PENERAPAN KEAMANAN *TWO FACTOR-AUTHENTICATION* (2FA) PADA APLIKASI PEMESANAN PERCETAKAN PEMUDA GRAFIKA BERBASIS *MOBILE*

Juliyono, Rezki Kurniati, Pretti Ristra
Teknik Informatika, Politeknik Negeri Bengkalis
Jalan Bathin Alam Desa Sungai Alam, Kab. Bengkalis, Indonesia
juliyonospk@gmail.com

ABSTRAK

Perkembangan teknologi *mobile* mendorong meningkatnya pemanfaatan aplikasi berbasis *smartphone* dalam mendukung aktivitas bisnis, termasuk di bidang percetakan. Namun, sistem pemesanan di Percetakan Pemuda Grafika masih dilakukan secara manual melalui kunjungan langsung atau komunikasi via WhatsApp dan telepon. Kondisi ini menyebabkan pelanggan kesulitan memperoleh informasi lengkap mengenai jenis layanan, harga produk, serta estimasi waktu pengerjaan, karena harus berkomunikasi satu per satu dengan admin. Selain itu, pelanggan tidak dapat memantau status pesanan secara langsung sehingga menimbulkan ketidakpastian dan ketidaknyamanan dalam proses pemesanan. Penelitian ini bertujuan untuk membangun aplikasi pemesanan percetakan berbasis *mobile* yang menampilkan katalog layanan secara lengkap serta dilengkapi dengan sistem keamanan *Two-Factor Authentication* (2FA) menggunakan *One-Time Password* (OTP). Metode pengembangan sistem yang digunakan adalah prototyping dengan melibatkan umpan balik pengguna secara bertahap. Hasil penelitian menunjukkan bahwa aplikasi mampu menyajikan informasi layanan secara jelas, memudahkan proses pemesanan, menyediakan pemantauan status pesanan secara *real-time*, serta penerapan 2FA berbasis OTP mampu meningkatkan keamanan proses login pengguna.

Kata kunci : *aplikasi mobile, pemesanan percetakan, keamanan sistem, two-factor authentication, OTP*

1. PENDAHULUAN

Kemajuan teknologi informasi dan meningkatnya penggunaan *smartphone* telah mengubah pola transaksi masyarakat, termasuk dalam proses pemesanan produk dan jasa. *Smartphone* yang mudah digunakan dan bersifat praktis mendorong pemanfaatannya dalam berbagai aktivitas, seperti pembelian produk secara *online*. Kondisi ini menjadikan aplikasi *mobile* sebagai solusi yang efektif untuk mendukung layanan usaha, termasuk di bidang percetakan [1].

Sejalan dengan perkembangan tersebut, tren belanja masyarakat Indonesia menunjukkan adanya pergeseran ke arah belanja online, yang sebagian besar konsumennya mengombinasikan belanja online dan offline dengan kecenderungan lebih memilih layanan online karena dinilai lebih praktis dan efisien [2].

Namun, sistem pemesanan di Percetakan Pemuda Grafika masih dilakukan secara manual, yaitu pelanggan harus datang langsung ke lokasi atau menghubungi admin melalui WhatsApp. Kondisi ini menyebabkan pelanggan kesulitan memperoleh informasi produk secara lengkap, seperti jenis layanan, harga, dan estimasi waktu pengerjaan. Selain itu, pelanggan tidak dapat memantau status pesanan secara langsung, sehingga menimbulkan ketidakpastian dan ketidaknyamanan. Dari sisi pengelola, sistem manual juga menyulitkan dalam pengelolaan dan pemantauan pesanan, sehingga proses pelayanan menjadi kurang efisien.

Berdasarkan permasalahan tersebut, penelitian ini bertujuan untuk membangun aplikasi pemesanan percetakan berbasis *mobile* yang mampu menyediakan katalog produk, fitur pemesanan *online*, unggah bukti pembayaran, serta pemantauan status pesanan secara *real-time*. Aplikasi ini diharapkan dapat meningkatkan efisiensi proses pemesanan serta memudahkan pelanggan dalam memperoleh informasi dan melakukan transaksi secara online.

Dalam pengembangannya, aplikasi ini juga menyimpan berbagai informasi penting seperti data pelanggan, detail pesanan, dan bukti pembayaran sehingga aspek keamanan akun pengguna menjadi hal yang perlu diperhatikan [3]. Sistem autentikasi berbasis password masih memiliki celah keamanan, terutama jika pengguna menggunakan kata sandi yang lemah dan mudah ditebak [4]. Oleh karena itu, penelitian ini menerapkan *Two-Factor Authentication* (2FA) menggunakan *One-Time Password* (OTP) yang dikirim melalui email sebagai lapisan keamanan tambahan untuk meningkatkan keamanan login dan melindungi data pengguna dari akses tidak sah. Penerapan 2FA berbasis OTP ini diharapkan dapat meminimalisir risiko penyalahgunaan akun serta meningkatkan kepercayaan dan kenyamanan pengguna dalam menggunakan aplikasi pemesanan percetakan berbasis *mobile*.

