PENERAPAN MULTI-FACTOR AUTHENTICATION MENGGUNAKAN FUNGSI HASH BCRYPT PADA PEMESANAN KOPI

I.Navila[1], Ramadhan Renaldy[2] dan W.Aprilia[3]

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

Gedung Pusat Lantai 6, Kampus 1 Jl. Sidodadi Timur 24, Semarang

E-mail : ilmanavila28@gmail.com[1], *ramadhanrenaldy@upgris.ac.id*[2], widyaaprila04@gmail.com[3]

Abstrak

Industri pemesanan kopi daring menghadapi tantangan signifikan terkait meningkatnya risiko kebocoran data pelanggan akibat serangan siber yang semakin canggih. Popularitas layanan pemesanan kopi melalui aplikasi memunculkan tantangan baru dalam melindungi data sensitif, seperti informasi pembayaran dan alamat pengiriman. Di Indonesia, lebih dari 700 juta serangan siber tercatat pada tahun 2022, membahayakan privasi pelanggan dan kepercayaan mereka terhadap bisnis daring. Penelitian ini bertujuan untuk mengembangkan sistem keamanan yang efektif melalui penerapan Multi-Factor Authentication (MFA) dan algoritma Bcrypt. Teknologi ini dirancang untuk meningkatkan keamanan akses pengguna sekaligus melindungi data sensitif dari potensi penyalahgunaan. Dengan penerapan ini, diharapkan integritas dan kerahasiaan informasi pelanggan dalam aplikasi pemesanan kopi dapat terjaga secara optimal.

Kata Kunci*: *Aplikasi Pemesanan Kopi, Bcrypt, Multi Factor Authentication (MFA)

I. PENDAHULUAN

Berkembangnya teknologi membuat dunia bisnis turut berkembang, termasuk dalam industri kopi. Saat ini, banyak kedai kopi yang menawarkan layanan pemesanan melalui aplikasi daring, memungkinkan pelanggan untuk menikmati kopi favorit mereka tanpa harus mengantri. Aplikasi ini tidak hanya mempermudah pelanggan, tetapi juga meningkatkan efisiensi operasional bagi para pelaku usaha. Namun, dengan kemudahan yang ditawarkan, muncul tantangan baru terkait keamanan data pelanggan, terutama dalam hal transaksi online. Data seperti detail pemesanan, alamat pengiriman, dan informasi pembayaran adalah informasi sensitif yang jika tidak diamankan dengan baik, dapat disalahgunakan untuk kejahatan atau menyebabkan kerugian bagi pelanggan. Kondisi ini diperburuk dengan meningkatnya kasus kebocoran data di Indonesia, yang menyebabkan keresahan di masyarakat mengenai privasi dan keamanan data pribadi mereka.

Keamanan siber adalah tindakan untuk melindungi komputer, jaringan, aplikasi perangkat lunak, sistem kritis, dan data dari potensi ancaman digital. Roxana Radu memaparkan bahwa cyber security merupakan seperangkat kebijakan, alat, instrumen, manajemen risiko dalam mencegah ancaman yang datang dari dunia maya (Radu dalam Kremer & Muller, 2014)(Ramadhan 2020). Cyber security atau keamanan siber berfungsi atau berperan untuk mengatasi, mendeteksi, menemukan, menangkal ataupun meminimalisasi tingkat resiko terjadinya gangguan, ancaman (cyber threat) dan serangan siber (cyber attack) serta seluruh aktifitas teknologi siber yang mengancam keamanan seluruh komponen sistem siber itu sendiri yang meliputi hardware, software, data/informasi maupun infrastruktur(Siagian, Budiarto, and Simatupang 2018). Selain itu, keamanan siber berperan penting dalam menjaga kerahasiaan, integritas, dan ketersediaan data, serta melindungi privasi individu dan organisasi di tengah semakin berkembangnya ancaman siber.

E-ISSN: 2985-3532

Autentikasi adalah proses elektronika yang memungkinkan identifikasiseseorang secara digital. Proses ini memastikan bahwa individu yang mencoba mengakses suatu sistem atau layanan adalah benar-benar pihak yang berwenang, dengan memverifikasi kredensial seperti kata sandi, sidik jari, atau metode otentikasi lainnya. Autentikasi mempunyai berbagai metode, salah satunya adalah Multi-Factor Authentication. Multi-Factor Authentication adalah autentikasi yang lebih aman dibandingkan dengan autentikasi satu faktor yaitu dengan nama pengguna atau email pengguna dan kata sandi. Multi-factor authentication menyediakan lapisan keamanan ekstra dalam proses autentikasi. Lapisan tambahan ini mengurangi kemungkinan peretas berhasil mengakses sistem komputer. Selain mendapatkan keuntungan, mekanisme ini juga memiliki kelemahan sebagai berikut (Pramartha, 2013);

One-Time Password (OTP), yang juga dikenal sebagai sandi sekali pakai, biasanya digunakan untuk transaksi online atau proses pendaftaran akun baru. Kode OTP terdiri dari kombinasi angka unik yang dihasilkan secara acak dan bersifat rahasia, dirancang untuk meningkatkan keamanan. OTP dianggap lebih aman karena kata sandi ini terus berubah setiap kali digunakan, sehingga mengurangi risiko penyalahgunaan oleh pihak yang tidak berwenang. Metode One Time Password adalah kata sandi yang valid (absah) dan dapat digunakan hanya untuk satu kali sesi login atau transaksi saja pada komputer atau alat digital lainnya(Sarah Hapsari, Fatman, and Penulis Korespondensi 2020). Salah satukelemahan utama dari penggunaan OTP yaitu rentan terhadap serangan Phising dan Man-in-the-middle-Attack(Sudiarto Raharjo, E.K. Ratri, and Susilo 2017).

