JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 4, No. 3 Tahun 2026
ISSN 3025-0919 (media online)
Hal 726-741

Implementasi Sistem Two-Factor Authentication (2FA) pada Website Ar-Ridho Tours & Travel Menggunakan OTP Berbasis Email

Ilham Rifkih Saputra[1], Farizi Ilham[2], Bryan Ranindito Prevalno[3], Rafie Fathurrachman[4]

[1,2,3,4] Fakultas Ilmu Komputer, Program Studi Teknik Informatika, Universitas Pamulang, Tangerang Selatan, Indonesia
Email: [1] kagaktau770@gmail.com , [2]dosen02954@unpam.ac.id, [3]bryanr3443@gmail.com, [4]rafiefaturachman18@gmail.com

Abstrak−Teknologi informasi yang terus berkembang memberikan banyak kemudahan, salah satu bidang yang dimudahkan adalah layanan pemesanan perjalanan ibadah secara online, tapi terdapat juga resiko yang muncul akibat perkembangan teknologi informasi tersebut seperti peretasan akun dan pencurian data pribadi. PT Nur Ridho Elsunury melalui website Ar-Ridho Tours & Travel masih menggunakan autentikasi satu faktor (password), jadi lebih rentan terkena serangan siber. Penelitian ini bermaksudkan untuk menerapkan fungsi sistem Two-Factor Authentication dengan menggunakan One-Time Password (OTP) yang dapat dikirim, salah satunya melalui email. Sistem dibuat dengan framework Laravel memakai bahasa pemrograman PHP dan basis data MySQL. Prototyping dengan fitur utama yang termasuk verifikasi OTP saat login, backup code saat ada disituasi yang darurat, trusted device agar tidak banyak-banyak verifikasi dengan perangkat yang sama, juga pengiriman ulang kode OTP adalah metode pengembangan yang digunakan. Blackbox juga dilakukan dalam seluruh pengujian skenario fungsional, termasuk verifikasi OTP benar atau salahnya, kadaluwarsa kode, penggunaan backup kode, serta batasan berapa banyak percobaan login boleh gagal. Hasil pengujian membuktikan bahwa sistem 2F berjalan sesuai yang diharapkan, dapat mencegah akses walaupun pihak lain mengetahui password yang benar, dan memberikan pengalaman pengguna yang tetapny nyaman dengan fitur perangkat terpercaya. Implementasi ini amat diharapkan dapat meningkatkan keamanan data pelanggan, memperkuat kepercayaan publik dan pengguna, serta menjadi nilai kompetitif tambahan bagi Ar-Ridho Tours & Travel.

Kata Kunci: Two-Factor Authentication, OTP, keamanan web, Laravel, backup code

Abstract−*The ever-evolving information technology provides many conveniences, one of the areas facilitated is the online pilgrimage booking service, but there are also risks that arise due to the development of information technology such as account hacking and personal data theft. PT Nur Ridho Elsunury through the Ar-Ridho Tours & Travel website still uses one-factor authentication (password), so it is more vulnerable to cyber attacks. This study intends to implement the Two-Factor Authentication system function using One-Time Password (OTP) which can be sent, one of which is via email. The system is made with the Laravel framework using the PHP programming language and MySQL database. Prototyping with main features including OTP verification when logging in, backup codes in emergency situations, trusted devices to avoid multiple verifications with the same device, and resending OTP codes is the development method used. Blackbox is also carried out in all functional scenario testing, including OTP verification whether it is correct or not, code expiration, use of backup codes, and limits on how many login attempts can fail. Test results demonstrated that the 2F system performed as expected, preventing access even if a third party knew the correct password, and providing a consistent user experience with trusted device features. This implementation is expected to improve customer data security, strengthen public and user trust, and provide added competitive value for Ar-Ridho Tours & Travel.*

Keywords: *Two-Factor Authentication, OTP, web security, Laravel, backup code*

1. PENDAHULUAN

Teknologi informasi digital telah mengubah berbagai sektor bisnis menjadi lebih baik, salah satu sektor yang terdampak adalah industri travel dan sektor keagamaan. PT Nur Ridho Elsunury, melalui brand Ar-Ridho Tours & Travel, menyediakan layanan pemesanan paket umrah dan haji secara online melalui website resmi. Fitur-fitur yang diimplementasikan ini memberikan pelanggan akses untuk melakukan pendaftaran, memilih paket, melakukan pembayaran, sampai memantau status keberangkatan dari mana saja dan kapan saja. Tetapi, tidak luput dari kemudahan tersebut, terdapat berbagai risiko digital terhadap keamanan data dan privasi pengguna. Ancaman ini adalah tantangan serius yang tidak dapat diabaikan.

JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 4, No. 3 Tahun 2026
ISSN 3025-0919 (media online)
Hal 726-741

Berdasarkan wawancara dan observasi yang telah dilakukan dengan pihak Ar-Ridho Tours & Travels, diketahui bahwa sistem yang digunakan saat ini masih cukup rentan, yaitu menggunakan autentikasi satu factor (single-factor authentication) yang hanya berupa email dan password tanpa verifikasi tambahan. Strategi ini dapat diretas dengan mudah melalui serangan seperti brute force, credential stuffing, atau pencurian kata sandi. Data pribadi pelanggan seperti nama lengkap, nomor telepon, alamat, nomor KTP, hingga bukti pembayaran, dapat disalahgunakan oleh pihak yang tidak bertanggung jawab. Lalu, tidak adanya pemulihan darurat seperti kode cadangan (backup code) juga menambah berisiko pelanggan yang kehilangan akses atau lupa kata sandi.

Salah satu solusi yang cukup efektif untuk menangani kelemahan tersebut adalah dengan menggunakan 2FA (two-factor athentication). 2FA adalah teknik yang mengharuskan pengguna untuk melakukan verifikasi dengan dua faktor berbeda untuk mendapatkan akses ke akun pengguna. Faktor pertama adalah kata sandi yang diketahui pengguna dan yang kedua dapat berupa One-Time-Password yang dapat dikirim melalui email, sms, atau aplikasi autentikator. Dengan adanya mekanisme ini, walaupun password pelanggan diketahui pihak lain, mereka tidak bisa melewati faktor kedua. Penggunaan media email sebagai pengiriman OTP, menggunakan asumsi bahwa setiap pengguna memiliki akun email yang aktif, dan implementasi sistem 2FA cenderung murah dan tidak memakan biaya banyak.

Bersumber dari masalah yang sudah dijelaskan, penelitian ini dimaksudkan untuk merancang dan mengimplementasikan sistem Two-Factor Authentication (2FA) pada website Ar-Ridho Tours & Travel menggunakan OTP berbasis email, yang dilengkapi dengan fitur backup code untuk situasi darurat, trusted device untuk menyimpan perangkat terpercaya, serta logging aktivitas 2FA untuk monitoring dan audit. Dengan menerapkan sistem tersebut, tingkat keamanan akun akan meningkat secara signifikan, kepercayaan publik terhadap sektor layanan digital perusahaan menguat dan memberikan kontribusi praktis di sektor keagamaan.

2. METODE

2.1 Lokasi dan Waktu Pelaksanaan

Peneliti memilih lokasi di PT Nur Ridho Elsunury, yaitu perusahaan yang bergerak di bidang biro perjalanan wisata, khususnya ibadah umrah dan haji, dengan merek dagang Ar-Ridho Tours & Travel. Perusahaan ini berlokasi di Villa Pamulang Blok CH8 No. 9, RT. 08/017, Kelurahan Bakti Jaya, Kecamatan Setu, Kota Tangerang Selatan, Provinsi Banten, 15315. Pelaksanaan penelitian dimulai pada tanggal 10 Maret 2026 dan berakhir pada tanggal 17 Juni 2026.