2. TINJAUAN PUSTAKA

Bagian ini membahas teori dan konsep yang relevan sebagai landasan untuk memahami permasalahan penelitian, menyusun alur pemikiran, serta mendukung proses analisis yang dilakukan.

2.1. Penelitian Terdahulu

Penelitian berjudul "Pengembangan Metode Login *Two-Factor Authentication* (2FA) untuk Keamanan Sistem Informasi Akademik" membahas

penerapan 2FA berbasis *One-Time Password* (OTP) untuk meningkatkan keamanan proses login. Metode yang digunakan adalah prototyping. Hasil penelitian menunjukkan bahwa penerapan 2FA mampu menambah lapisan keamanan dan mencegah akses tidak sah ke dalam sistem [3].

Penelitian berjudul "Implementasi Algoritma OTP dan HMAC untuk Two-Factor Authentication Sistem Login Relawan Pemilu" membahas penerapan kombinasi *One-Time Password* (OTP) dan HMAC pada sistem login. Hasil penelitian menunjukkan bahwa penerapan OTP yang bersifat dinamis dan verifikasi HMAC mampu meningkatkan keamanan autentikasi serta melindungi sistem dari serangan pencurian kata sandi dan brute force [4].

Penelitian berjudul "Aplikasi E-Commerce Berbasis Android yang Terintegrasi Payment Gateway pada Pondok Grafis" membahas pengembangan aplikasi *e-commerce* berbasis Android untuk mendukung usaha percetakan digital. Hasil penelitian menunjukkan bahwa aplikasi yang dikembangkan mampu meningkatkan efisiensi transaksi, pengelolaan produk, serta mendukung pembayaran online dan komunikasi dengan pelanggan secara terintegrasi [1].

2.2. Penerapan

Penerapan merupakan suatu proses implementasi dari teori, konsep, atau kebijakan yang diwujudkan melalui kegiatan nyata oleh pihak terkait. Proses ini menjadi dasar dalam pelaksanaan suatu tindakan, baik yang dilakukan secara individu maupun kelompok, dengan tujuan mencapai sasaran yang telah ditetapkan. Penerapan tidak hanya mencakup tahap pelaksanaan, tetapi juga melibatkan proses penyesuaian terhadap kondisi dan kebutuhan yang ada agar tujuan yang diharapkan dapat tercapai secara efektif.

Selain itu, penerapan dapat dipahami sebagai bentuk realisasi suatu kebijakan yang dilakukan oleh instansi pemerintah maupun swasta untuk mewujudkan target tertentu. Dalam konteks sistem informasi, penerapan berperan penting dalam mengimplementasikan rancangan sistem ke dalam bentuk yang dapat digunakan secara langsung oleh pengguna, sehingga konsep dan perencanaan yang telah dibuat dapat memberikan manfaat nyata sesuai dengan fungsi yang dirancang [5].

2.3. Keamanan

Keamanan adalah kondisi di mana sistem dan data berada dalam keadaan terlindungi dari berbagai potensi ancaman, baik yang berasal dari aktivitas manusia maupun kejadian yang tidak terduga. Ancaman keamanan dapat berupa perusakan data, kebocoran informasi, perubahan data tanpa izin, hingga penyalahgunaan sistem. Dalam aplikasi digital, aspek keamanan sangat penting karena berkaitan dengan perlindungan data pengguna serta keandalan sistem. Penerapan mekanisme keamanan yang baik dapat meningkatkan kepercayaan pengguna dan mendukung keberlangsungan layanan serta aktivitas bisnis [6].

2.4. Two-Factor Authentication

Two-Factor Authentication (2FA) merupakan metode autentikasi pengguna yang memanfaatkan dua faktor verifikasi yang bersifat independen untuk memastikan keaslian identitas pengguna. Metode ini mengharuskan pengguna tidak hanya memasukkan kata sandi sebagai faktor pertama, tetapi juga melalui proses verifikasi tambahan yang berasal dari sumber berbeda sebagai faktor kedua. Faktor autentikasi tambahan tersebut dapat berupa kode verifikasi, perangkat tertentu, atau karakteristik lain yang dimiliki oleh pengguna. Dengan penerapan 2FA, risiko pihak yang tidak berwenang memperoleh akses ke dalam sistem dapat diminimalkan, karena meskipun kata sandi berhasil diketahui, akses tetap tidak dapat dilakukan tanpa memenuhi faktor autentikasi kedua yang valid [7].