Kriptografi berasal dari bahasa Yunani yaitu crypto dan graphia. Crypto berarti rahasia dan graphia berarti tulisan. Secara terminologi kriptografi berarti ilmu dan seni untuk menjaga keamanan pesan(Widyasari 2016). Dengan cara mengubah informasi atau pesan asli (plaintext) menjadi bentuk yang tidak dapat dibaca (ciphertext), melalui proses enkripsi dan dipulihkan dengan proses dekripsi. Proses ini bertujuan untuk melindungi kerahasiaan informasi dari pihak- pihak yang tidak berwenang, sehingga hanya penerima yang sah dengan kunci dekripsi yang benar yang dapat mengembalikan informasi tersebut ke bentuk aslinya. Selain menjaga kerahasiaan, kriptografi juga berperan dalam memastikan integritas data, otentikasi pengirim, dan non-repudiation, yang menjadikannya elemen kunci dalam keamanan siber.

Bcrypt merupakan sebuah fungsi hash yang dibuat oleh Niels Provos dan David Mazières dengan berdasarkan Blowfish cipher. Penamaan Bcrypt terdiri dari B untuk Blowfish dan Crypt yang merupakan nama fungsi hash yang digunakan pada sistem kata sandi di UNIX(Permatasari and Mardiana 2023). Algoritma blowfish menggunakan kunci yang sama untuk proses enkripsi dan dekripsi data dengan membagi pesan ke dalam blok-blok dengan ukuran yang sama panjang. Blowfish termasuk dalam enkripsi block cipher 64 bit dengan panjang kunci antara 32 bit sampai 448 bit(Akbar and Antoni 2022). Bcrypt memiliki algoritma yang mirip dengan fungsi dari Blowfish block cipher. Bcrypt menggunakan metode EKSBlowfish untuk memperkuat enkripsi, khususnya untuk menghindari serangan brute force. Dalam algoritma Bcrypt, jumlah proses hash acak yang dijalankan disebut dengan cost. Cost memiliki jumlah minimal sebanyak 10 kali. Perulangan yang dilakukan juga dapat bervariasi hingga lebih dari 31 kali. Dengan kemampuannya untuk menyesuaikan jumlah iterasi, Bcrypt dapat menghasilkan hash yang lebih kuat dan lebih sulit ditembus terhadap serangan brute-force, meskipun dengan kebutuhan sumber daya komputasi yang lebih besar.

Tujuan penelitian ini untuk mengembangkan dan menerapkan sistem MFA dalam aplikasi pemesanan kopi untuk meningkatkan keamanan akses pengguna. Selain itu juga mengimplementasikan Algoritma Bcrypt untuk melindungi data sensitif pengguna, sehingga menjaga kerahasiaan dan integritas informasi pelanggan.

