Jurnal Minfo Polgan
Volume 14, Nomor 2, Desember 2025
DOI : https://doi.org/10.33395/jmp.v14i2.15724
e-ISSN : 2797-3298
p-ISSN : 2089-9424

Penggunaan OTP (One Time Password) Sebagai Lapisan Keamanan Tambahan dalam Aplikasi AY Pulsa

[1]Dhea Nurandani, [2]Sahat Parulian Sitorus, [3]Aisyah Rahmadiyah Manoppo, [4]Doni Adrian, [5]Muhammad Irfan Ayuda
[1,2,3,4,5] Fakultas Sains Dan Teknologi, Prodi Teknologi Informasi, Universitas Labuhanbatu, Indonesia
[1]deanurandhani@gmail.com, [2]sahatparuliansitorus4@gmail.com,
[3]aisyahrahmadiyah5@gmail.com, [4]doniadrian520@gmail.com, [5]mhdirfan842@gmail.com

Submit : 30 Nov 2025 | **Diterima** : 18 Des 2025 | **Terbit** : 22 Des 2025

ABSTRAK

Keamanan data dan autentikasi pengguna merupakan aspek penting dalam pengembangan aplikasi digital, terutama aplikasi yang berkaitan dengan transaksi online. AY Pulsa sebagai aplikasi penyedia layanan pembelian produk digital berupaya meningkatkan perlindungan akun pengguna melalui penerapan fitur One-Time Password (OTP) sebagai lapisan keamanan tambahan. Penelitian ini bertujuan untuk menganalisis peran, manfaat, serta dampak penggunaan OTP dalam meningkatkan keamanan login pada aplikasi AY Pulsa. Metode penelitian yang digunakan adalah deskriptif kualitatif dengan sumber data primer melalui wawancara langsung bersama pemilik aplikasi. Hasil wawancara menunjukkan bahwa sebelum penerapan OTP, sistem autentikasi hanya menggunakan username, email, dan password, yang secara umum sudah fungsional namun tetap memiliki potensi risiko penyalahgunaan, seperti password ditebak, dibocorkan, atau digunakan di banyak platform oleh pengguna. Meskipun pemilik aplikasi menyatakan bahwa belum pernah terjadi kasus pembajakan akun, kekhawatiran terkait keamanan tetap menjadi pertimbangan penting. Penerapan OTP dipilih karena sifatnya yang mudah diimplementasikan, tidak memerlukan biaya tambahan, serta memiliki tingkat keamanan yang tinggi. Dalam proses login, sistem mengirimkan kode OTP melalui WhatsApp atau email yang hanya berlaku selama 20 menit. Hal ini memastikan bahwa setiap upaya login benar-benar dilakukan oleh pemilik akun. Hasil penelitian menunjukkan bahwa setelah OTP diterapkan, pengguna memberikan respon positif dan merasa lebih aman ketika mengakses aplikasi. Rating aplikasi juga mengalami peningkatan. Secara keseluruhan, OTP terbukti mampu meningkatkan standar keamanan AY Pulsa sekalipun tidak ada riwayat kasus penyalahgunaan sebelumnya. Penerapan fitur ini juga memberikan kepercayaan lebih kepada pengguna bahwa akun mereka terlindungi dengan baik.

Kata Kunci: *OTP,* keamanan aplikasi, autentikasi, sistem informasi, digital protection**.**