2.5. OTP

Proses autentikasi dilakukan oleh sistem dengan menghasilkan kode verifikasi yang bersifat dinamis setiap kali pengguna melakukan aktivitas tertentu, atau kode tersebut dapat berubah secara otomatis dalam periode waktu tertentu. *One-Time Password* (OTP) dirancang dengan masa berlaku terbatas untuk meningkatkan tingkat keamanan sistem dengan memastikan bahwa kode hanya dapat digunakan dalam jangka waktu tertentu. Penerapan batas waktu ini bertujuan untuk mengurangi kemungkinan penyalahgunaan kode oleh pihak yang tidak berwenang. Apabila kode OTP memiliki waktu aktif yang terlalu lama, maka risiko terjadinya serangan brute force akan meningkat, yaitu upaya penebakan kode secara berulang hingga berhasil. Setelah proses autentikasi berhasil dilakukan dan kode OTP terverifikasi dengan benar, pengguna dapat melanjutkan aktivitas atau transaksi pada sistem e-commerce secara aman [8].

2.6. Android

Android merupakan sistem operasi sekaligus platform pengembangan aplikasi yang dikembangkan oleh Google untuk perangkat seluler, seperti smartphone dan tablet. Platform ini bersifat terbuka dan dapat digunakan pada berbagai jenis perangkat dari beragam produsen, sehingga memiliki tingkat adopsi yang sangat luas. Android menyediakan Software Development Kit (SDK) yang memungkinkan pengembang untuk merancang, membangun, menguji, dan mengimplementasikan aplikasi secara native dengan memanfaatkan berbagai Application Programming Interface (API) yang tersedia. Selain itu, Android menyediakan layanan distribusi aplikasi melalui marketplace resmi, yang mendukung proses publikasi, pembaruan, serta pengelolaan aplikasi secara terpusat. Dengan ekosistem yang terintegrasi tersebut, Android menjadi

salah satu platform utama dalam pengembangan aplikasi *mobile* [9].

2.7. Flutter

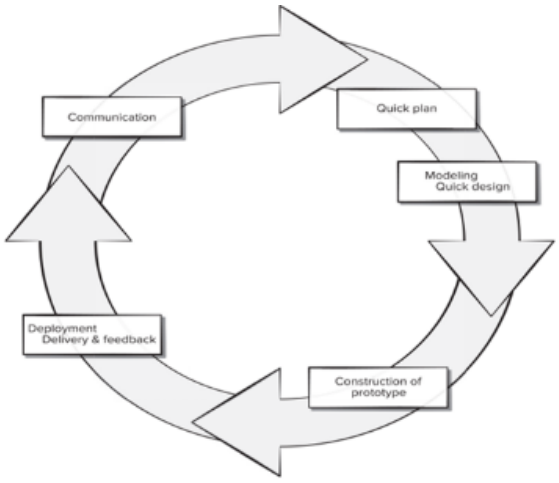
Flutter merupakan perangkat pengembangan aplikasi yang berfungsi sebagai framework sekaligus Software Development Kit (SDK) untuk membangun antarmuka pengguna pada aplikasi *mobile* secara efisien. Framework ini bersifat open-source sehingga pengembang dari berbagai komunitas dapat berkontribusi dalam pengembangannya. Flutter memungkinkan pembuatan aplikasi lintas platform dengan satu basis kode yang dapat dijalankan pada berbagai platform, seperti *mobile*, web, dan desktop. Tujuan utama penggunaan Flutter adalah menghasilkan performa aplikasi yang mendekati aplikasi native, sekaligus mempercepat dan mempermudah proses pengembangan aplikasi [10].

3. METODE PENELITIAN

Bagian ini membahas metode penelitian yang digunakan dalam pengembangan sistem serta tahapan-tahapan yang dilakukan dalam proses penelitian.

3.1. Metode Prototyping

Penelitian ini menggunakan metode prototyping sebagai metode pengembangan sistem. Metode prototyping memiliki tahapan yang dimulai dari komunikasi antara pengembang dan pengguna untuk menggali kebutuhan sistem. Selanjutnya dilakukan perencanaan cepat (quick plan) dan pembuatan desain awal (modeling quick design). Tahap berikutnya adalah pembangunan prototype (construction of prototype) yang kemudian diuji dan dievaluasi melalui proses penyerahan serta umpan balik pengguna (deployment, delivery & feedback). Umpan balik yang diperoleh digunakan sebagai dasar penyempurnaan sistem hingga sesuai dengan kebutuhan pengguna. Tahapan metode prototyping yang digunakan dalam penelitian ini ditunjukkan pada gambar 1 [3].