II. METODOLOGI PENELITIAN

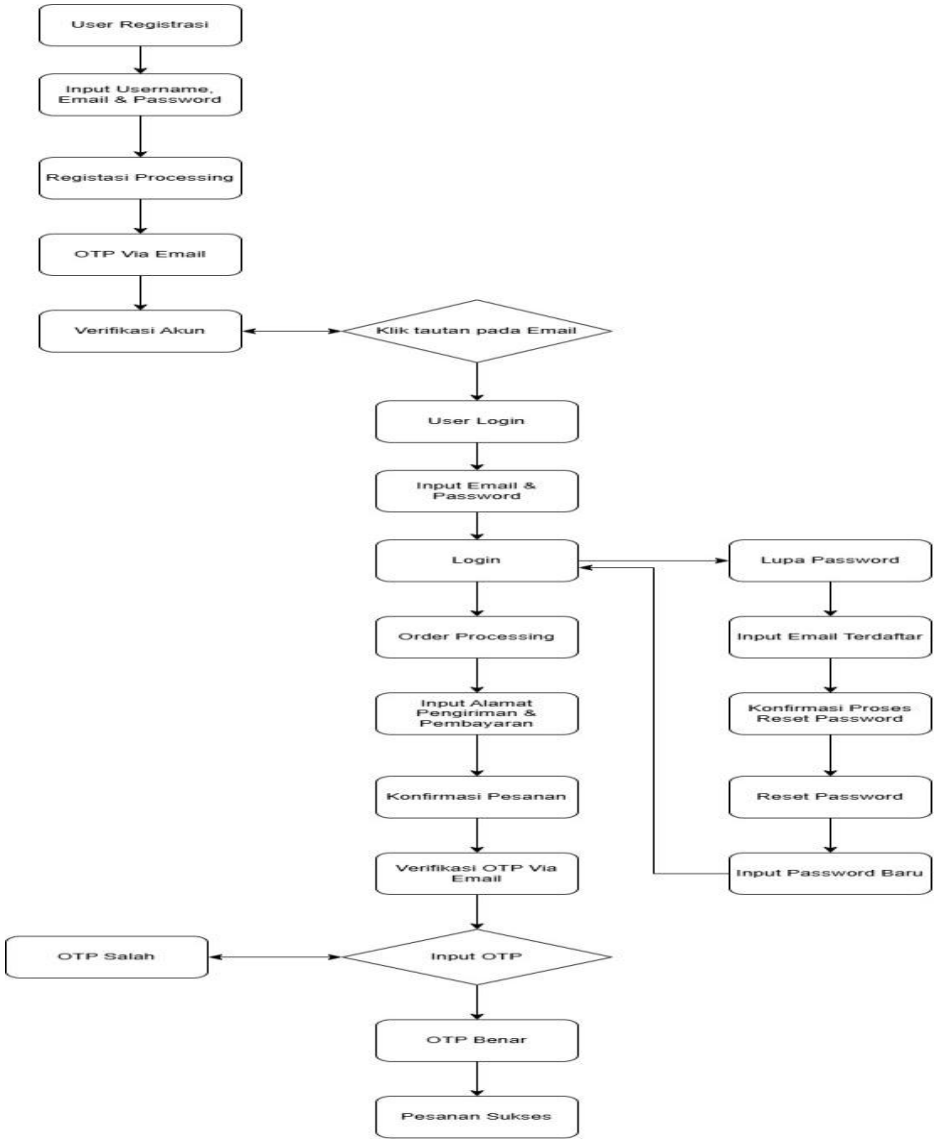
41. Metodologi Penelitian

E-ISSN: 2985-3532

Metode yang dipilih melibatkan dua aspek utama, yaitu penerapan Multi-Factor Authentication (MFA) dan penggunaan algoritma Bcrypt untuk menjaga kerahasiaan serta integritas data pelanggan. Berikut langkah-langkah yang dilakukan dalam pengembangan sistem ini :

42. Alur Pengembangan Sistem

Alur atau flowchart dari sistem yang dikembangkan dapat dilihat pada Gambar 1 di bawah ini. Flowchart ini menunjukkan bagaimana sistem berjalan mulai dari pengguna melakukan Pendaftaran Akun, Order Processing, Proses Verifikasi OTP lewat Email hingga Transaksi Pesanan Selesai.



Gambar 1. Flowchart Sistem Keamanan Aplikasi Pemesanan Kopi

E-ISSN: 2985-3532

Cara kerja dari sistem yang dikembangkan tersebut meliputi :

1. User Registration

   Pengguna mengisi form registrasi yang berisi data pribadi seperti nama, email, dan kata sandi. Sistem akan memvalidasi, jika berhasil maka akan dikirimkan email verifikasi akun ke email yang didaftarkan.

2. Verifikasi Akun

   Setelah registrasi berhasil, user akan menerima email konfirmasi yang berisi link untuk memverifikasi akun atau untuk mengaktifkan akun.

3. Proses Lupa Kata Sandi

   Jika pengguna lupa kata sandi, maka dapat memilih opsi “Lupa Password” pada halaman login. Pengguna memasukan email yang terdaftar, jika email ditemukan maka sistem akan mengirimkan link reset password ke email user.

4. Reset Kata Sandi

   User mengklik link reset password, maka sistem akan mengarahkan ke halaman dimana mereka bisa memasukan kata sandi baru.

   Sistem akan memperbarui kata sandi pengguna.

5. Proses Konfirmasi Pesanan

   - Input Detail Pesanan

     Pengguna mengisi data terkait pesanan, seperti Nama Lengkap, Alamat Lengkap, No. Telepon, Alamat Email, Jasa Pengiriman dan Pilihan Bank

   - Konfirmasi Pesanan

     Jika semua data sudah benar, dan melakukan order, selanjutnya pengguna akan dikirimkan kode OTP via email untuk mengkonfirmasi pesanan yang telah dilakukan. Namun, jika kode OTP yang di masukkan salah, maka pengguna belum bisa melanjutkan proses pemesanan dan sistem akan meminta pengguna untuk mengulang langkah OTP.

6. Pesanan Sukses

   Setelah proses pemesanan berhasil dan Kode OTP yang dimasukkan benar, maka sistem mengubah status pesanan menjadi Pesanan Terkonfirmasi. Kemudian Pengguna akan menerima notifikasi pada sistem bahwa pesanan telah berhasil diproses.

Langkah-langkah Metode Bcrypt dalam Sistem Pemesanan Kopi

E-ISSN: 2985-3532

Metode Bcrypt adalah algoritma hashing yang dirancang untuk melindungi kata sandi dengan cara yang aman. Dalam konteks sistem pemesanan kopi, penerapan Bcrypt dapat dilakukan melalui beberapa langkah penting yang memastikan keamanan data pengguna, terutama kata sandi.

1. **Pembuatan Salt**

   Setiap kata sandi yang akan di-hash dimulai dengan pembuatan nilai acak yang disebut "salt". Salt ini ditambahkan ke kata sandi sebelum proses hashing. Tujuannya agar mencegah penggunaan tabel lookup (rainbow tables) dalam serangan brute force, sehingga meningkatkan keamanan kata sandi

2. **Ekspansi Kunci (Key Expansion)**

   Bcrypt menggunakan algoritma yang dikenal sebagai Eks-P (Eksblowfish) untuk mengembangkan kunci dari kombinasi kata sandi dan salt. Proses ini membuat kunci lebih kompleks dan sulit untuk dipecahkan. Hal tersebut bertujuan untuk meningkatkan kekuatan hashing dengan memperpanjang kunci dari input awal

3. **Proses Hashing (Rounds)**

   Hashing dilakukan melalui sejumlah iterasi yang disebut "rounds". Setiap iterasi menambah waktu yang dibutuhkan untuk menghasilkan hash, sehingga membuatnya lebih sulit bagi penyerang untuk membalikkan hash menjadi kata sandi asli.