2.2 Metode Pengumpulan Data

Untuk memperoleh data yang diperlukan dan juga akurat serta relevan, peneliti melakukan pengumpulan data dengan wawancara dan observasi.

Metode yang dilakukan pertama adalah wawancara. Wawancara dilakukan oleh peneliti secara langsung dengan pihak perusahaan. Wawancara berlangsung secara terstruktur dengan daftar pertanyaan yang sudah disiapkan sebelum wawancara dilakukan. Topik yang menjadi bahan pertanyaan meliputi sistem keamanan yang sedang berjalan, kendala yang sering dihadapi dalam pengelolaan akun pelanggan, harapan terhadap fitur keamanan tambahan seperti Two-Factor Authentication, serta kesiapan infrastruktur pendukung seperti alamat email aktif untuk seluruh pengguna. Dari wawancara, diketahui perusahaan membutuhkan sistem 2FA untuk meningkatkan keamanan data pribadi pelanggan.

Metode yang kedua adalah observasi. Observasi dilakukan secara langsung dengan mengamati cara pengguna login dan melakukan pemesanan diwebsite Ar-Riddho Tours & Travel. Dari observasi ini, peneliti mendapatkan bahwa proses login hanya menggunakan email dan password tanpa adanya verifikasi pengaman tambahan. Peneliti juga menemukan tidak adanya sistem untuk memulihkan akun darurat seperti backup code. Observasi ini menjadi pendorong dilakukannya implementasi sistem 2FA, seperti halaman verifikasi setelah login.

2.3 Metode Pengembangan sistem

Metode yang digunakan untuk mengembangkan sistem adalah prototyping. Metode ini digunakan karena bisa dikembangkan secara bertahap, dimulai dengan membuat model awal

JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 4, No. 3 Tahun 2026
ISSN 3025-0919 (media online)
Hal 726-741

(prototype) dari fitur-fitur utama, maka bisa disesuaikan dengan masukan atau saran. Pendekatan ini sesuai dengan sifat proyek yang berupa kerja praktek yang memerlukan fleksibilitas terhadap perubahan kebutuhan atau fitur.

Proses pengembangan metode prototype ini dilakukan dalam tiga tahap. Prototype I berfokus ke integrasi verifikasi OTP setelah berhasil login, tanpa penyimpanan statu perangkat. Prototype II ditambahkan fitur backup code dan pengaturan 2FA di profil akun pengguna. Lalu, Prototype III lebih berfokus ke penyempurnaan antarmuka pengguna dan uji keamanan dasar seperti pembatasan percobaan OTP yang salah dan masa berlaku kode.

Framework yang digunakan untuk membangun sistem adalah Laravel, bahasa pemrograman yang digunakan adalah PHP dan menggunakan basis data MYSQL. Laravel dipilih karena menyediakan fitur bawaan yang cukup membantu seperti autentikasi, pengiriman email, dan juga mendukung implementasi 2FA melalui paket Laravel Fortify. Pengembangan dilakukan dalam lingkungan lokal dengan XAMPP, menggunakan laptop yang memiliki spesifikasi perangkat keras prosesor Core i5, RAM 8 GB, dan SSD 256 GB. Sistem operasi yang digunakan adalah Windows 10.

2.4 Landasan Teori

2.4.1 Pengertian Two-Factor Authentication (2FA)

Two-Factor Authentication (2FA) atau autentikasi dua faktor adalah mekanisme keamanan yang memerlukan dua jenis bukti identitas berbeda sebelum pengguna diberikan akses ke suatu sistem. Dua faktor tersebut umumnya terdiri dari sesuatu yang diketahui pengguna (seperti kata sandi) dan sesuatu yang dimiliki pengguna (seperti kode OTP yang dikirim ke perangkat atau email). Dengan adanya lapisan kedua, risiko pengambilalihan akun akibat kebocoran kata sandi dapat diminimalkan secara signifikan, karena penyerang tetap membutuhkan faktor kedua yang hanya berada dalam kendali pemilik akun yang sah.

2.4.2 Pengertian One-Time Password (OTP)

One-Time Password (OTP) adalah kode autentikasi yang bersifat sementara dan hanya dapat digunakan satu kali dalam satu sesi. OTP biasanya berbentuk deretan angka (4 hingga 6 digit) yang dibangkitkan secara acak oleh sistem. Karakteristik utama OTP adalah masa berlakunya yang terbatas (umumnya 3–5 menit) dan ketidakmampuannya untuk diprediksi, sehingga menyulitkan pihak tidak berwenang untuk memanfaatkannya meskipun berhasil menyadap komunikasi. Dalam implementasi di website, OTP dapat dikirim melalui berbagai saluran seperti SMS, email, atau aplikasi autentikator.

2.4.3 Pengertian Keamanan Web

Keamanan web adalah serangkaian upaya perlindungan terhadap aplikasi berbasis internet dari berbagai ancaman siber, seperti peretasan akun, pencurian data, serangan brute force, phishing, dan man-in-the-middle. Keamanan web tidak hanya bergantung pada satu lapisan perlindungan, melainkan memerlukan pendekatan berlapis yang mencakup autentikasi yang kuat, enkripsi data (HTTPS), perlindungan terhadap serangan injeksi kode, serta pengelolaan sesi pengguna yang aman. Penerapan 2FA merupakan salah satu pilar penting dalam membangun keamanan web yang tangguh.

2.4.4 Pengertian Implementasi Sistem

Implementasi sistem adalah tahap penerapan hasil rancangan sistem ke dalam bentuk yang nyata dan dapat dioperasikan. Tahap ini mencakup penulisan kode program, pengujian unit, integrasi antarmuka, serta penyiapan lingkungan produksi. Dalam konteks pengembangan perangkat lunak, implementasi juga melibatkan instalasi perangkat keras dan perangkat lunak pendukung, migrasi data, serta pelatihan pengguna. Keberhasilan implementasi sangat bergantung pada sejauh mana sistem yang dibangun sesuai dengan kebutuhan yang telah didefinisikan pada tahap analisis dan perancangan.

JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 4, No. 3 Tahun 2026
ISSN 3025-0919 (media online)
Hal 726-741

2.4.5 Pengertian Framework Laravel

Laravel adalah sebuah kerangka kerja (framework) open source untuk bahasa pemrograman PHP yang mengadopsi pola arsitektur Model-View-Controller (MVC). Laravel menyederhanakan pengembangan aplikasi web dengan menyediakan fitur-fitur bawaan seperti routing, autentikasi, sesi, caching, dan pengiriman email. Untuk mendukung keamanan berlapis, Laravel menyediakan paket Laravel Fortify dan Laravel JetStream yang sudah mendukung implementasi Two-Factor Authentication secara native, termasuk pembangkitan OTP, pengiriman melalui email, serta pengelolaan kode cadangan (backup code). Kemudahan integrasi dengan basis data MySQL dan dokumentasi yang lengkap menjadikan Laravel sebagai pilihan utama dalam pengembangan sistem 2FA pada penelitian ini.

2.4.6 Pengertian Backup Code

Backup code adalah serangkaian kode cadangan yang diberikan oleh sistem kepada pengguna saat pertama kali mengaktifkan fitur 2FA. Kode-kode ini dapat digunakan masing-masing satu kali sebagai alternatif verifikasi ketika pengguna tidak dapat mengakses faktor kedua (misalnya tidak menerima OTP karena masalah jaringan atau lupa kata sandi email). Backup code biasanya disediakan dalam jumlah 8 hingga 10 kode, dan setelah digunakan akan dinonaktifkan secara otomatis. Untuk menjaga keamanan, backup code disimpan dalam bentuk hash di dalam basis data, sehingga meskipun terjadi kebocoran data, kode cadangan tidak dapat langsung dimanfaatkan oleh pihak tidak berwenang.