PENDAHULUAN

Perkembangan teknologi informasi yang pesat mendorong meningkatnya penggunaan komputer dan internet, namun juga meningkatkan risiko terjadinya kejahatan siber (cybercrime). Untuk menangani kejahatan tersebut diperlukan forensik digital sebagai metode ilmiah dalam mengidentifikasi, mengumpulkan, menganalisis, dan menyajikan bukti digital yang valid dan dapat dipertanggungjawabkan secara hukum. Forensik digital berperan penting dalam menjaga keaslian bukti serta mendukung proses penegakan hukum sesuai dengan ketentuan Undang-Undang Informasi dan Transaksi Elektronik. Teknologi digital telah mendorong meningkatnya penggunaan aplikasi transaksi online, termasuk aplikasi pembelian produk digital. Seiring tingginya aktivitas digital, ancaman keamanan seperti pembajakan akun, pencurian password, dan penyalahgunaan identitas semakin meningkat. Oleh karena itu, aplikasi digital memerlukan sistem autentikasi yang kuat untuk melindungi data pengguna. AY Pulsa adalah aplikasi layanan digital yang menyediakan berbagai produk seperti pulsa, paket data, dan layanan digital lainnya. Untuk meningkatkan

Jurnal Minfo Polgan
Volume 14, Nomor 2, Desember 2025 e-ISSN : 2797-3298
DOI : https://doi.org/10.33395/jmp.v14i2.15724 p-ISSN : 2089-9424

keamanan akses, aplikasi ini menerapkan One-Time Password (OTP) sebagai lapisan autentikasi tambahan (Parulian Sitorus et al., 2023). OTP merupakan kode verifikasi yang dikirimkan kepada pengguna saat login untuk memastikan bahwa yang mengakses akun benar-benar pemiliknya. Penelitian ini menganalisis bagaimana OTP diterapkan di AY Pulsa, dampaknya terhadap keamanan aplikasi, serta persepsi pengguna setelah implementasinya.

STUDI LITERATUR

Keamanan Sistem Informasi

Keamanan sistem informasi adalah upaya untuk melindungi data, perangkat, dan sistem dari ancaman seperti pencurian, kerusakan, modifikasi, serta akses ilegal. Menurut Stallings (2017), keamanan sistem informasi mencakup tiga aspek utama, yaitu confidentiality, integrity, dan availability. Dalam konteks aplikasi digital seperti AY Pulsa, aspek keamanan ini menjadi penting karena aplikasi menangani transaksi dan data pribadi pengguna.

Selain itu, penelitian terbaru menunjukkan bahwa aplikasi yang memiliki proses login dan transaksi digital membutuhkan mekanisme keamanan berlapis untuk mengurangi ancaman seperti cracking, phishing, dan serangan otomatis (Mayorga & Yoo, 2025). Temuan tersebut menguatkan urgensi penerapan autentikasi tambahan seperti OTP pada aplikasi transaksi digital.

Autentikasi Pengguna

Autentikasi adalah proses verifikasi identitas pengguna sebelum diberikan akses ke sistem. Autentikasi tradisional menggunakan kombinasi username dan password. Namun penelitian menunjukkan pengguna sering menggunakan password yang lemah, mudah ditebak, atau digunakan ulang di banyak platform (Florêncio & Herley, 2007). Hal ini meningkatkan risiko pencurian akun.Hasil penelitian Fitriyansyah & Hazri (2020) menunjukkan bahwa sistem login berbasis password statis sangat rentan terhadap serangan brute force dan credential stuffing. Ketika autentikasi ditambahkan OTP sebagai faktor kedua, tingkat keberhasilan serangan menurun secara signifikan, membuktikan kelemahan metode password tunggal.

Kelemahan Sistem Password

Studi perilaku password (Das et al., 2014) mengungkap bahwa sebagian besar pengguna membuat password sederhana seperti tanggal lahir atau pola berulang. Password juga rentan terhadap serangan phishing, brute force, keylogger, dan pencurian data di server (Bonneau et al., 2012).Penelitian terbaru dalam sektor perbankan mengungkapkan bahwa lebih dari 30% pelanggaran keamanan berawal dari kebocoran password yang kemudian dipakai untuk mengakses OTP API atau sistem terkait (Author, 2023). Hal ini menegaskan bahwa password saja tidak cukup dalam melindungi akun, sehingga perlu tambahan autentikasi berbasis perangkat atau token unik.