Gambar 1. Metode Prototyping [3]

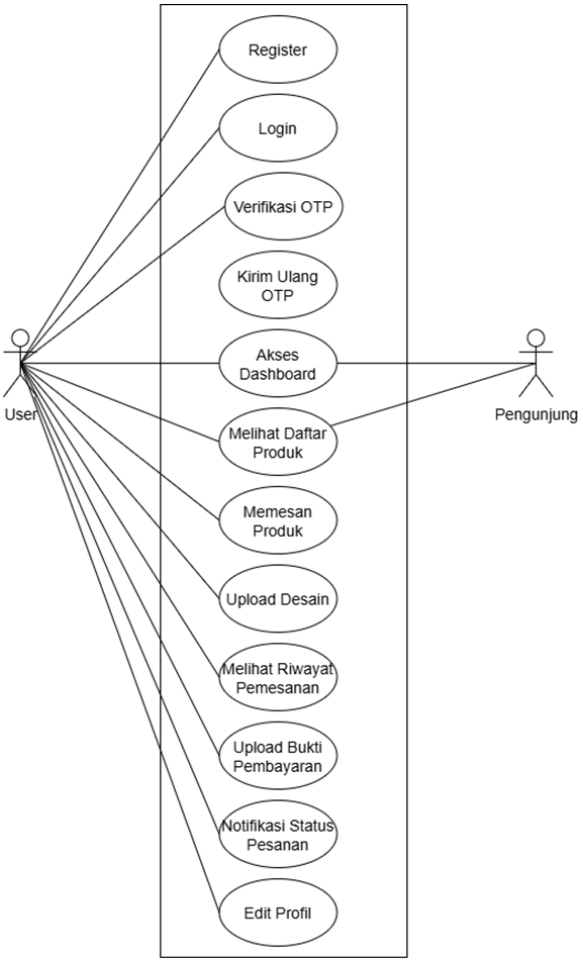
3.2. Tahapan Metode Prototyping

Berdasarkan diagram metode prototyping pada gambar tersebut, tahapan pengembangan sistem dilakukan secara berulang dan melibatkan pengguna secara langsung. Tahapan metode prototyping terdiri dari beberapa langkah sebagai berikut:

a. Communication
   Tahap ini merupakan proses komunikasi antara pengembang dan pengguna untuk menggali kebutuhan sistem. Pada tahap ini dilakukan pengumpulan informasi terkait kebutuhan fungsional dan nonfungsional, termasuk kebutuhan keamanan login dan alur pemesanan aplikasi.
b. Quick Plan
   Setelah kebutuhan sistem diperoleh, dilakukan perencanaan cepat untuk menentukan ruang lingkup pengembangan, fitur utama yang akan dibangun, serta tujuan pembuatan prototype. Tahap ini bertujuan memberikan gambaran awal arah pengembangan sistem.
c. Modeling / Quick Design
   Tahap ini meliputi perancangan desain awal sistem sebagai representasi dari kebutuhan pengguna. Desain yang dibuat mencakup rancangan antarmuka aplikasi, alur proses sistem, serta mekanisme autentikasi pengguna menggunakan OTP.
d. Construction of Prototype
   Pada tahap ini dilakukan pembangunan prototype berdasarkan desain awal yang telah dibuat. Prototype mencakup implementasi fitur utama sistem, seperti login, verifikasi OTP, dan pemesanan produk, sehingga pengguna dapat mencoba langsung sistem yang dikembangkan.
e. Deployment, Delivery & Feedback
   Prototype yang telah dibangun kemudian diserahkan kepada pengguna untuk diuji dan dievaluasi. Pengguna memberikan umpan balik terkait fungsionalitas, kemudahan penggunaan, dan keamanan sistem. Umpan balik ini digunakan sebagai dasar untuk melakukan perbaikan dan penyempurnaan prototype.

3.3. Perancangan Sistem

Use case diagram digunakan untuk menggambarkan interaksi antara aktor dan sistem pada proses pemesanan produk. Diagram ini menunjukkan fungsi utama sistem yang dapat diakses oleh masing-masing aktor sesuai dengan perannya.