   Pengaturan

   Nilai default biasanya adalah 10 rounds, namun dapat disesuaikan untuk meningkatkan keamanan sesuai kebutuhan sistem

4. **Output Hash**

   Hasil akhir dari proses hashing adalah string hash yang mencakup informasi tentang salt dan jumlah rounds yang digunakan. Format output biasanya diawali dengan prefix seperti "$2a$" untuk menunjukkan bahwa itu adalah hash Bcrypt. Tujuannya untuk memastikan bahwa meskipun dua pengguna menggunakan kata sandi yang sama, hasil hash mereka tetap berbeda karena penggunaan salt yang unik

5. **Pembuatan Salt**

   Setiap kata sandi yang akan di-hash dimulai dengan pembuatan nilai acak yang disebut "salt". Salt ini ditambahkan ke kata sandi sebelum proses hashing. Tujuannya agar mencegah penggunaan tabel lookup (rainbow tables) dalam serangan brute force, sehingga meningkatkan keamanan kata sandi

6. **Ekspansi Kunci (Key Expansion)**

   Bcrypt menggunakan algoritma yang dikenal sebagai Eks-P (Eksblowfish) untuk mengembangkan kunci dari kombinasi kata sandi dan salt. Proses ini membuat kunci lebih kompleks dan sulit untuk

E-ISSN: 2985-3532

dipecahkan. Hal tersebut bertujuan untuk meningkatkan kekuatan hashing dengan memperpanjang kunci dari input awal

7. **Proses Hashing (Rounds)**

   Hashing dilakukan melalui sejumlah iterasi yang disebut "rounds". Setiap iterasi menambah waktu yang dibutuhkan untuk menghasilkan hash, sehingga membuatnya lebih sulit bagi penyerang untuk membalikkan hash menjadi kata sandi asli.

   Pengaturan

   Nilai default biasanya adalah 10 rounds, namun dapat disesuaikan untuk meningkatkan keamanan sesuai kebutuhan sistem

8. **Output Hash**

   Hasil akhir dari proses hashing adalah string hash yang mencakup informasi tentang salt dan jumlah rounds yang digunakan. Format output biasanya diawali dengan prefix seperti "$2a$" untuk menunjukkan bahwa itu adalah hash Bcrypt. Tujuannya untuk memastikan bahwa meskipun dua pengguna menggunakan kata sandi yang sama, hasil hash mereka tetap berbeda karena penggunaan salt yang unik

9. **Penyimpanan Hash**

   Hash yang dihasilkan harus disimpan dalam basis data, bukan kata sandi asli. Ini penting untuk menjaga keamanan data pengguna.

   Praktik Baik

   Pastikan bahwa hash disimpan dengan aman dan hanya dapat diakses oleh sistem yang memerlukan otentikasi pengguna.

10. **Verifikasi Kata Sandi**

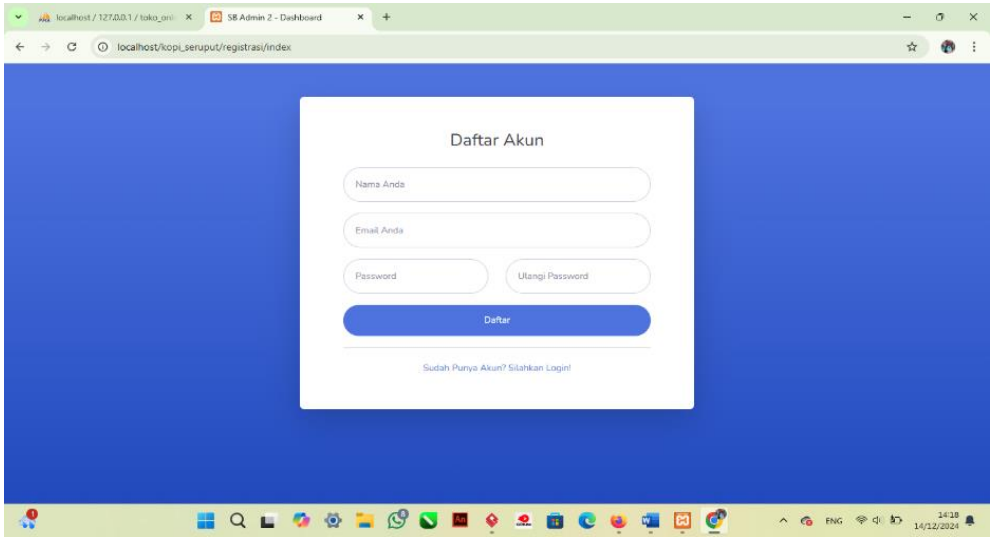
    Saat pengguna mencoba masuk, sistem akan mengambil hash yang tersimpan dan melakukan proses hashing pada kata sandi yang dimasukkan oleh pengguna dengan menggunakan salt dan rounds yang sama. Hasilnya, jika hasil hash baru cocok dengan hash yang tersimpan, akses diberikan; jika tidak, akses ditolak

11. **Verifikasi Kata Sandi**

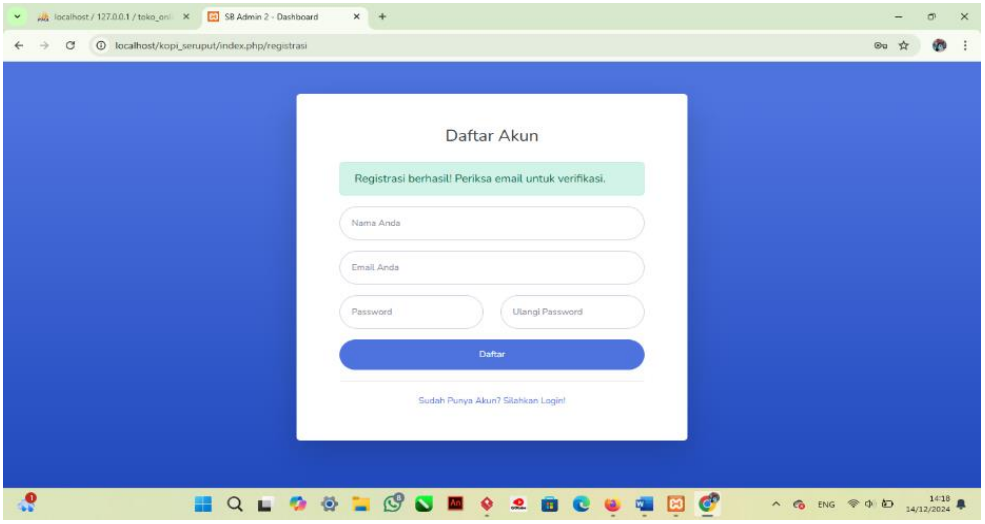
    Saat pengguna mencoba masuk, sistem akan mengambil hash yang tersimpan dan melakukan proses hashing pada kata sandi yang dimasukkan oleh pengguna dengan menggunakan salt dan rounds yang sama. Hasilnya, jika hasil hash baru cocok dengan hash yang tersimpan, akses diberikan, jika tidak, akses ditolak.