2.5 Penelitian Terkait

Dalam penelitian yang dilakukan, peneliti mencari beberapa penelitian sebelumnya yang sudah dilakukan dan relevan dengan topik 2FA dengan sistem OTP. Kegiatan ini bermaksudkan untuk memahami metode serta pendekatan dan hasil 2FA di berbagai sistem informasi, yang akan digunakan sebagai acuan untuk implementasi sistem tersebut pada website Ar-Ridho Tours & Travels

Penelitian oleh Adha et al. (2026) berjudul "Rancang Bangun Sistem Informasi Persuratan Berbasis Web dengan Keamanan Two-Factor Authentication di Politeknik Negeri Bengkalis" mengimplementasikan 2FA menggunakan algoritma TOTP melalui Google Authenticator pada sistem persuratan. Sistem dikembangkan dengan framework Laravel dan database MYSQL. Penelitian ini relevan karena menggunakan framework Laravel dan basis data MYSQL dapat digunakan diintegrasikan ke sistem berbasis web.

Selain itu, ada juga artikel dari Laravel Daily (2025) berjudul "Two-Factor Authentication in Laravel: Packages and Options" memberikan penjelasan bahwa Laravel memberikan tiga opsi resmi untuk mengimplementasikan 2FA, yaitu official starter kit, laravel fortify dan laravel jetstream. Artikel ini menjadi panduan untuk menggunakan framework Laravel dalam pengembangan sistem 2FA, terutama dalam OTP, pengirim email dan backup code.

Penelitian oleh Anwar & Sriani (2024) berjudul "Implementasi Algoritma OTP dan HMAC untuk Two-Factor Authentication Sistem Login Relawan Pemilu" menggunakan OTP 6 digit yang berganti setiap 15 detik. Hasil penelitian ini membuktikan penggunaan sistem OTP dan HMAC dapat meningkatkan keamanan sistem secara signifikan, terutama terhadap serangan brute force

Penelitian oleh Kurniawan (2025) berjudul "Penerapan Two-Factor Authentication dengan Menggunakan Metode Time-Based One-Time Password Real-Time Database" mengimplementasikan 2FA ke sistem e-menu di Kafe Legi menggunakan Laravel dan Google Authenticator. Hasil penelitian menunjukkan sistem TOTP dapat menghasilkan kode unik yang terbatas dalam jangka waktu tertentu, sistem juga berhasil autentikasi dengan akurasi 100% di kode yang benar.

3. ANALISA DAN PEMBAHASAN

3.1 Usecase Diagram

Usecase diagram adalah diagram yang menggambarkan hubungan interaksi apa yang dimiliki antara tiap sistem dan aktor. Usecase berguna memperlihatkan proses aktivitas sistem secara urut,

JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 4, No. 3 Tahun 2026
ISSN 3025-0919 (media online)
Hal 726-741

menggambarkan proses bisnis, menampilkan urutan aktivitas proses dan jembatan antara pembuat dengan konsumen untuk mendeskripsikan sebuah sistem.

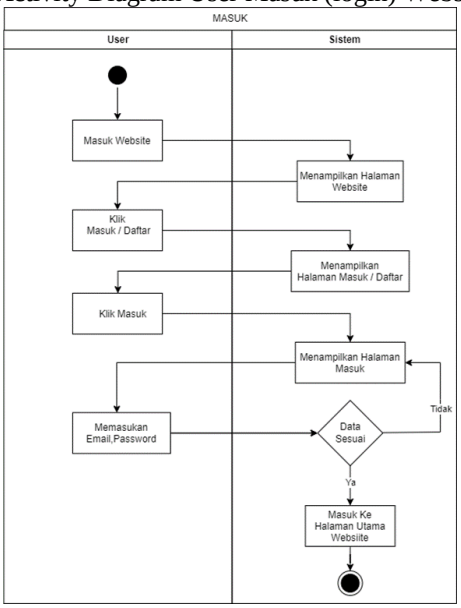
Gambar 1. Use Case Diagram

a. User
User adalah pengguna sistem yang akan melakukan pemesanan umrah secara online. Akses yang dimiliki oleh user diantaranya, yaitu registrasi akun, login ke dalam sistem, melakukan verifikasi OTP (sebagai bagian dari 2FA), menggunakan backup code untuk login alternatif, mengaktifkan fitur trusted device, melihat daftar paket umrah, melihat detail paket, melakukan booking paket, serta logout.

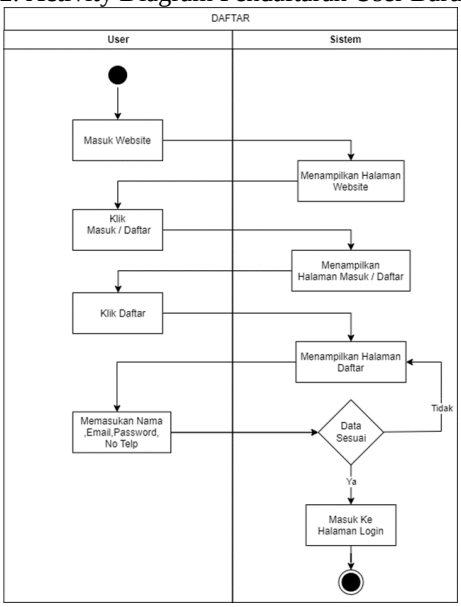
b. Admin
Admin adalah pihak yang mengurus website dan mengelola data pendaftaran. Admin memiliki hak akses yang mencakup login ke sistem, mengelola data paket umrah (menambah, mengedit, menghapus paket), melihat seluruh data booking yang dilakukan oleh user, melakukan verifikasi atau penolakan terhadap pendaftaran user, serta logout. Admin juga harus memiliki fitur yang menggunakan 2FA(OTP, trusted device, backup code) karena admin tetap harus login ke sistem.

3.2 Activity Diagram

1. Activity Diagram User Masuk (login) Website

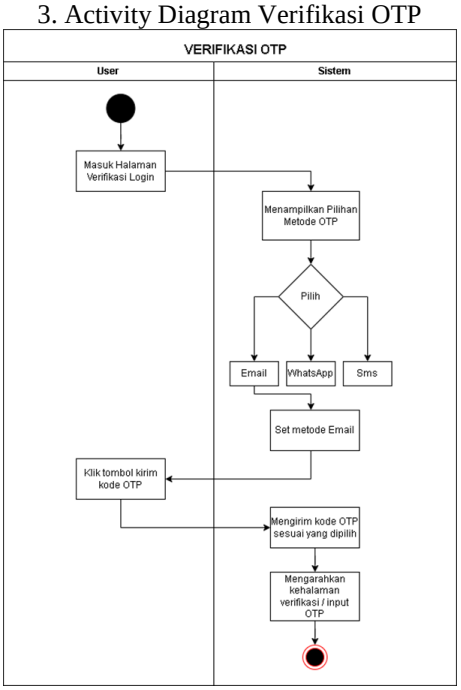


2. Activity Diagram Pendaftaran User Baru

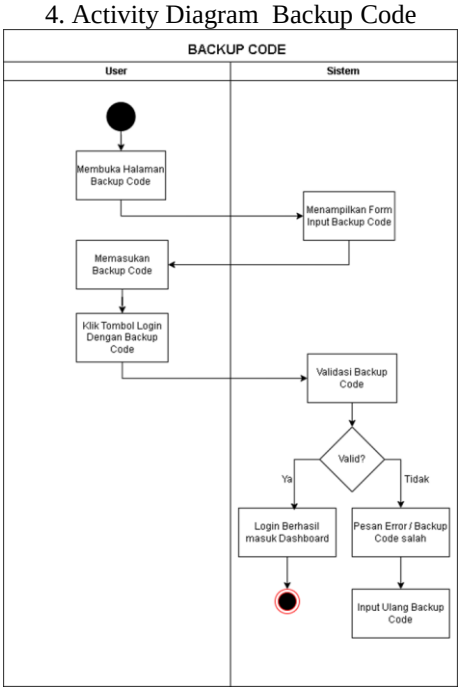


JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 4, No. 3 Tahun 2026
ISSN 3025-0919 (media online)
Hal 726-741