Gambar 2. *Use Case* Diagram

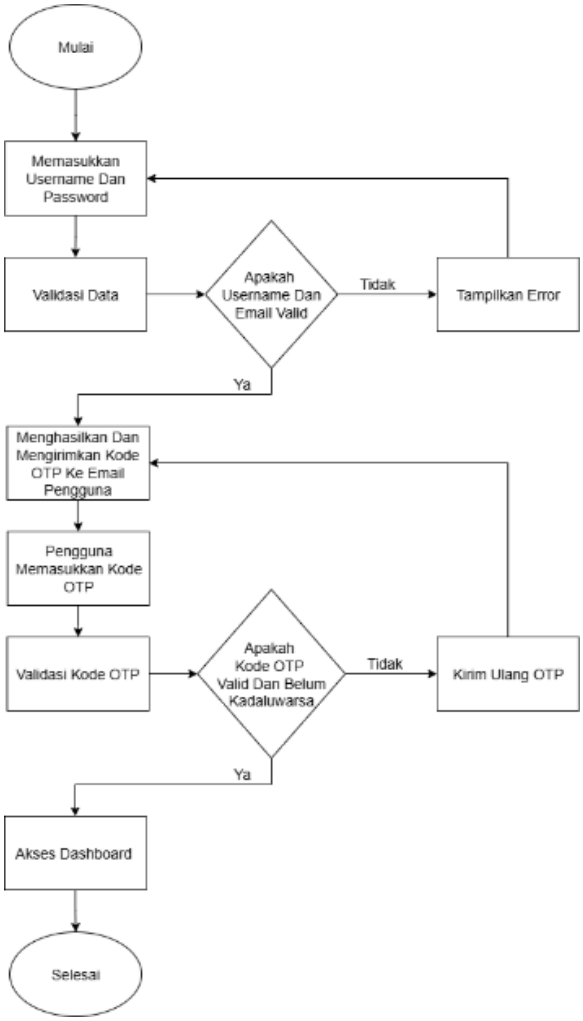
Berdasarkan Gambar 2, sistem melibatkan dua aktor utama, yaitu User dan Pengunjung, yang masing-masing memiliki hak akses berbeda sesuai dengan perannya. Pengunjung memiliki akses terbatas yang hanya mencakup melihat daftar produk dan mengakses *dashboard* sebagai bentuk interaksi awal dengan sistem tanpa harus melakukan autentikasi. Akses ini memungkinkan calon pengguna untuk memperoleh informasi terkait produk yang tersedia sebelum memutuskan untuk menggunakan layanan secara penuh.

Sementara itu, User merupakan aktor yang telah terdaftar dan memiliki hak akses penuh terhadap seluruh fungsi utama sistem. Hak akses tersebut meliputi pendaftaran akun, login, verifikasi *One-Time Password* (OTP), pemesanan produk, unggah desain, unggah bukti pembayaran, serta pemantauan status pesanan. Dengan adanya pembagian peran ini, sistem dapat mengelola interaksi pengguna secara lebih terstruktur dan memastikan bahwa setiap fungsi hanya dapat diakses oleh pengguna yang memiliki otorisasi yang sesuai.

Perancangan use case ini bertujuan untuk memodelkan kebutuhan fungsional sistem serta menggambarkan batasan interaksi antara aktor dan sistem. Pembagian hak akses antara User dan Pengunjung juga berperan dalam meningkatkan keamanan sistem dan menjaga keteraturan proses pemesanan, sehingga alur penggunaan sistem menjadi lebih jelas dan terkontrol.

3.4. Perancangan Keamanan Menggunakan OTP

Untuk meningkatkan keamanan proses login, sistem menerapkan mekanisme *Two-Factor Authentication* (2FA) yang mengombinasikan penggunaan password dan *One-Time Password* (OTP). Mekanisme ini dirancang untuk memberikan lapisan keamanan tambahan sehingga hanya pengguna yang memiliki kredensial dan akses ke email terdaftar yang dapat masuk ke dalam sistem.



Gambar 3. Alur *Two-Factor Authentication*

Berdasarkan Gambar 3, proses autentikasi dirancang melalui dua tahap verifikasi untuk meningkatkan keamanan akses pengguna ke dalam sistem. Tahap pertama dilakukan dengan memvalidasi email dan password yang dimasukkan oleh pengguna sebagai faktor autentikasi awal. Pada tahap ini, sistem akan mencocokkan data login pengguna dengan data yang tersimpan pada basis data. Apabila data login tidak valid, sistem akan menolak akses dan meminta pengguna untuk mengulangi proses login.

Jika tahap pertama berhasil, sistem akan melanjutkan ke tahap kedua dengan mengirimkan kode *One-Time Password* (OTP) ke email pengguna yang telah terdaftar. OTP berfungsi sebagai faktor autentikasi tambahan yang bersifat unik dan hanya dapat digunakan dalam jangka waktu tertentu. Setelah menerima kode OTP, pengguna diminta untuk memasukkan kode tersebut ke dalam sistem untuk dilakukan proses verifikasi lanjutan. Sistem akan memeriksa kesesuaian kode OTP yang dimasukkan serta memastikan bahwa kode tersebut masih berada dalam masa aktif.

Apabila kode OTP valid dan belum kedaluwarsa, sistem akan memberikan akses kepada pengguna untuk masuk ke *dashboard*. Sebaliknya, jika kode OTP yang dimasukkan tidak sesuai atau telah melewati batas waktu penggunaan, sistem akan menolak proses autentikasi. Dalam kondisi tersebut, pengguna disediakan fitur pengiriman ulang OTP untuk memperoleh kode baru yang masih aktif. Perancangan mekanisme autentikasi dua tahap ini bertujuan untuk memastikan bahwa proses login hanya dapat diselesaikan oleh pengguna yang memiliki kredensial akun dan akses sah terhadap email terdaftar, sehingga risiko akses tidak sah dapat diminimalkan.