E-ISSN: 2985-3532

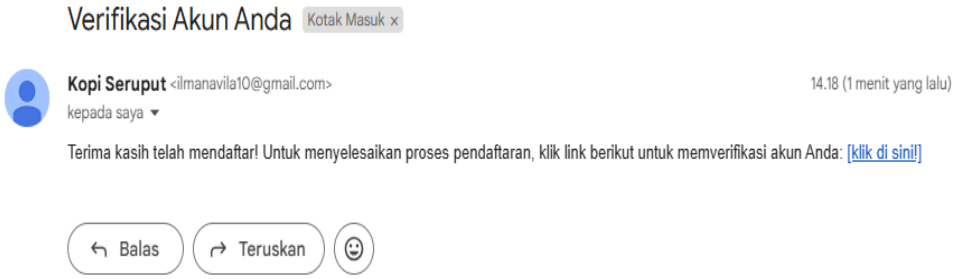
III. HASIL DAN PEMBAHASAN



Gambar 2. Tampilan Registrasi

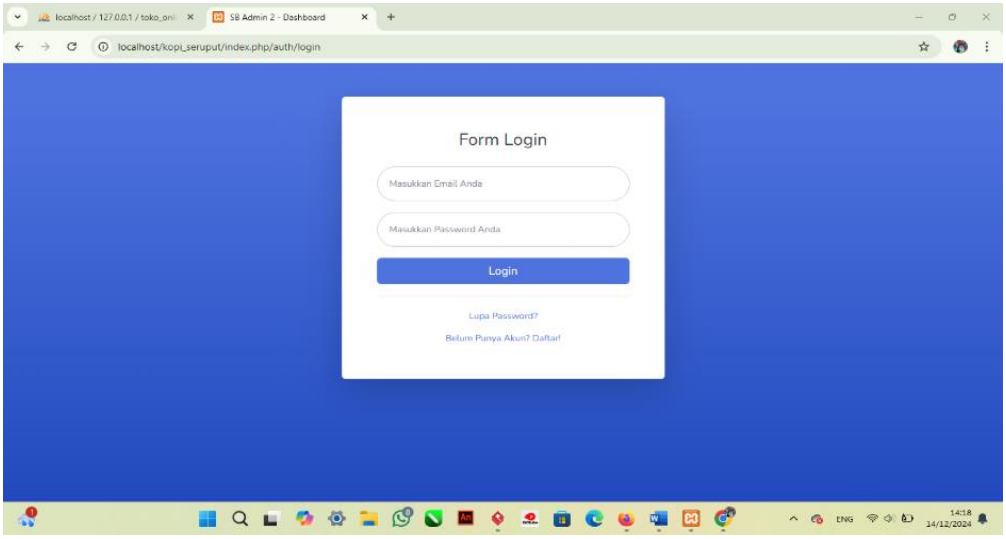


Gambar 3. Tampilan Setelah Mendaftar Akun

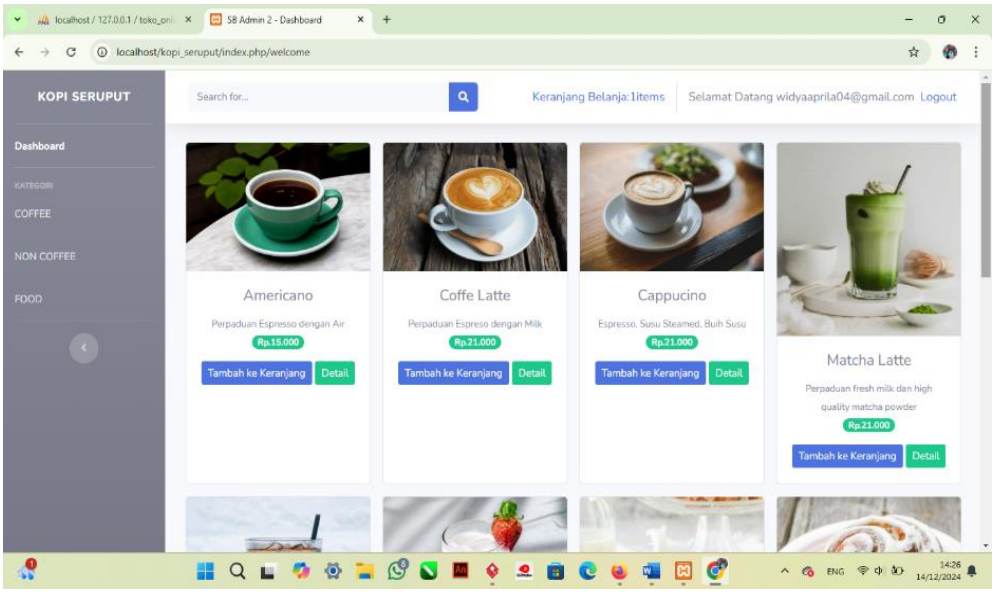


Gambar 4. Tampilan Email Verifikasi Akun