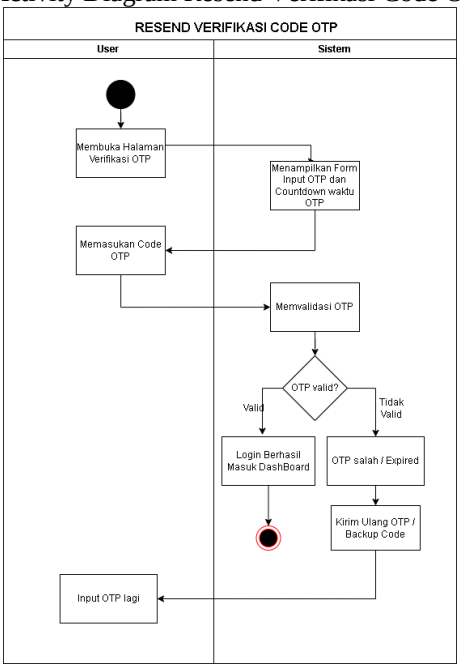
3. Activity Diagram Verifikasi OTP



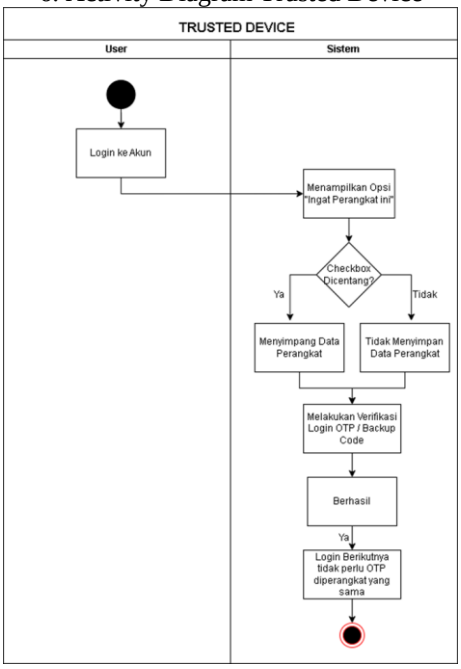
4. Activity Diagram Backup Code



5. Activity Diagram Resend Verifikasi Code OTP

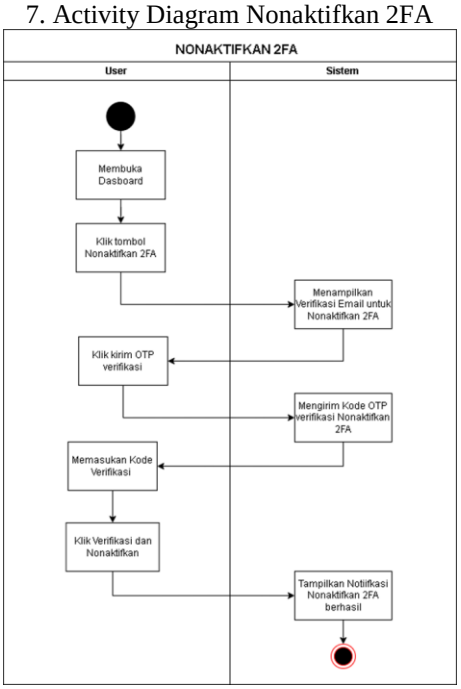


6. Activity Diagram Trusted Device

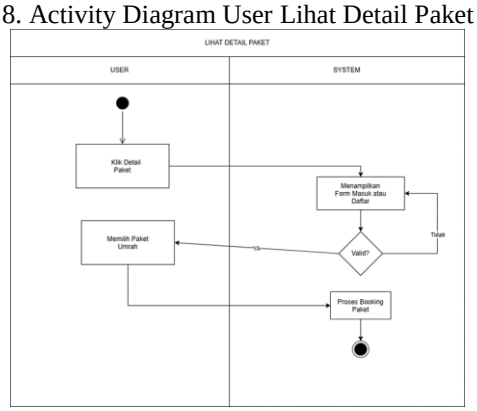


JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 4, No. 3 Tahun 2026
ISSN 3025-0919 (media online)
Hal 726-741

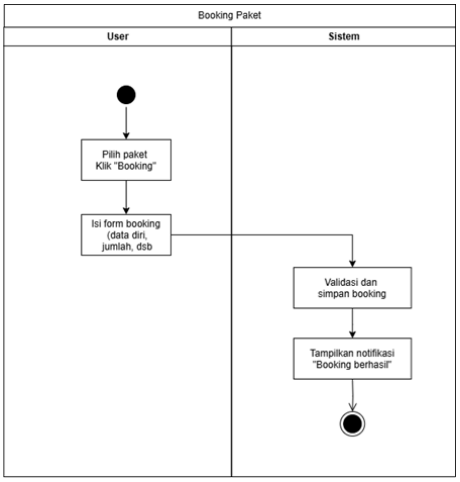
7. Activity Diagram Nonaktifkan 2FA



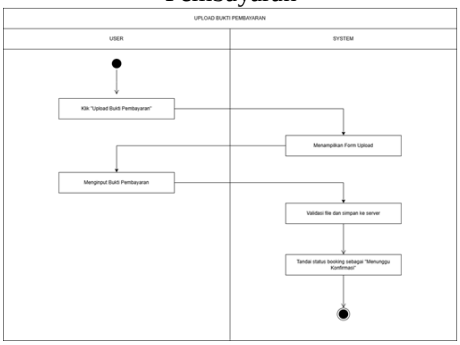
8. Activity Diagram User Lihat Detail Paket



9. Activity Diagram User Melakukan Booking Paket

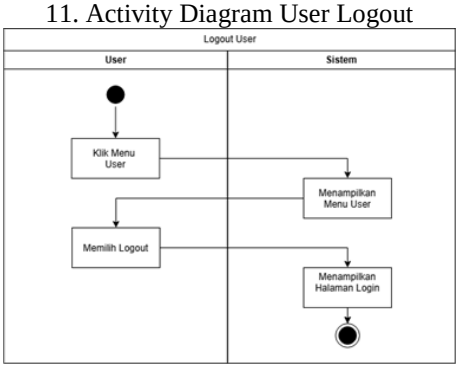


10. Activity Diagram User Upload Bukti Pembayaran

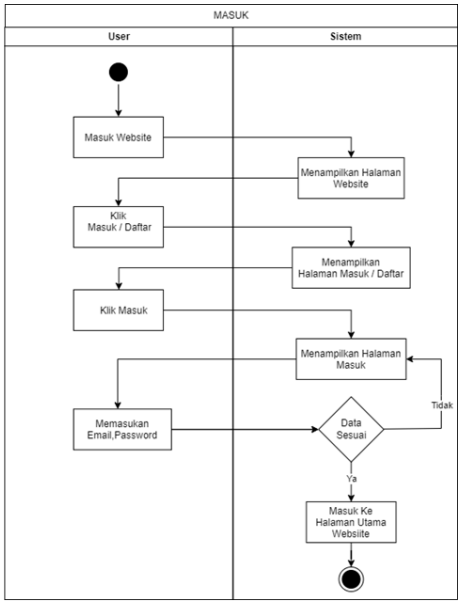


JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 4, No. 3 Tahun 2026
ISSN 3025-0919 (media online)
Hal 726-741