4. HASIL DAN PEMBAHASAN

Bagian ini menyajikan hasil pengujian sistem serta pembahasan terhadap penerapan keamanan dan fungsionalitas sistem yang dikembangkan.

4.1. Hasil Pengujian Sistem

Pengujian sistem dilakukan untuk mengevaluasi kinerja sistem dari sisi keamanan dan fungsionalitas. Pengujian keamanan difokuskan pada penerapan *Two-Factor Authentication* (2FA) berbasis *One-Time* Password (OTP) guna memastikan proses autentikasi pengguna berjalan sesuai dengan rancangan. Sementara itu, pengujian fungsional dilakukan untuk memastikan bahwa fitur utama sistem dapat berjalan dengan baik dan saling terintegrasi dalam mendukung proses pemesanan. Melalui pengujian ini, sistem dievaluasi untuk mengetahui kesesuaian antara fungsi yang dirancang dengan kebutuhan pengguna.

Tabel 1. Hasil Pengujian *Two-Factor Authentication* (2FA)

No	Skenario Pengujian	Hasil yang diharapkan	Keterangan
1	Login email dan password benar	Kode OTP dikirm ke email	Berhasil
2	Login email dan password salah	Login ditolak	Berhasil
3	OTP benar dan aktif	Login berhasil	Berhasil
4	OTP salah	Login gagal	Berhasil
5	OTP kadaluwarsa	Login ditolak	Berhasil
6	Kirim ulang OTP	Kode OTP baru dikirim	Berhasil

Berdasarkan Tabel 1, hasil pengujian menunjukkan bahwa mekanisme *Two-Factor Authentication* (2FA) berbasis *One-Time Password* (OTP) dapat berjalan dengan baik dan sesuai dengan rancangan sistem. Sistem mampu mengirimkan kode OTP ketika data login valid serta menolak akses ketika kredensial login atau kode OTP yang dimasukkan tidak sesuai maupun telah kedaluwarsa. Hal ini menunjukkan bahwa proses autentikasi dua tahap dapat diterapkan secara konsisten untuk meningkatkan keamanan akses pengguna.

Keberhasilan sistem dalam menangani berbagai skenario pengujian, seperti OTP salah, OTP kedaluwarsa, dan pengiriman ulang OTP, menunjukkan bahwa mekanisme verifikasi yang diterapkan cukup andal dalam mencegah akses tidak sah. Fitur kirim ulang OTP juga berfungsi dengan baik untuk menghasilkan kode baru ketika pengguna tidak menerima OTP sebelumnya atau ketika masa aktif OTP telah berakhir, sehingga proses login tetap dapat dilanjutkan tanpa mengurangi tingkat keamanan sistem.

Penerapan OTP dengan masa aktif terbatas berperan penting dalam meminimalkan risiko penyalahgunaan kode verifikasi oleh pihak yang tidak berwenang. Dengan demikian, mekanisme 2FA berbasis OTP tidak hanya meningkatkan keamanan autentikasi, tetapi juga tetap mempertahankan kemudahan penggunaan sistem karena proses verifikasi dapat dilakukan secara cepat dan sederhana oleh pengguna.

Tabel 2. Hasil Pengujian Aplikasi

No	Skenario Pengujian	Hasil yang diharapkan	Keterangan
1	Akses beranda setelah login	Halaman beranda ditampilkan	Berhasil
2	Memilih produk dari katalog	Sistem menampilkan detail produk	Berhasil
3	Mengisi form pemesanan	Data pesanan tersimpan	Berhasil
4	Upload desain pesanan	File desain berhasil diunggah	Berhasil
5	Melakukan upload bukti pembayaran	Bukti pembayaran tersimpan	Berhasil
6	Verifikasi pembayaran	Status pesanan diperbarui	Berhasil
7	Melihat status pesanan	Daftar dan status pesanan ditampilkan	Berhasil
8	Konfirmasi pesanan selesai	Status pesanan menjadi selesai	Berhasil

Berdasarkan Tabel 2, hasil pengujian menunjukkan bahwa seluruh fitur fungsional sistem dapat berjalan sesuai dengan yang diharapkan dan mendukung alur pemesanan secara menyeluruh. Proses pemesanan, unggah desain, konfirmasi

pembayaran, serta pemantauan status pesanan dapat dilakukan dengan baik tanpa kendala yang berarti, sehingga pengguna dapat menyelesaikan proses pemesanan secara berurutan dan terstruktur.

Kemampuan sistem dalam menampilkan dan memperbarui status pesanan sesuai dengan tahapan proses yang berjalan menunjukkan bahwa integrasi antarfitur telah berjalan dengan baik. Setiap perubahan status dapat diinformasikan kepada pengguna secara tepat, sehingga pengguna dapat memantau perkembangan pesanan tanpa harus melakukan komunikasi manual dengan pihak percetakan.

