSN: 2985-3532

Beberapa penelitian terkait telah dilakukan. Penelitian sebelumnya mengembangkan sistem OTP (One Time Password) sebagai proses otentikasi ganda melalui SMS (Short Message Service). Namun, sistem ini memiliki kelemahan karena jika nomor handphone pengguna telah disalahgunakan, proses OTP menjadi tidak efektif [3]. Selain itu, penelitian sebelumnya berhasil membangun mekanisme 2FA menggunakan OTP yang dikirimkan melalui SMS, namun ia juga menjelaskan bahwa SMS memerlukan biaya berupa pulsa untuk mengirimkan kode OTP kepada pengguna [4]. Oleh karena itu, diperlukan solusi OTP yang dapat memanfaatkan layanan gratis seperti WhatsApp, Telegram, atau e-mail.

Berdasarkan penelitian sebelumnya, penelitian ini berfokus pada pembangunan mekanisme MFA yang memanfaatkan layanan e-mail untuk mengurangi risiko keamanan apabila data pengguna disalahgunakan oleh pihak lain. Dengan mekanisme ini, diharapkan confidentiality, integrity, dan availability (CIA) dari data dan informasi yang terdapat pada e-commerce dapat terjaga dan terlindungi dari berbagai ancaman keamanan siber.

II. METODOLOGI PENELITIAN



Gambar 1. Tahapan Metode *Waterfall*

Metodologi penelitian yang diterapkan dalam penelitian ini adalah dengan pengembangan metode *Waterfall*. Metode *Waterfall* merupakan model pengembangan sistem informasi yang sistematik dan sekuensial. Metode *Waterfall* terdiri dari beberapa tahapan, seperti yang ditampilkan pada Gambar 1. Tahapan pertama adalah Analisa Kebutuhan Sistem, di mana dilakukan identifikasi kebutuhan sistem autentikasi untuk meningkatkan keamanan platform e-commerce. Sistem yang dirancang mencakup penggunaan hashing SHA-256 untuk perlindungan kata sandi dan penerapan OTP berbasis email sebagai faktor autentikasi tambahan. Hasil analisis ini menjadi dasar untuk langkah-langkah selanjutnya dalam merumuskan sistem yang akan dikembangkan.

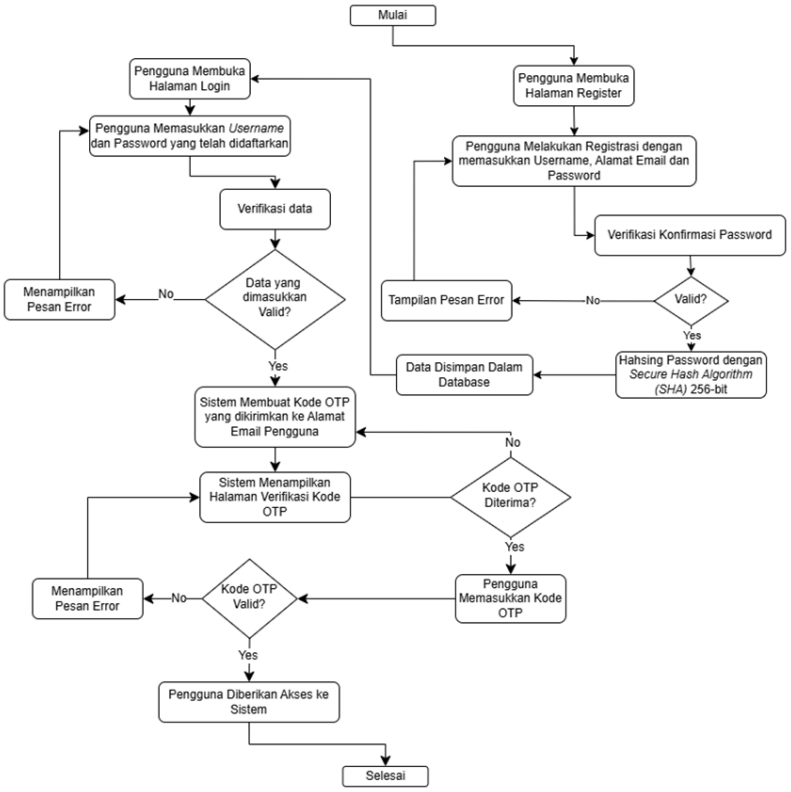
Tahapan berikutnya adalah Desain Sistem dan Perangkat Lunak, yang melibatkan perancangan sistem MFA. Perancangan dilakukan menggunakan beberapa diagram, seperti Use Case Diagram untuk menggambarkan interaksi antara pengguna dan sistem, Activity Diagram untuk memvisualisasikan alur autentikasi, serta flowchart untuk memetakan alur logika dan proses dalam sistem secara terperinci.