One Time Password (OTP)

OTP adalah kode keamanan yang hanya berlaku satu kali dan memiliki masa berlaku singkat. Menurut Meng (2020), OTP termasuk ke dalam autentikasi dua faktor (2FA) karena selain password, sistem memverifikasi identitas pengguna melalui perangkat yang dimiliki seperti nomor telepon atau email.

Penelitian terbaru menunjukkan efektivitas OTP dalam mengurangi risiko akses ilegal. Menurut Wibawa, Suryanto & Ningsih (2024), OTP berbasis TOTP lebih sulit dipalsukan karena dihasilkan oleh algoritma waktu yang hanya valid dalam periode sangat singkat. Penelitian itu menegaskan bahwa OTP mampu mencegah penyalahgunaan akun meskipun password pengguna bocor.

Keunggulan OTP:

1. Sulit ditebak karena dihasilkan secara acak atau berbasis waktu.
2. Masa berlaku pendek sehingga tidak mudah disalahgunakan.
3. Melindungi akun ketika password dicuri (Fitriyansyah & Hazri, 2020).

Autentikasi Dua Faktor (2FA)

Two-Factor Authentication (2FA) menggunakan dua jenis bukti, yaitu:

1. Something you know (password), dan

Jurnal Minfo Polgan
Volume 14, Nomor 2, Desember 2025 e-ISSN : 2797-3298
DOI : https://doi.org/10.33395/jmp.v14i2.15724 p-ISSN : 2089-9424

2. Something you have (OTP atau token).

Menurut Aloul (2010), sistem dua faktor meningkatkan keamanan hingga 90% lebih baik dibanding penggunaan password tunggal. Hal ini diperkuat oleh Mayorga & Yoo (2025) yang menyatakan bahwa 2FA dengan OTP (baik HOTP maupun TOTP) sangat efektif mengurangi serangan unauthorized login pada aplikasi mobile dan web.

Implementasi OTP pada aplikasi AY Pulsa termasuk dalam kategori 2FA berbasis perangkat pengguna, sehingga memberikan perlindungan terhadap risiko pembajakan akun maupun penyalahgunaan akses.

Keamanan Aplikasi Mobile

Aplikasi mobile memiliki tantangan keamanan seperti kebocoran data, penyalahgunaan sesi, dan pencurian akun. Bhatia (2019) menjelaskan bahwa aplikasi yang menangani transaksi digital harus menerapkan lapisan keamanan tambahan seperti OTP, PIN, dan enkripsi data.

Rahayuda & Santiari (2023) menambahkan bahwa aplikasi yang memanfaatkan OTP Firebase perlu diuji menggunakan metode SAST dan IAST untuk memastikan tidak ada kerentanan pada implementasi OTP, seperti intercept SMS atau bypass verifikasi. Dengan demikian, penggunaan OTP pada AY Pulsa sebagai autentikasi login dan PIN 4 digit untuk transaksi internal sudah sejalan dengan praktik keamanan aplikasi modern.

Penelitian Terkait OTP

Berbagai penelitian menunjukkan bahwa OTP efektif menurunkan risiko pembajakan akun, terutama pada aplikasi finansial dan e-commerce. Kaspersky (2018) menyatakan bahwa OTP menjadi solusi keamanan populer karena efisien dan mudah digunakan.

Penelitian lebih baru oleh Wibawa, Suryanto & Ningsih (2024) menemukan bahwa TOTP mampu meningkatkan keamanan sistem secara signifikan karena tidak bergantung pada jaringan telekomunikasi seperti SMS. Sementara penelitian di sektor perbankan (Author, 2023) menegaskan pentingnya implementasi OTP yang aman, karena kesalahan pada API OTP dapat membuka peluang serangan.