Hasil pengujian ini menunjukkan bahwa sistem yang dikembangkan mampu memberikan kemudahan dan efisiensi dalam proses pemesanan dibandingkan dengan sistem manual. Dengan adanya sistem pemesanan berbasis *mobile*, pengguna dapat melakukan pemesanan dan pemantauan status pesanan secara mandiri, sehingga dapat meningkatkan kualitas layanan serta mengurangi potensi kesalahan dalam pengelolaan pesanan.

4.2. Tampilan Antarmuka Autentikasi Sistem

Bagian ini menampilkan antarmuka sistem yang digunakan dalam proses autentikasi pengguna sebagai pendukung hasil pengujian mekanisme *Two-Factor Authentication* (2FA) berbasis *One-Time Password* (OTP) yang telah dilakukan sebelumnya. Antarmuka ini menunjukkan tahapan autentikasi yang harus dilalui pengguna, mulai dari login menggunakan email dan password hingga proses verifikasi OTP sebagai faktor keamanan tambahan.

Gambar 4. Tampilan Login Menggunakan Email dan Password

Gambar 4 menunjukkan halaman login sistem yang digunakan oleh pengguna untuk mengakses aplikasi. Pada halaman ini, pengguna diminta memasukkan email dan password sebagai tahap awal autentikasi sebelum sistem melanjutkan ke proses pengiriman kode OTP.

Setelah pengguna berhasil melewati tahap autentikasi awal dengan memasukkan email dan password yang valid, sistem akan melanjutkan proses keamanan ke tahap berikutnya, yaitu pengiriman *One-Time Password* (OTP). Tahap ini merupakan bagian dari penerapan *Two-Factor Authentication* (2FA) yang bertujuan untuk memastikan bahwa pengguna yang melakukan login benar-benar memiliki akses sah terhadap akun dan alamat email yang terdaftar pada sistem.

Gambar 5. Hasil Pengiriman *One-Time Password* (OTP) ke Email Pengguna

Setelah proses login menggunakan email dan password berhasil, sistem secara otomatis mengirimkan kode One-*Time Password* (OTP) ke alamat email pengguna. Gambar 5 menunjukkan contoh pesan email yang diterima oleh pengguna yang berisi kode OTP beserta informasi masa berlaku kode selama 1 menit. Pengiriman OTP melalui email ini berfungsi sebagai faktor autentikasi kedua yang bersifat sementara dan hanya dapat digunakan dalam jangka waktu tertentu, sehingga dapat meningkatkan keamanan akses sistem dan mencegah penyalahgunaan kode oleh pihak yang tidak berwenang.

Selanjutnya, sistem menampilkan halaman verifikasi One-Time Password (OTP) sebagai tahap lanjutan autentikasi sebelum pengguna diberikan akses ke dalam sistem.

Setelah menerima kode OTP melalui email, pengguna diarahkan ke halaman verifikasi OTP untuk memasukkan kode yang diterima seperti ditunjukkan pada Gambar 6. Halaman ini digunakan sebagai tahap kedua autentikasi untuk memvalidasi keaslian pengguna sebelum diberikan akses ke dalam sistem, sehingga keamanan proses login dapat lebih terjamin.

Gambar 6. Tampilan Verifikasi *One-Time Password* (OTP)

4.3. Pembahasan Hasil Pengujian

Hasil pengujian sistem menunjukkan bahwa mekanisme keamanan dan fitur fungsional sistem dapat berjalan sesuai dengan kebutuhan. Penerapan *Two-Factor Authentication* (2FA) berbasis *One-Time Password* (OTP) memberikan lapisan keamanan tambahan pada proses autentikasi pengguna, sehingga risiko akses tidak sah dapat diminimalkan meskipun kredensial login diketahui oleh pihak lain.

Dari hasil pengujian autentikasi, sistem mampu melakukan verifikasi dua tahap secara konsisten, termasuk pengiriman OTP, validasi kode, serta penanganan kondisi OTP tidak valid maupun kedaluwarsa. Hal ini menunjukkan bahwa mekanisme keamanan yang diterapkan cukup andal dan dapat digunakan sebagai solusi pengamanan akses pada sistem pemesanan berbasis *mobile*.

Selain dari sisi keamanan, hasil pengujian fungsional menunjukkan bahwa seluruh fitur utama sistem dapat digunakan dengan baik dan saling terintegrasi. Proses pemesanan, unggah desain, unggah bukti pembayaran, serta pemantauan status pesanan dapat dilakukan secara berurutan tanpa kendala berarti. Hal ini menunjukkan bahwa sistem mampu mendukung alur pemesanan lebih terstruktur dibandingkan proses manual yang sebelumnya digunakan.

Penerapan mekanisme keamanan 2FA pada sistem tidak mengganggu kenyamanan pengguna dalam menggunakan aplikasi. Proses verifikasi tambahan tetap dapat dilakukan secara cepat dan sederhana, sehingga tercapai keseimbangan antara peningkatan keamanan dan kemudahan penggunaan. Dengan demikian, sistem yang dikembangkan tidak hanya aman, tetapi juga tetap efisien dan mudah digunakan oleh pengguna.