Tahap terakhir adalah Implementasi, di mana sistem MFA dikembangkan menggunakan Visual Studio Code sebagai lingkungan pengembangan utama. Proses hashing dilakukan dengan implementasi algoritma SHA-256, sementara pengiriman OTP berbasis email memanfaatkan integrasi layanan email. Sistem ini dirancang untuk memastikan keamanan pengguna tetap terjaga tanpa mengorbankan kinerja platform.

III. HASIL DAN PEMBAHASAN

1. Perancangan Sistem

E-ISSN: 2985-3532



Gambar 2. *Flowchart* Sistem

Seperti yang terlihat pada Gambar 2, flowchart ini menggambarkan alur proses dalam sistem e-commerce yang menerapkan Multi-Factor Authentication (MFA) menggunakan metode hashing SHA-256 untuk meningkatkan keamanan pengguna. Proses dimulai ketika pengguna membuka halaman login, di mana mereka diminta memasukkan username dan password yang telah terdaftar. Sistem akan memverifikasi data yang dimasukkan, dan jika data tidak valid, sistem akan menampilkan pesan error. Jika data valid, sistem akan membuat kode OTP yang dikirimkan ke alamat email pengguna. Setelah menerima kode OTP, pengguna memasukkannya pada halaman verifikasi. Sistem kemudian memvalidasi kode OTP tersebut; jika valid, pengguna diberikan akses ke sistem, namun jika tidak valid, sistem akan menampilkan pesan error dan meminta pengguna untuk mencoba kembali.

Jika pengguna belum memiliki akun, mereka diarahkan ke halaman registrasi untuk memasukkan username, alamat email, password, dan konfirmasi password. Sistem akan memverifikasi kesesuaian password dan konfirmasi password. Jika tidak sesuai, sistem akan menampilkan pesan error, tetapi jika sesuai, data pengguna akan disimpan dalam database setelah melalui proses hashing menggunakan algoritma SHA-256. Proses hashing ini bertujuan untuk memastikan bahwa password asli tidak disimpan di database, melainkan hasil hashing berupa string tetap yang tidak dapat diubah kembali menjadi password asli.

Pada proses registrasi, sistem juga mengirimkan kode OTP ke email pengguna untuk memverifikasi alamat email. Pengguna harus memasukkan kode OTP pada halaman verifikasi, dan sistem akan memvalidasi kode tersebut. Jika kode OTP valid, proses registrasi berhasil, dan akun pengguna diaktifkan. Namun, jika kode OTP tidak valid, sistem akan meminta pengguna untuk mencoba kembali. Setelah login atau registrasi berhasil, pengguna diberikan akses ke sistem sesuai hak akses yang dimilikinya. Dengan menggunakan kombinasi hashing password dan OTP, sistem ini dirancang untuk memberikan keamanan maksimal, memastikan perlindungan data pengguna, dan memberikan lapisan autentikasi tambahan untuk memvalidasi akses ke sistem.

E-ISSN: 2985-3532

2. Implementasi

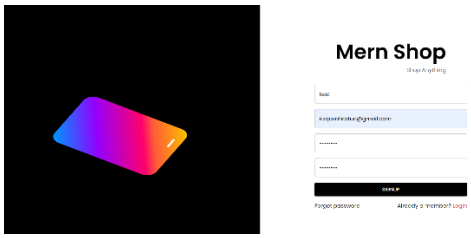
Pada tahap ini, implementasi dilakukan dengan membuat aplikasi e-commerce berbasis web yang dilengkapi dengan fitur Multi-Factor Authentication (MFA). Proses pengembangan dimulai dengan mengintegrasikan hashing SHA-256 untuk mengamankan kata sandi pengguna selama proses pendaftaran dan login. Hashing adalah proses yang mengubah kata sandi pengguna menjadi string tetap melalui algoritma matematika yang bersifat satu arah, sehingga kata sandi asli tidak disimpan dalam basis data. Untuk meningkatkan keamanan, sebelum proses hashing, sistem menambahkan *salt*—yaitu nilai acak—ke kata sandi.

Gambar 3. Implementasi Hashing SHA 256

Kombinasi kata sandi dan salt ini kemudian diproses menggunakan algoritma SHA-256, menghasilkan string unik sepanjang 256-bit atau 64 karakter heksadesimal. Sebagai contoh, jika pengguna memasukkan kata sandi "password123" dengan *salt* "f8h4G7", hasil hashing akan berupa string seperti "e72d8b5cf9b29700754713fcab96e91ff3bda0df2e6d8b73e8e6c90e3c5cd724", yang kemudian disimpan dalam basis data. Saat login, kata sandi yang dimasukkan pengguna akan digabungkan dengan salt yang sama, di-hash kembali, dan dibandingkan dengan nilai hash yang tersimpan.