METODE PENELITIAN

Metode Penelitian

Penelitian ini menggunakan pendekatan deskriptif kualitatif, yaitu suatu metode yang bertujuan mendeskripsikan, menggambarkan, dan menjelaskan fenomena penggunaan OTP (One Time Password) sebagai lapisan keamanan tambahan pada aplikasi AY Pulsa berdasarkan fakta yang diperoleh dari lapangan. Pendekatan ini dipilih karena penelitian berfokus pada pemahaman mendalam terkait proses keamanan aplikasi, pengalaman pengguna, dan alasan pemilik dalam menerapkan OTP, bukan pada pengukuran numerik.

1. Lokasi dan Subjek Penelitian

Lokasi penelitian adalah aplikasi AY Pulsa, sebuah platform transaksi digital yang telah mengintegrasikan OTP untuk proses login dan verifikasi transaksi. Subjek penelitian terdiri dari owner aplikasi yang memiliki pemahaman menyeluruh mengenai alur keamanan, integrasi OTP, hingga riwayat pembaruan sistem yang dilakukan.Pemilihan owner sebagai sumber data primer relevan dengan penelitian sebelumnya mengenai implementasi OTP menggunakan WhatsApp API, yang juga menjadikan stakeholder sistem sebagai narasumber utama karena mereka memahami aspek teknis dan operasional sistem secara langsung (Hayuningtyas, 2025).

2. Jenis dan Sumber Data

Penelitian menggunakan data primer dan data sekunder:

a. Data Primer

Data primer diperoleh melalui wawancara, observasi sistem, serta pengalaman langsung peneliti saat menggunakan aplikasi AY Pulsa. Informasi mendalam dikumpulkan mengenai alur OTP, kecepatan pengiriman, masa berlaku kode, tingkat keberhasilan verifikasi, hingga mekanisme pengendalian keamanan yang diterapkan.Penelitian terdahulu menunjukkan bahwa observasi langsung terhadap proses OTP sangat penting untuk mengidentifikasi potensi delay, kerentanan SMS gateway, dan pola perilaku pengguna (Bartłomiejczyk & El Fray, 2024). Hal ini memperkuat

Jurnal Minfo Polgan
Volume 14, Nomor 2, Desember 2025 e-ISSN : 2797-3298
DOI : https://doi.org/10.33395/jmp.v14i2.15724 p-ISSN : 2089-9424

penggunaan data primer dalam penelitian ini.

b. Data Sekunder

Data sekunder dalam penelitian ini mencakup jurnal ilmiah dan artikel penelitian yang relevan mengenai keamanan sistem autentikasi, penggunaan One-Time Password (OTP), serta tantangan dan efektivitasnya dalam konteks autentikasi dua faktor (2FA). Literatur yang ditelaah memberikan dasar teoretis kuat untuk mendukung pembahasan dan analisis implementasi OTP pada aplikasi AY Pulsa. beberapa penelitian menunjukkan bahwa aplikasi yang menerapkan autentikasi dua faktor dengan OTP dapat memperkuat keamanan login karena kode yang dihasilkan bersifat unik, acak, dan hanya berlaku dalam periode singkat, sehingga meminimalkan peluang akses oleh pihak yang tidak berwenang (*Mayorga & Yoo, 2025*). Studi komprehensif ini menyoroti bahwa OTP dapat meningkatkan proteksi terhadap akses tidak sah, terutama ketika password statis saja tidak lagi cukup untuk menghadapi risiko serangan siber modern (*Mayorga & Yoo, 2025*). Penelitian lain membahas pengalaman pengguna terhadap keamanan OTP yang secara langsung memengaruhi kepercayaan pengguna terhadap sistem autentikasi. Studi ini menunjukkan bahwa pengalaman yang baik terhadap pengiriman dan penggunaan OTP berkorelasi positif dengan peningkatan kepercayaan pengguna terhadap keamanan sistem, yang penting dalam konteks aplikasi digital yang intensif transaksi seperti AY Pulsa (*Wiranto & Salis, 2025*). meski demikian, bukan berarti OTP bebas risiko. Analisis kerentanan terhadap implementasi API OTP SMS pada sektor perbankan menunjukkan adanya celah pada mekanisme pertukaran SMS OTP yang berpotensi dieksploitasi oleh penyerang. Temuan ini menekankan perlunya evaluasi teknis mendalam terhadap implementasi OTP pada sistem nyata untuk memastikan keamanan operasional (*App-based detection…, 2024*). selain itu, penelitian implementasi OTP melalui jalur WhatsApp menunjukkan bahwa penggunaan alternatif distribusi kode seperti WhatsApp API dapat memberikan respons pengiriman yang lebih cepat dan stabil dibandingkan SMS tradisional, sehingga meningkatkan efektivitas sistem secara keseluruhan (*Implementasi One Time Password…, 2025*). dengan demikian, data sekunder ini memperkuat dasar teoretis bahwa OTP, sebagai bagian dari autentikasi dua faktor, merupakan mekanisme yang efektif dan umum digunakan dalam sistem autentikasi modern, namun tetap perlu dikaji secara komprehensif dari aspek teknis dan pengalaman pengguna agar implementasinya optimal.