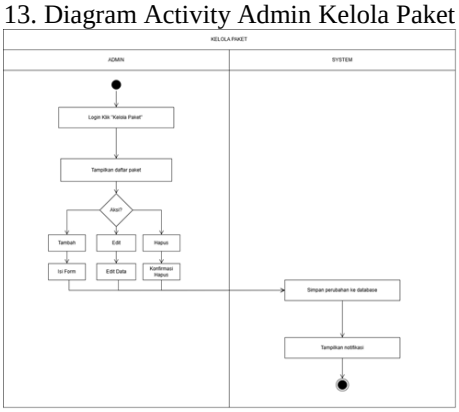
11. Activity Diagram User Logout



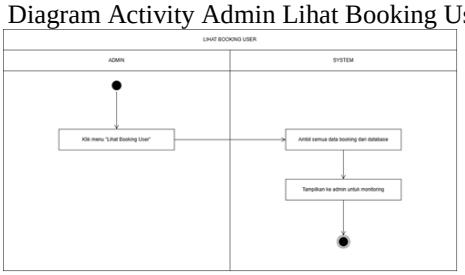
12. Diagram Activity Admin Masuk (login) Website



13. Diagram Activity Admin Kelola Paket

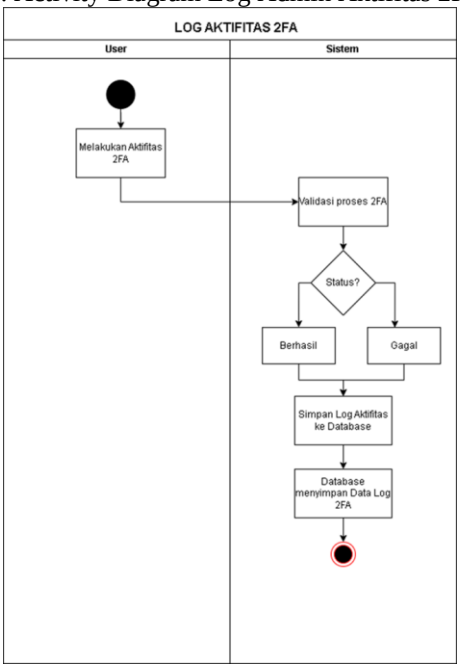


14. Diagram Activity Admin Lihat Booking User

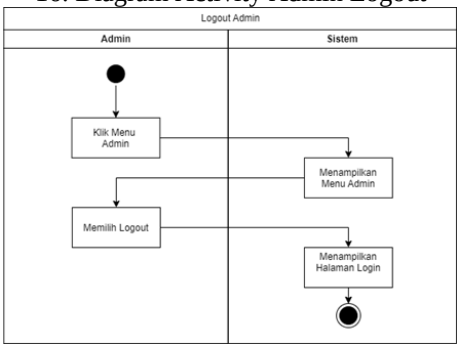


JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 4, No. 3 Tahun 2026
ISSN 3025-0919 (media online)
Hal 726-741

15. Activity Diagram Log Admin Aktifitas 2FA

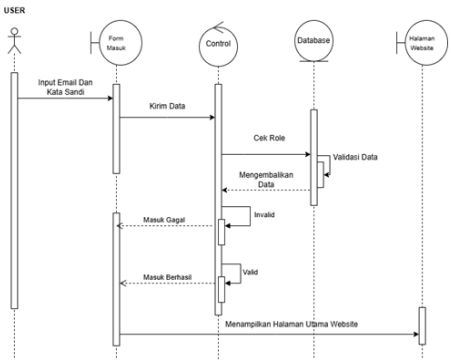


16. Diagram Activity Admin Logout

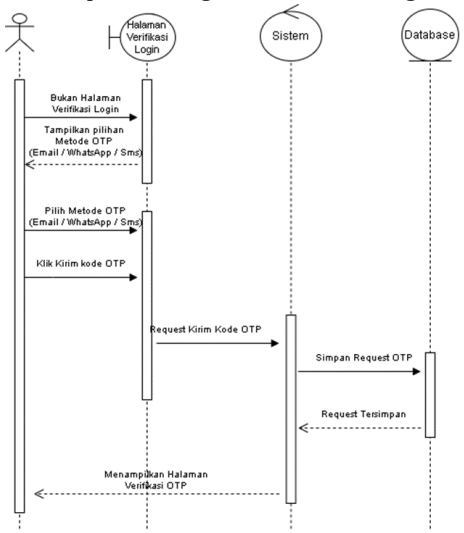


3.3 Sequence Diagram

1. Sequence Diagram User Masuk (login) website

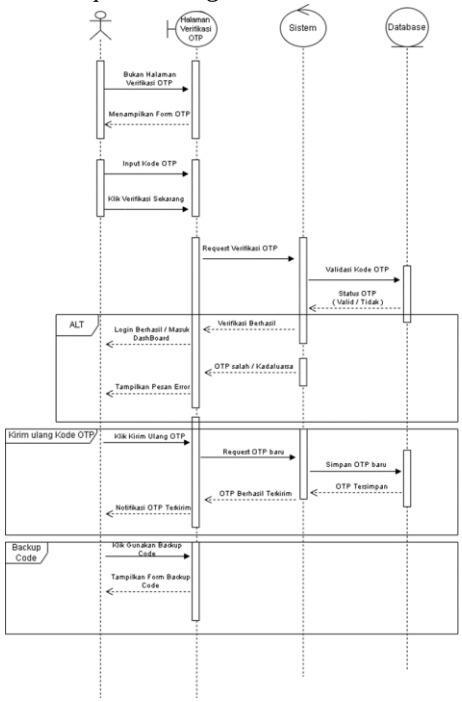


2. Sequence Diagram Verifikasi Login

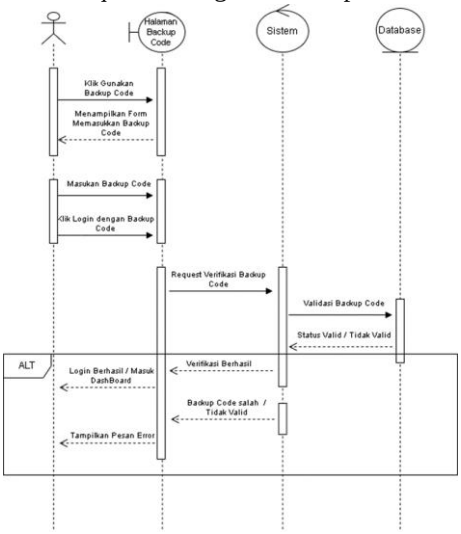


JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 4, No. 3 Tahun 2026
ISSN 3025-0919 (media online)
Hal 726-741