Setelah proses verifikasi hash berhasil, langkah autentikasi dilengkapi dengan pengiriman One-Time Password (OTP) berbasis email sebagai faktor keamanan tambahan. OTP ini merupakan kode unik yang hanya berlaku sekali dan memiliki batas waktu tertentu untuk digunakan. Proses ini memastikan bahwa hanya pengguna yang memiliki akses ke email terdaftar yang dapat menyelesaikan autentikasi.

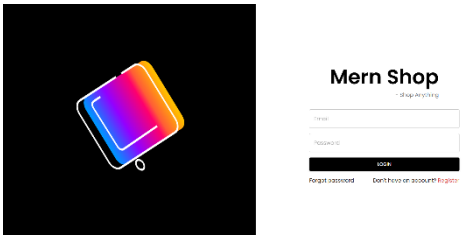
Dengan implementasi ini, aplikasi e-commerce tidak hanya melindungi data pengguna melalui hashing SHA-256, tetapi juga memperkuat keamanan dengan lapisan MFA berbasis OTP, sehingga meminimalkan risiko serangan seperti pencurian kata sandi dan meningkatkan kepercayaan pengguna dalam melakukan transaksi online. Berikut merupakan implementasi antarmuka yang dibuat pada sistem.



Gambar 4. Halaman *Register*

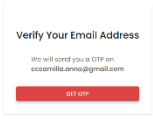
Pada halaman *Register* terdapat form pengisian nama, alamat email, password dan konfirmasi password. Setelah pengguna mengisi semua form untuk mendaftar dengan valid dan pengguna meng-klik tombol register maka sistem akan menyimpan data dan melakukan hashing password menggunakan algoritma SHA-256 ke dalam database.

E-ISSN: 2985-3532



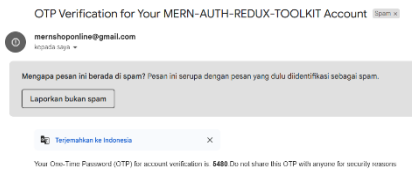
Gambar 5. Halaman Login

Setelah melakukan registrasi, pengguna diarahkan ke halaman login, pengguna dapat memasukkan alamat email dan password, dan melakukan login.



Gambar 6. Halaman Verifikasi Email

Setelah melakukan registrasi, sistem akan mengarahkan pengguna untuk melakukan verivikasi alamat email mereka seperti pada Gambar 5. Proses verifikasi dimulai dengan pengiriman One-Time Password (OTP) ke alamat email yang telah didaftarkan oleh pengguna. Pengguna kemudian mengklik tombol "GET OTP" untuk menerima kode OTP unik yang akan digunakan dalam langkah berikutnya.



Gambar 7. Email terkirimnya *One-Time Password* (OTP)

Seperti yang terlihat pada Gambar 6, *One-Time Password* (OTP) berhasil terkirim ke alamat email pengguna yang terdaftar. Pesan email ini berisi kode OTP unik, yang diperlukan untuk menyelesaikan proses verifikasi akun. Pengguna diingatkan untuk tidak membagikan kode OTP ini kepada siapa pun demi alasan keamanan.

Gambar 8. Halaman Autentikasi dengan OTP

Setelah One-Time Password (OTP) berhasil terkirim ke alamat email pengguna, pengguna dapat memasukkan kode OTP tersebut ke dalam form halaman verifikasi OTP. Jika valid, maka sistem akan memberikan akses masuk sistem ke tahap selanjutnya.

E-ISSN: 2985-3532

Gambar 9. Halaman Utama

Setelah pengguna memasukkan kode OTP yang diterima melalui email ke dalam sistem dan kode tersebut divalidasi sebagai benar, sistem akan memberikan akses ke halaman utama e-commerce. Pada tahap ini, pengguna telah berhasil melewati proses Multi-Factor Authentication (MFA), yang mencakup validasi kredensial menggunakan password yang di-hash dengan algoritma SHA-256 serta verifikasi kode OTP.

Dengan akses yang diberikan, pengguna dapat mulai menjelajahi fitur utama dari e-commerce, seperti mencari produk, melihat detail produk, menambahkannya ke keranjang, serta menyelesaikan transaksi melalui pembayaran. Proses ini memastikan bahwa hanya pengguna yang terverifikasi dengan baik yang dapat masuk ke dalam sistem, meningkatkan keamanan dan kepercayaan dalam penggunaan platform.