3. Teknik Pengumpulan Data

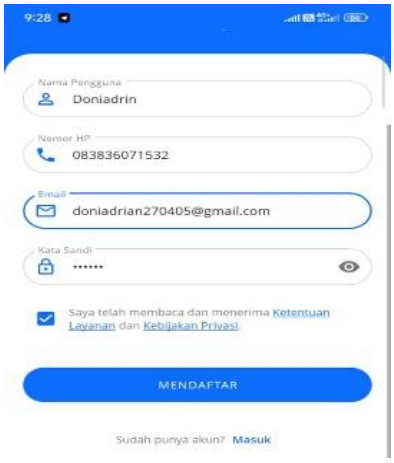
Teknik pengumpulan data pada penelitian ini disusun untuk memperoleh pemahaman mendalam mengenai implementasi OTP sebagai lapisan keamanan tambahan pada aplikasi AY Pulsa. Penelitian menggunakan pendekatan kualitatif sehingga teknik pengumpulan data difokuskan pada wawancara mendalam, observasi sistem, dan dokumentasi. Ketiga teknik ini diterapkan secara terpadu untuk menghasilkan data yang holistik sebagaimana dianjurkan dalam penelitian kualitatif berbasis studi kasus (Creswell, 2021; Yin, 2018)

a. Proses Login

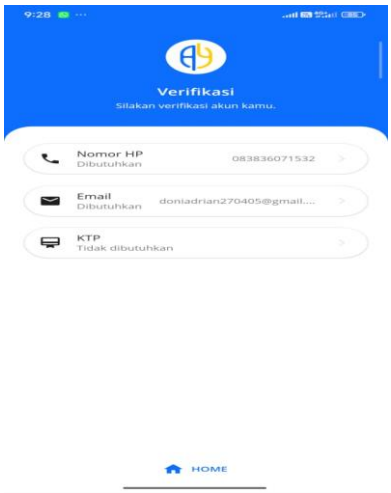
Observasi sistem dilakukan dengan menguji secara langsung mekanisme autentikasi menggunakan OTP pada aplikasi AY Pulsa. Observasi diarahkan untuk memahami keandalan alur login, metode pengiriman OTP melalui SMS dan email, serta cara sistem memvalidasi kode OTP. Observasi ini penting untuk mengetahui performa aktual implementasi OTP, karena kerentanan umumnya muncul pada pelaksanaan, bukan pada konsep OTP itu sendiri (Bartłomiejczyk & El Fray, 2024).

Peneliti mencatat kecepatan pengiriman kode, stabilitas server, masa berlaku OTP, serta perbedaan pengalaman pengguna pada SMS dan email OTP. Aspek waktu pengiriman menjadi perhatian utama, mengingat penelitian menyatakan bahwa delay OTP dapat menurunkan tingkat kepercayaan pengguna terhadap aplikasi (Hayuningtyas, 2025b). Observasi ini memberikan pemahaman faktual yang mendukung data wawancara.