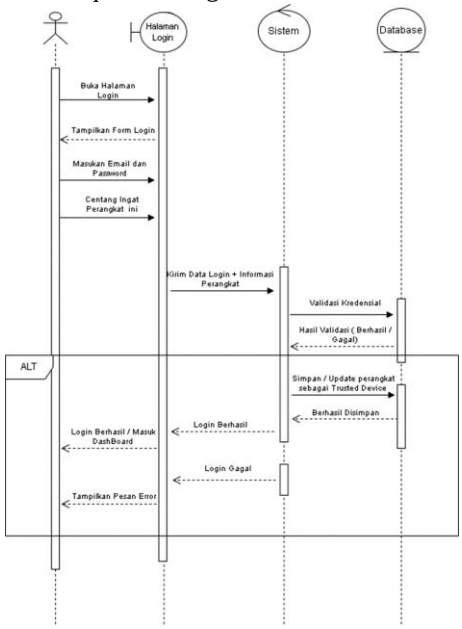
3. Sequence Diagram Verifikasi OTP



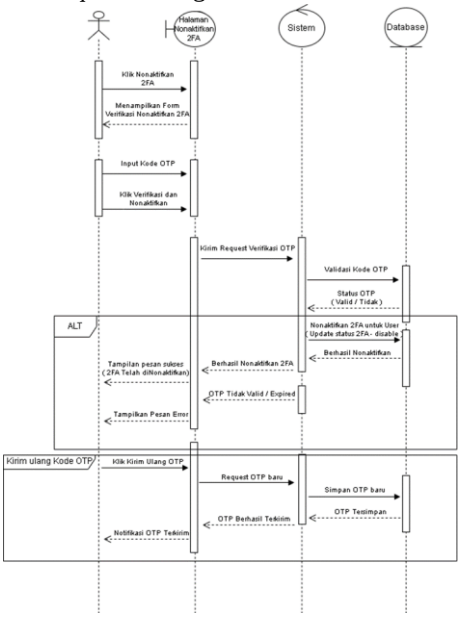
4. Sequence Diagram Backup Code



5. Sequence Diagram Trusted Device

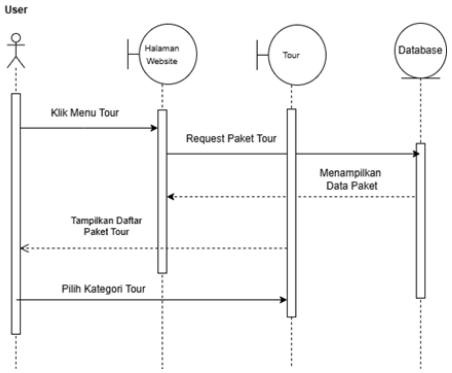


6. Sequence Diagram Nonaktifkan 2FA

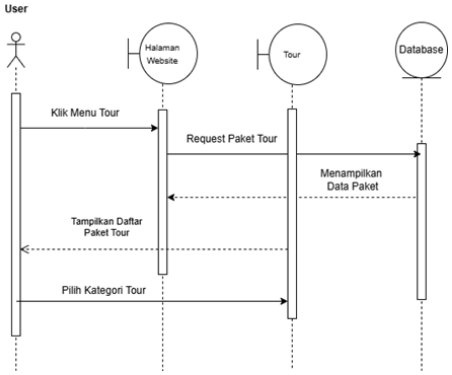


JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 4, No. 3 Tahun 2026
ISSN 3025-0919 (media online)
Hal 726-741

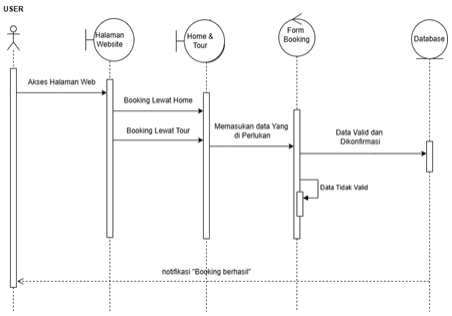
7. Sequence Diagram User Lihat Paket



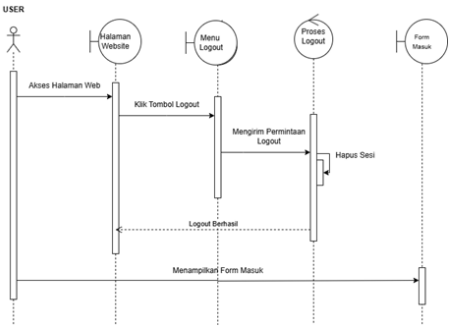
8. Sequence Diagram User Lihat Detail Paket



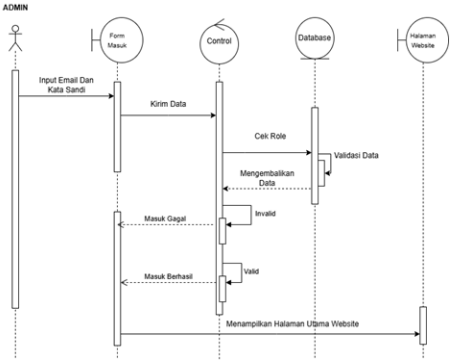
9. Sequence Diagram User Booking Paket



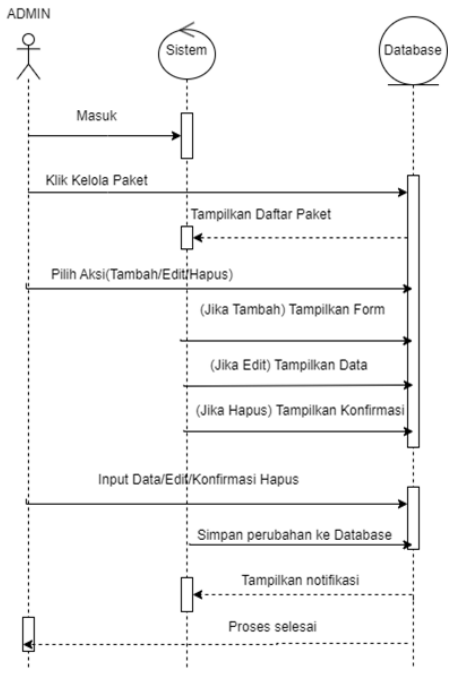
10. Sequence Diagram User Logout



11. Sequence Diagram Admin Masuk (Login)

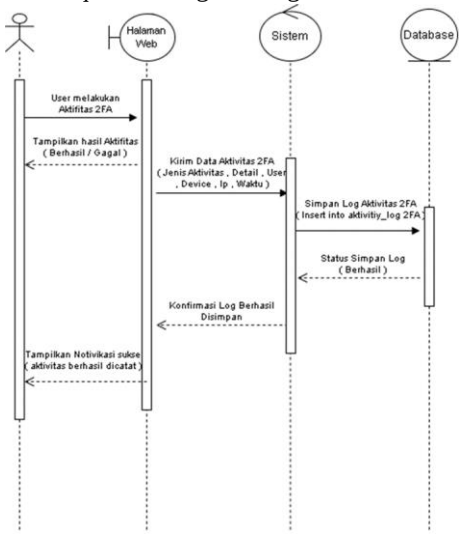


12. Sequence Diagram Admin Kelola Paket

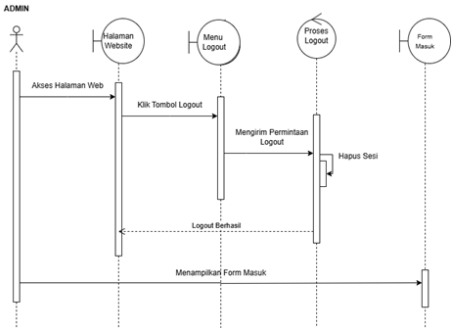


JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 4, No. 3 Tahun 2026
ISSN 3025-0919 (media online)
Hal 726-741