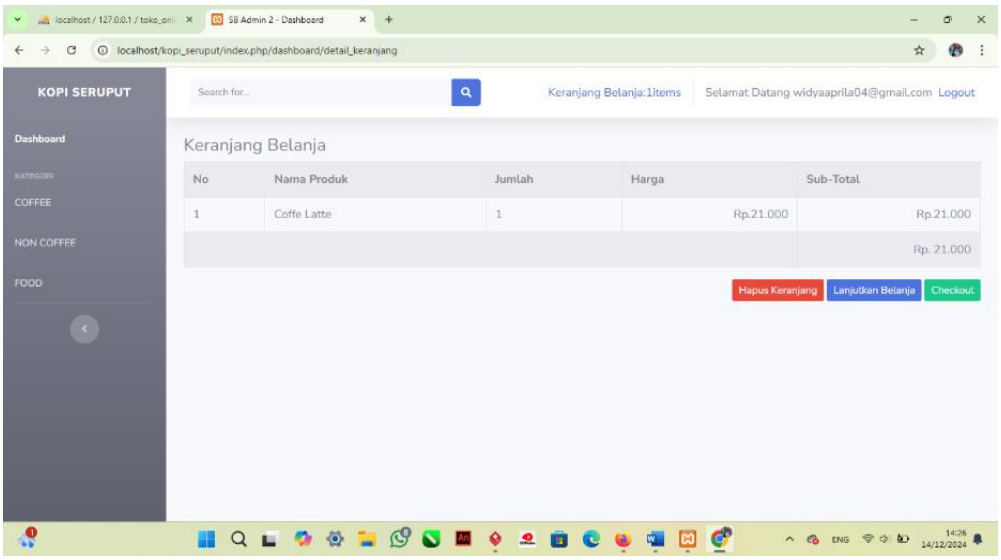
E-ISSN: 2985-3532



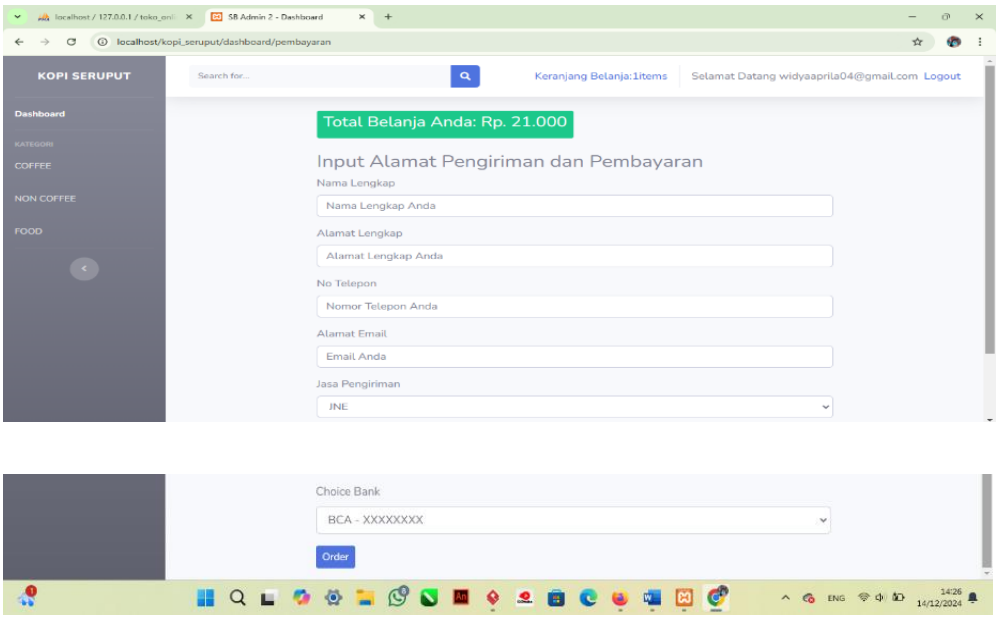
Gambar 5. Tampilan Login



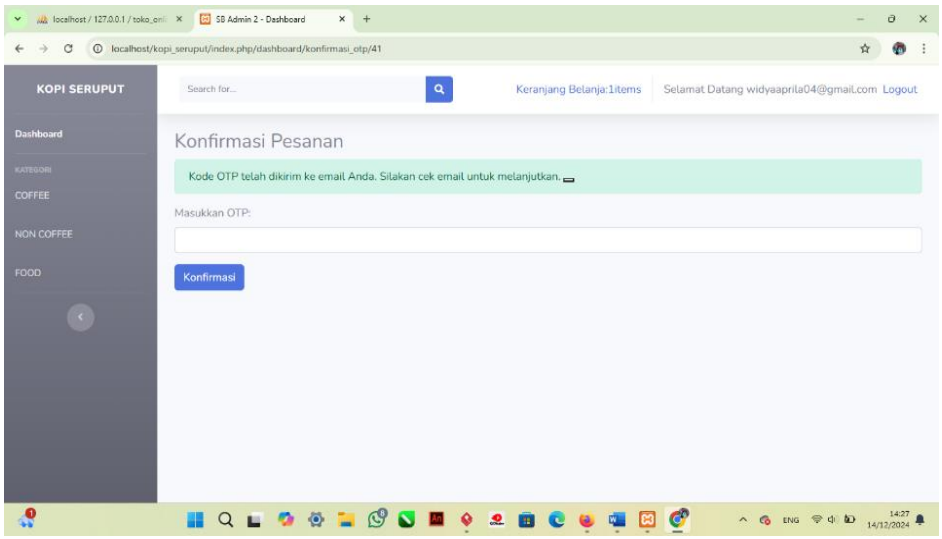
Gambar 6. Tampilan Dashboard



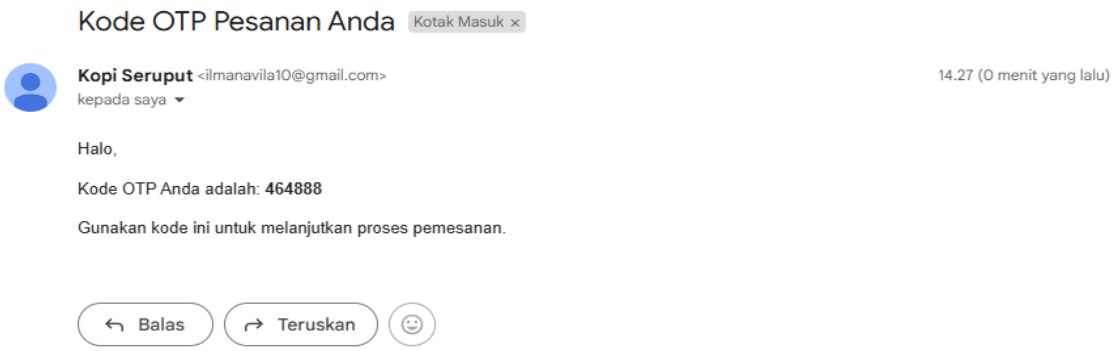
Gambar 7. Tampilan Keranjang Belanja



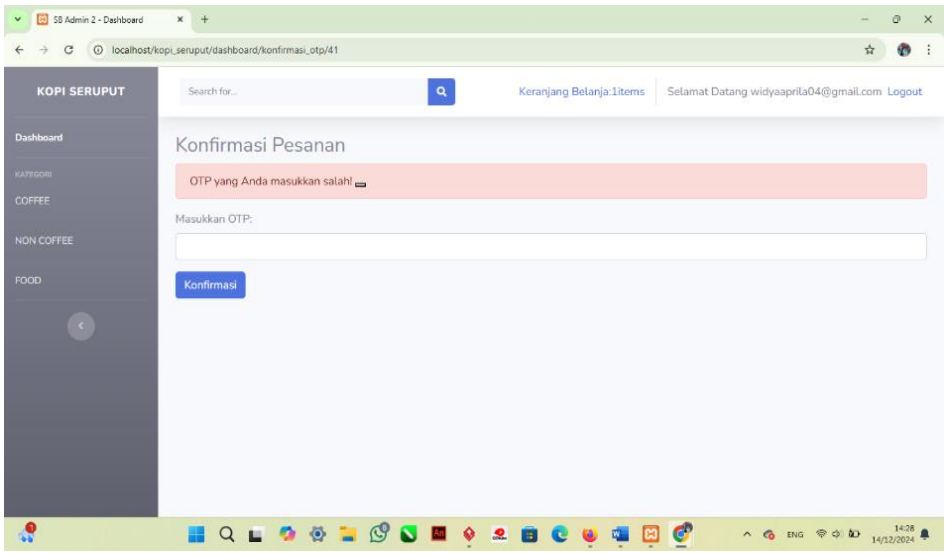