3. Pengujian Sistem

Setelah sistem selesai dikembangkan, langkah berikutnya adalah melakukan pengujian sistem untuk memastikan bahwa semua fungsi dan fitur berjalan sesuai dengan yang diharapkan dan untuk menemukan kesalahan sistem yang mungkin terjadi saat digunakan oleh pengguna. Pengujian ini dilakukan dengan metode blackbox, di mana fokusnya adalah pada pemeriksaan keluaran dari fungsi-fungsi tanpa melihat kode internal.

Blackbox testing mengevaluasi apakah input yang diberikan menghasilkan output yang sesuai dengan spesifikasi sistem. Dalam pengujian ini, setiap fitur penting dari sistem e-commerce, termasuk proses login dengan hashing password dan verifikasi One-Time Password (OTP) , diuji secara menyeluruh. Hal ini mencakup pemeriksaan alur login, pendaftaran, pengiriman OTP, validasi OTP, serta berbagai fungsi transaksi seperti pencarian produk, penambahan produk ke keranjang, dan pembayaran. Hasil pengujian menggunakan metode black box testing pada sistem ini dapat dilihat pada Tabel 1.

Tabel 1. Pengujian *Multi Factor Authentication* Pada *E-Commerce* dengan Metode *Blackbox Testing.*

No	Pengujian	*Test Case*	Hasil Didapat	Hasil Pengujian	Keterangan
1	Menu *register*	Melakukan registrasi	Sistem berhasil menyimpan data registrasi *user*	Sesuai Harapan	Valid
2	Menu *login*	Melakukan *login*	Sistem berhasil menerima *request login* dan membuat kode OTP yang dikirimkan pada alamat email *user* yang telah didaftarkan saat registrasi	Sesuai Harapan	Valid

E-ISSN: 2985-3532

3	Menu verifikasi OTP	Melakukan verifikasi kode OTP	Sistem berhasil mengirimkan kode OTP pada alamat email pengguna dan menerima *request* verifikasi kode OTP jika kode yang dimasukkan valid	Sesuai Harapan	Valid

IV. KESIMPULAN

Berdasarkan penelitian yang dilakukan, dapat disimpulkan bahwa implementasi *Multi-Factor Authentication* (MFA) dengan *hashing* SHA-256 untuk kata sandi terbukti mampu meningkatkan keamanan pada platform e-commerce secara signifikan. Selain itu, penggunaan OTP berbasis email sebagai faktor autentikasi tambahan memberikan solusi yang lebih hemat biaya dibandingkan metode berbasis SMS, meskipun memiliki kelemahan terkait aksesibilitas jaringan. Sistem yang dikembangkan juga menunjukkan kemampuan yang efektif dalam melindungi data pengguna dari berbagai ancaman keamanan siber, seperti pencurian kata sandi dan data transaksi, tanpa mengorbankan kinerja platform.

V. UCAPAN TERIMA KASIH

Penulis mengucapkan puji syukur ke hadirat Tuhan Yang Maha Esa atas limpahan rahmat, hidayah, dan karunia-Nya sehingga artikel ini dapat diselesaikan dengan baik. Penulis juga menyampaikan terima kasih yang sebesar-besarnya kepada dosen pembimbing yang telah memberikan bimbingan, arahan, serta masukan berharga selama proses penulisan artikel ini. Ucapan terima kasih juga penulis sampaikan kepada seluruh rekan dan teman-teman yang telah memberikan dukungan, semangat, serta kontribusi, baik secara langsung maupun tidak langsung, dalam penyelesaian artikel ini.

VI. REFERENSI

[1] Raihan, M. (2023). Perlindungan Data Diri Konsumen dan Tanggungjawab Marketplace terhadap Data Diri Konsumen (Studi Kasus: Kebocoran Data 91 Juta Akun Tokopedia). *Jurnal Inovasi Penelitian*. 3(10): 7847-7856.

[2] ALSaleem, B. O., & Alshoshan, A. I. (2021). Multi-Factor Authentication to System Login. *2021 National Computing Colleges Conference (NCCC)*.

[3] Fitriyansyah, A. Y., & Hazri, M. (2020). Analisis Security Web Login Mahasiswa menggunakan Algoritma Two-Factor Time-Based One Time Password. *Jurnal Penelitian dan Pengkajian Sains Teknologi*. 3(10): 7847-7856.

[4] Mahardhika, G. C., & David, F. (2020). Implementasi Two Factor Authentication (2FA) pada Sistem Keamanan Otentikasi User di Aplikasi Kasir Legends Barbershop. *Jurnal Sistem dan Teknologi Informasi*. 8(4): 357-361.

E-ISSN: 2985-3532