13. Sequence Diagram Log Aktifitas 2FA

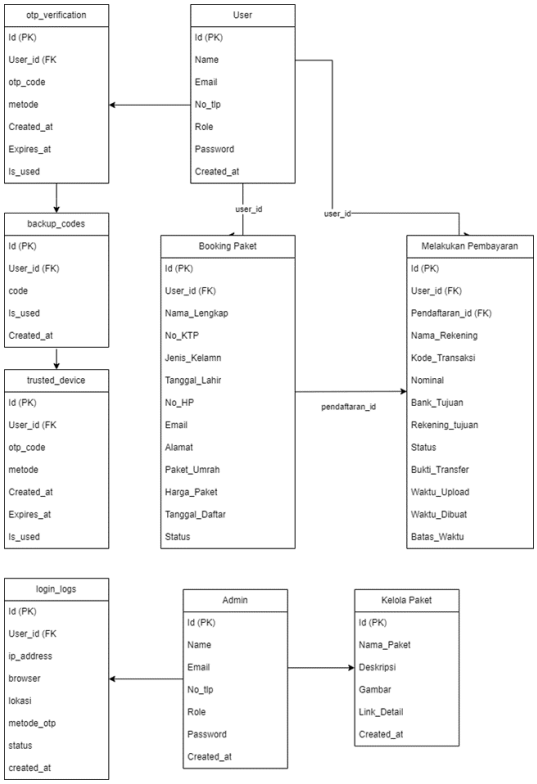


14. Sequence Diagram Admin Logout



3.4 Class Diagram

Class diagram adalah diagram yang menunjukkan struktur dan hubungan antar komponen sistem secara jelas dan sistematis. Class diagram dapat membantu pengembang memahami bagaimana entitas-entitas dalam sistem saling berinteraksi melalui hubungan antar kelas, atribut, dan metode.



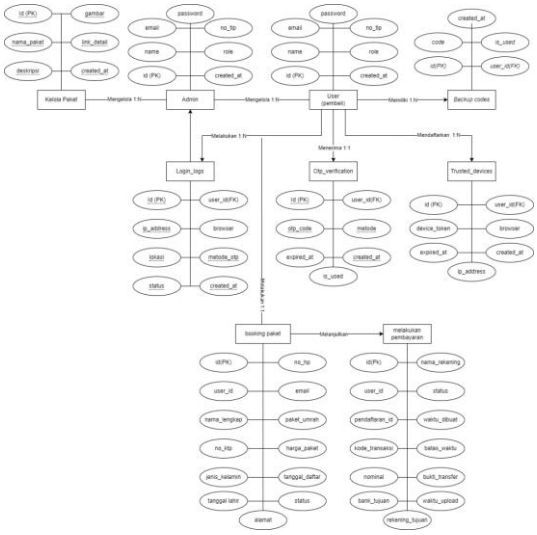
Class diagram diatas memiliki empat kelas utama, yaitu Users menyimpan data akun pengguna (user_id, nama, email, password, role). OtpCodes menyimpan kode OTP sementara (id, user_id, code, expires_at, used_at). BackupCodes menyimpan kode cadangan untuk situasi darurat (id, user_id, code, used_at). LoginAttempts mencatat riwayat percobaan login (id, user_id, ip_address, success, attempted_at). Relasi antara Users dengan ketiga kelas lainnya bersifat one-to-

JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 4, No. 3 Tahun 2026
ISSN 3025-0919 (media online)
Hal 726-741

many, berarti satu pengguna bisa memiliki banyak kode OTP, backup code dan banyak catatan percobaan login.

3.5 Entity Relationship Diagram

Entity Relationship Diagram (ERD) adalah suatu model diagram yang digunakan untuk menggambarkan struktur data secara konseptual beserta hubungan antar data dalam suatu sistem informasi. ERD menggambarkan entitas-entitas (yang mewakili tabel dalam database), atribut-atribut (yang mewakili kolom atau field pada setiap tabel), serta relasi atau hubungan antar entitas yang dilengkapi dengan notasi kardinalitas seperti satu ke satu (one-to-one), satu ke banyak (one-to-many), atau banyak ke banyak (many-to-many).



Berdasarkan Gambar X, ERD sistem Two-Factor Authentication pada website Ar-Ridho Tours & Travel dirancang dengan empat entitas utama, yaitu Users, OtpCodes, BackupCodes, dan LoginAttempts. Entitas Users berperan sebagai entitas induk yang menyimpan data akun pengguna (user_id, nama, email, password, role, serta status 2FA). Entitas OtpCodes menyimpan kode OTP sementara yang dikirimkan ke email pengguna, dengan atribut seperti id, user_id, code, expires_at, dan used_at. Entitas BackupCodes menyimpan kode cadangan untuk situasi darurat ketika pengguna tidak dapat mengakses email, dengan atribut id, user_id, code, dan used_at. Sementara itu, entitas LoginAttempts mencatat riwayat percobaan login (id, user_id, ip_address, success, attempted_at) yang berguna untuk memantau potensi serangan brute force.

Relasi antara Users dengan ketiga entitas lainnya (OtpCodes, BackupCodes, LoginAttempts) bersifat one-to-many (satu ke banyak), yang berarti satu pengguna dapat memiliki banyak kode OTP (setiap kali login berbeda), banyak backup code, dan banyak catatan percobaan login. Desain ERD ini secara keseluruhan dirancang untuk mencerminkan alur verifikasi dua faktor mulai dari pembangkitan OTP, validasi, penggunaan backup code, hingga pencatatan log aktivitas secara terstruktur dan efisien.

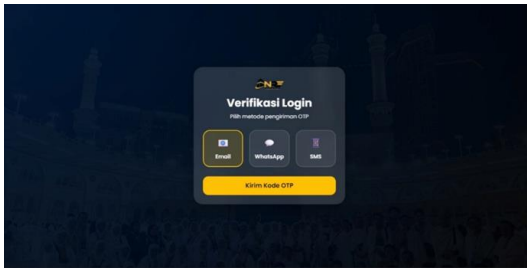
3.6 Analisa dan Fitur Utama

a. Halaman Login

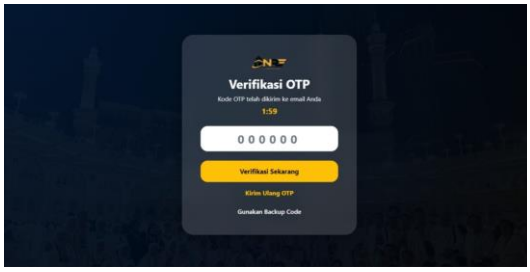
b. Halaman Daftar

JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 4, No. 3 Tahun 2026
ISSN 3025-0919 (media online)
Hal 726-741

c. Halaman Pengiriman Kode Multi OTP

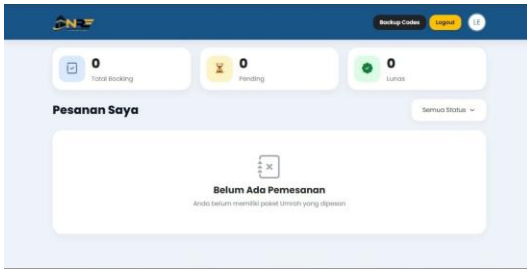


d. Halaman Verifikasi OTP



e. Halaman Generasi Kode OTP

f. Halaman Dashboard



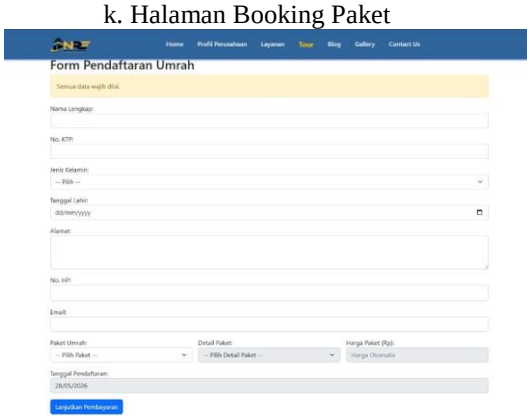
g. Halaman Kode Cadangan

h. Login Menggunakan kode Backup

i. Halaman Trusted Device

j. Halaman Detail Paket

k. Halaman Booking Paket



JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 4, No. 3 Tahun 2026
ISSN 3025-0919 (media online)
Hal 726-741

3.7 Hasil dan Analisa

Berdasarkan tabel hasil pengujian, sistem Two-Factor Authentication yang dibangun berfungsi dengan baik sesuai kebutuhan PT Nur Ridho Elsunury. Sistem mampu mengirimkan OTP 6 digit ke email pengguna, memvalidasi kode dengan benar, menolak kode yang salah atau kedaluwarsa, serta menyediakan mekanisme pengiriman ulang. Fitur backup code memberikan alternatif verifikasi yang aman karena setiap kode hanya dapat digunakan sekali dan disimpan dalam bentuk hash. Fitur trusted device berhasil mengurangi gesekan pengguna tanpa mengorbankan keamanan, karena perangkat terpercaya tetap memerlukan verifikasi ulang setelah 30 hari.