Gambar 8. Tampilan Order Processing



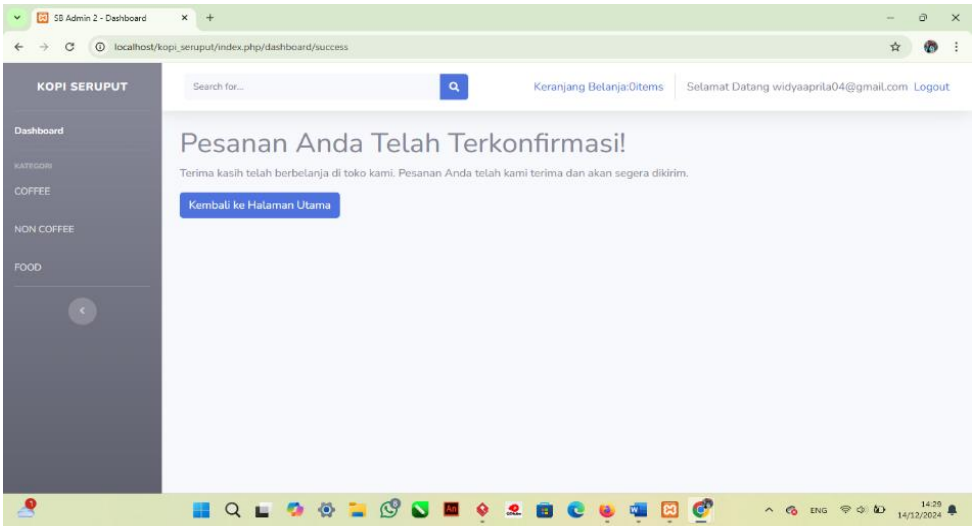
Gambar 9. Tampilan Konfirmasi Pesanan



Gambar 10. Tampilan Email Konfirmasi Pesanan



Gambar 11. Tampilan Konfirmasi Pesanan Dengan OTP Salah



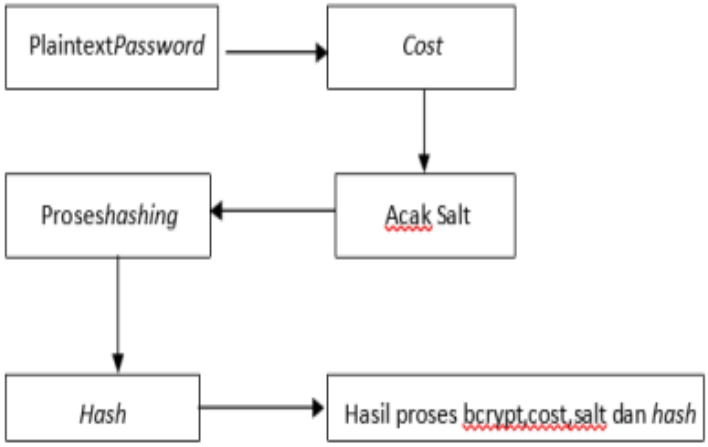
Gambar 12. Tampilan Halaman Pesanan Sukses