5. KESIMPULAN DAN SARAN

Berdasarkan hasil penelitian yang telah dilakukan, penerapan *Two-Factor Authentication* (2FA) berbasis *One-Time Password* (OTP) pada sistem pemesanan percetakan berbasis *mobile* mampu meningkatkan keamanan proses autentikasi pengguna melalui mekanisme verifikasi dua tahap. Hasil pengujian menunjukkan bahwa sistem mampu menolak akses tidak sah serta seluruh fitur fungsional, seperti pemesanan, unggah desain, unggah bukti pembayaran, dan pemantauan status pesanan, dapat berjalan dengan baik tanpa mengganggu alur penggunaan aplikasi. Sebagai saran untuk pengembangan selanjutnya, sistem dapat ditingkatkan dengan menambahkan integrasi pembayaran otomatis, notifikasi status pesanan, serta metode autentikasi alternatif guna meningkatkan kenyamanan dan keamanan pengguna.

DAFTAR PUSTAKA

[1] M. A. Yaqin, T. Listyorini, and E. Supriyati, "Aplikasi E-Commerce Berbasis Android Yang Terintegrasi Payment Gateway Pada Pondok Grafis," *Jurnal Dialektika Informatika (Detika)*, vol. 4, no. 1, pp. 19–25, Jan. 2024, doi: 10.24176/detika.v4i1.11005.

[2] J. P. Tambusai, D. Naagista, and H. Riofita, "Faktor Penyebab Pelanggan Lebih Memilih Pembelian Secara Online dari Pada Offline," *Jurnal Pendidikan Tambusai*, vol. 8, no. 3, pp. 47102–47108, Jan. 2024.

[3] Yusuf Heriyanto, Anas Azhimi Qalban, and Iif Alfiatul Mukaromah, "Pengembangan Metode Login Two Factor Authentication (2FA) untuk Keamanan Sistem Informasi Akademik," *Journal of Innovation Information Technology and Application (JINITA)*, vol. 4, no. 2, pp. 142–150, Dec. 2022, doi: 10.35970/jinita.v4i2.1637.

[4] J. Teknika and C. Anwar, "Implementasi Algoritma OTP dan HMAC untuk Two-Factor Authentication Sistem Login Relawan Pemilu," *JURNAL TEKNIKA*, vol. 19, no. 1, pp. 83–94, Sep. 2024.

[5] R. RINJANI and N. Sari, "Analisis Penerapan Aplikasi Mobile Jkn Terhadap Peserta Badan Penyelenggara Jaminan Sosial Kesehatan Cabang Subulussalam," *PUBLIKA : Jurnal Ilmu Administrasi Publik*, vol. 8, no. 2, pp. 209–223, Oct. 2022, doi: 10.25299/jiap.2022.vol8(2).10491.

[6] M. O. Hoshmand and S. Ratnawati, "Analisis Keamanan Infrastruktur Teknologi Informasi dalam Menghadapi Ancaman Cybersecurity," *Jurnal Sains dan Teknologi*, vol. 5, no. 2, pp. 679–686, 2023, doi: 10.55338/saintek.v5i2.2347.

[7] N. J. Dewi, A. Firdonsyah, and D. Wijayanto, "Two factor authentication pada sistem login rekam medis elektronik berbasis web menggunakan metode prototype," in *Prosiding*

Seminar Nasional Penelitian dan Pengabdian Kepada Masyarakat, Feb. 2025.

[8] J. Rekayasa *et al.*, "IMPLEMENTASI ALGORITMA RSA DAN ONE TIME PASSWORD (OTP) UNTUK PENGAMANAN DATA PENGGUNA DAN PROSES TRANSAKSI PADA WEBSITE E-COMMERCE," *Coding: Jurnal Komputer dan Aplikasi*, vol. 11, no. 1, pp. 62–72, 2023.

[9] S. A. Wibawa and S. Noor, "SISTEM INFORMASI PEMESANAN DI KEDAI KOPI BERBASIS MOBILE ANDROID MENGGUNAKAN FLUTTER STUDI KASUS SOENDA KOPI SUBANG," *GLOBAL*, vol. 9, no. 2, Jul. 2022, [Online]. Available: http://ejournal.unsub.ac.id/index.php/Fasilkom

[10] M. B. Sinatria, Oman Komarudin, and Kamal Prihamdani, "PENERAPAN CLEAN ARCHITECTURE DALAM MEMBANGUN APLIKASI BERBASIS MOBILE DENGAN FRAMEWORK GOOGLE FLUTTER," *INFOTECH journal*, vol. 9, no. 1, pp. 132–146, May 2023, doi: 10.31949/infotech.v9i1.5237