Selain itu, sistem memiliki keunggulan pada fitur log aktivitas 2FA yang memungkinkan admin memantau percobaan login mencurigakan, seperti login gagal berulang dari IP yang sama. Hal ini mendeteksi potensi serangan brute force. Namun, pengujian hanya terbatas pada fungsionalitas (black box), belum mencakup uji keamanan tingkat lanjut seperti SQL injection atau XSS. Dengan demikian, sistem 2FA ini telah layak digunakan untuk meningkatkan keamanan akun pada website Ar-Ridho Tours & Travel.

Tabel 1. Pengujian Blackbox dari Sudut Pandang User

No.	Fitur yang Diuji	Hasil yang Diharapkan	Hasil Pengujian	Status
1	User memasukkan email dan password valid (2FA aktif)	Sistem menampilkan halaman verifikasi OTP	Halaman verifikasi OTP muncul	Valid
2	User memasukkan OTP yang sesuai dengan yang dikirim ke email	Sistem mengizinkan akses ke dashboard	Halaman OTP ditampilkan	Valid
3	User memasukkan OTP yang salah	Sistem menolak akses dan menampilkan pesan "Kode OTP salah"	Pesan error muncul, tetap di halaman verifikasi	Valid
4	User mengklik tombol "Kirim Ulang Kode"	Sistem mengirimkan OTP baru ke email pengguna	Email baru diterima	Valid
5	User memilih opsi "Login dengan Backup Code" dan memasukkan backup code yang benar	Sistem mengizinkan akses ke dashboard dan menandai backup code sebagai sudah terpakai	Berhasil login, backup code tidak dapat dipakai lagi	Valid
6	User memasukkan backup code yang sudah pernah digunakan	Sistem menolak akses dan menampilkan pesan "Backup code tidak valid"	Pesan error muncul	Valid
7	User login dari perangkat baru, centang "Ingat perangkat ini" saat verifikasi OTP	Sistem tidak meminta OTP lagi dari perangkat yang sama selama 30 hari	Login berikutnya tanpa OTP dari perangkat yang sama	Valid
8	User menonaktifkan 2FA melalui halaman pengaturan akun	Sistem menonaktifkan 2FA, login hanya memerlukan email dan password	2FA nonaktif, login tanpa halaman OTP	Valid

Tabel 2. Pengujian Blackbox dari Sudut Pandang Admin

No	Skenario Pengujian	Hasil yang Diharapkan	Hasil Pengujian	Status
1	Admin memasukkan email dan password valid (2FA aktif)	Sistem menampilkan halaman verifikasi OTP	Halaman verifikasi OTP muncul	Valid
2	Admin memasukkan OTP yang sesuai dengan yang dikirim ke email	Sistem mengizinkan akses ke dashboard admin	Berhasil login ke dashboard admin	Valid

JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 4, No. 3 Tahun 2026
ISSN 3025-0919 (media online)
Hal 726-741

3	Admin memasukkan OTP yang salah	Sistem menolak akses dan menampilkan pesan "Kode OTP salah"	Pesan error muncul, tetap di halaman verifikasi	Valid
4	Admin memilih opsi "Login dengan Backup Code" dan memasukkan backup code valid	Sistem mengizinkan akses ke dashboard admin	Berhasil login, backup code tidak dapat dipakai lagi	Valid
5	Admin membuka halaman log aktivitas 2FA	Sistem menampilkan daftar percobaan login (waktu, IP, status sukses/gagal) untuk semua pengguna	Log aktivitas ditampilkan sesuai data	Valid
6	Admin menonaktifkan 2FA pada akunnya sendiri melalui halaman pengaturan	Sistem menonaktifkan 2FA untuk akun admin tersebut	Admin login berikutnya tanpa OTP	Valid

4. KESIMPULAN

Berdasarkan hasil perancangan, implementasi, dan pengujian sistem Two-Factor Authentication (2FA) pada website Ar-Ridho Tours & Travel, dapat disimpulkan bahwa sistem 2FA berbasis OTP email berhasil dibangun dan diintegrasikan ke dalam proses login. Seluruh fitur yang dikembangkan, meliputi verifikasi OTP setelah login berhasil, pengiriman ulang kode OTP (resend), kode cadangan (backup code) untuk situasi darurat, perangkat terpercaya (trusted device) untuk mengurangi pengulangan verifikasi, serta nonaktifkan 2FA, berfungsi sesuai yang diharapkan sesuai dengan berdasarkan pengujian blackbox. Metode perkembangan prototyping terbukti dapat dengan baik digunakan untuk proses pengembangan sistem ini karena memungkinkan pengembangan secara bertahap dan evaluasi. Sistem 2FA meningkatkan keamanan akun pengguna karena jika password pengguna diketahui oleh pihak yang tidak bertanggung jawab, pihak tersebut tidak dapat melewati sistem OTP. Dengan implementasi sistem ini, keamanan pelanggan PT Nur Ridho Elsunury dapat meningkat dan kepercayaan publik terhadap layanan digital Ar-Ridho Tours & Travels menjadi lebih baik.

REFERENCES

Firmansyah, E., & Utami, P. (2025). Penerapan Laravel Fortify untuk Two-Factor Authentication pada Sistem Pemesanan Paket Umrah. *Jurnal Teknik Informatika Universitas Pamulang*, 3(1), 55–63.

Hidayat, T., & Nugroho, A. (2024). Analisis Keamanan Fitur Trusted Device pada Sistem Two-Factor Authentication Website. *Prosiding Seminar Nasional Keamanan Siber*, 45–52.

Maulana, F., & Wibowo, S. (2025). Pengelolaan Backup Code pada Two-Factor Authentication: Studi Kasus Penyimpanan Hash dan Regenerasi Kode. *Jurnal Ilmiah Informatika*, 8(1), 33–41.

Nugraha, Y., & Lestari, M. (2024). Perbandingan Metode Pengiriman OTP (Email, SMS, WhatsApp) untuk Two-Factor Authentication pada Aplikasi Berbasis Web. *Jurnal Komputer dan Aplikasi*, 12(3), 99–108.

Pratama, R., & Sari, D. (2025). Implementasi Two-Factor Authentication Berbasis One-Time Password pada Aplikasi E-Commerce Travel Menggunakan Framework Laravel. *Jurnal Teknologi Informasi dan Komputer*, 11(2), 112–120.

Rachmawati, L., & Kurniawan, B. (2024). Evaluasi Ketahanan Two-Factor Authentication terhadap Serangan Brute Force dan Phishing pada Layanan Online Travel. *Jurnal Keamanan Sistem Informasi*, 6(2), 78–86.