Penjelasan

Gambaran password bcrypt yang telah dibuat diamankan oleh algoritma bcrypt. Misalnya pengguna mencoba memasukkan sebuah password dengan nama kalimat yang di inginkan yaitu “password” maka password bcrypt yang di hasilkan:

$2y$10$HSn/q2XQXKJJ.JOBFUnL/eFlEfQOWHnc1m9Jy5KZp9kSA.mj2B5IC

Berikut ini adalah proses pembuatan password Bcrypt



Gambar 13. Alur Proses Pembuatan Password Bycript

Dari Gambar 13 menampilkan hasil pembuatan password yang diproses algoritma Bcrypt dengan penggabungan dari algortima Bcrypt, cost, salt dan hash untuk menghasilkan password Bcrypt yang mana hasilnya seperti di bawah ini:

$2y$10$HSn/q2XQXKJJ.JOBFUnL/eFlEfQOWHnc1m9Jy5KZp9kSA.mj2B5IC

Keterangan

$2y$: Bycrypt

10$: Cost

HSn/q2XQXKJJ.JOBFUnL/e : Salt

FlEfQOWHnc1m9Jy5KZp9kSA.mj2B5IC : Password Hash

Langkah-langkah proses pada Gambar 13 dijelaskan sebagai berikut:

1. Tentukan nama password yang akan di inputkan. Disini penulis mengambil contoh dari dengan nama kalimat yang di inginkan.
2. Inputkan jumlah cost yang akan diproses hash. Default yang penulis inputkan yaitu cost 10. Standar jumlah cost bisa 10-14.
3. Saat cost telah di inputkan atau dipilih maka proses salt akan berjalan dengan sendirinya melakukan proses acak salt. Saat proses acak salt telah diproseskan menghasilkan kode unik dengan jumlah 22 karakter. Yaitu sebagai berikut:
4. Selanjutnya proses hashing dengan menggabungkan salt dan hash hingga menghasilkan karakter hash dan salt sebagai berikut:

   HSn/q2XQXKJJ.JOBFUnL/eFlEfQOWHnc1m9Jy5KZp9kSA.mj2B5IC

E-ISSN: 2985-3532

Terakhir menghasilkan password bcrypt dari semua proses yang telah dilakukan Algoritma Bcrypt. Berikut hasilnya:

$2y$10$HSn/q2XQXKJJ.JOBFUnL/eFlEfQOWHnc1m9Jy5KZp9kSA.mj2B5IC

IV. KESIMPULAN

Penerapan Multi-Factor Authentication (MFA) dan Algoritma Hash Bcrypt merupakan cara untuk meningkatkan keamanan data pengguna pada sistem pemesanan kopi. MFA menambahkan perlindungan tambahan dengan memastikan hanya pengguna yang memiliki akses ke perangkat atau informasi tertentu yang dapat masuk ke sistem. Sementara itu, algoritma hash Bcrypt menjaga kerahasiaan kata sandi dengan mengacaknya menggunakan metode yang sulit diretas. Pengujian membuktikan bahwa kombinasi sistem ini mampu mencegah akses yang tidak sah, melindungi data sensitif, dan mengurangi risiko pencurian informasi. Dengan begitu, sistem pemesanan kopi menjadi lebih aman, andal, dan dapat meningkatkan rasa percaya pengguna terhadap layanan yang diberikan.

V. REFERENSI

Akbar, Mochamad Dandi, and Antoni Antoni. 2022. "Aplikasi Absensi Pegawai Pada Dinas Komunikasi Dan Informatika Kabupaten Deli Serdang Dengan QR Code Menggunakan Algoritma Bcrypt." *sudo Jurnal Teknik Informatika* 1(1): 8–16. doi:10.56211/sudo.v1i1.2.

Permatasari, Nelly, and Yessi Mardiana. 2023. "Aplikasi Penyandian Pesan Teks Berbasis Web Menggunakan Algoritma Blowfish." *Mardiana, Yessi* 3(1): 61–68. https://proceeding.unived.ac.id/index.php/snasikom/article/view/145.

Ramadhan, Iqbal. 2020. "Strategi Keamanan Cyber Security Di Kawasan Asia Tenggara." *Jurnal Asia Pacific Studies* 3(2): 181–92. doi:10.33541/japs.v3i1.1081.

Sarah Hapsari, Nani, Yenni Fatman, and Email Penulis Korespondensi. 2020. "JURNAL MEDIA INFORMATIKA BUDIDARMA Implementasi Metode One Time Password Pada Sistem Pemesanan Online." *Jurnal Media Informatika Budidarma* 4: 930–39. doi:10.30865/mib.v4i4.2195.

Siagian, Lauder, Arief Budiarto, and Simatupang. 2018. "Peran Keamanan Siber Dalam Mengatasi Konten Negatif Guna Mewujudkan Ketahanan Informasi Nasional." *Jurnal Peperangan Asimetris (PA)* 4(3): 1–18.

Sudiarto Raharjo, Willy, Ignatia Dhian E.K. Ratri, and Henry Susilo. 2017. "Implementasi Two Factor Authentication Dan Protokol Zero Knowledge Proof Pada Sistem Login." *Jurnal Teknik Informatika dan Sistem Informasi* 3(1): 127–36. doi:10.28932/jutisi.v3i1.579.

Widyasari, Ratnadira. 2016. "Implementasi Algoritma Boyer-Moore Untuk Menyisipkan Pesan Rahasia Pada Gambar."

E-ISSN: 2985-3532