Jurnal Minfo Polgan
Volume 14, Nomor 2, Desember 2025 e-ISSN : 2797-3298
DOI : https://doi.org/10.33395/jmp.v14i2.15724 p-ISSN : 2089-9424



Gambar. 1 Login



Gambar. 2 Opsi Menerima OTP

b. Menerima Kode OTP

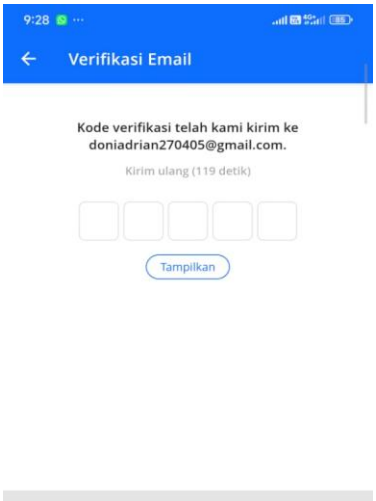
Peneliti melakukan pengamatan langsung terhadap proses penerimaan kode OTP untuk menilai kecepatan pengiriman, keandalan jaringan, serta kualitas implementasi autentikasi pada aplikasi AY Pulsa. Observasi dilakukan pada dua jalur pengiriman, yaitu melalui WhatsApp dan email, karena kedua media ini memiliki karakteristik teknis yang berbeda. Kecepatan penerimaan kode menjadi indikator penting dalam menilai efektivitas OTP, mengingat delay atau keterlambatan dapat mengurangi tingkat keamanan dan menurunkan kenyamanan pengguna (Hayuningtyas, 2025b).

Selain waktu pengiriman, peneliti juga mencatat format OTP yang diterima, termasuk panjang kode, komponen acak, dan pesan notifikasi pendukung. Hal ini penting karena struktur pesan OTP sering dikaitkan dengan tingkat kerentanan terhadap serangan phishing dan manipulasi jaringan, terutama pada OTP berbasis SMS maupun jaringan publik (Bartłomiejczyk & El Fray, 2024). Analisis validitas kode juga dilakukan, seperti durasi masa berlaku OTP, batas maksimal percobaan login, serta apakah sistem menerapkan pengamanan tambahan berupa mekanisme lock-out ketika pengguna salah memasukkan kode secara berulang.

Aspek kemudahan penggunaan turut diamati karena pengalaman pengguna (user experience) memiliki peran penting dalam efektivitas sistem autentikasi. Penelitian sebelumnya menunjukkan bahwa implementasi OTP yang cepat, konsisten, dan mudah dipahami pengguna akan meningkatkan persepsi keamanan dan kepercayaan terhadap aplikasi digital (Wiranto & Salis, 2025c). Hasil observasi ini menjadi dasar evaluasi apakah mekanisme OTP yang diterapkan pada AY Pulsa telah memenuhi standar keamanan dan kenyamanan sesuai praktik terbaik autentikasi digital.

Jurnal Minfo Polgan
Volume 14, Nomor 2, Desember 2025 e-ISSN : 2797-3298
DOI : https://doi.org/10.33395/jmp.v14i2.15724 p-ISSN : 2089-9424

digital systems
Gambar. 3 Verfikkasi Kode WhatsApp

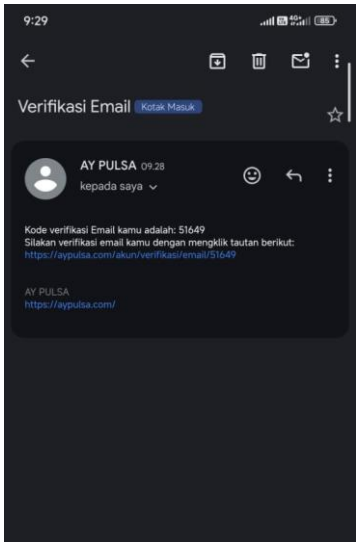


Gambar. 4 Verfikasi Kode Melalui Email

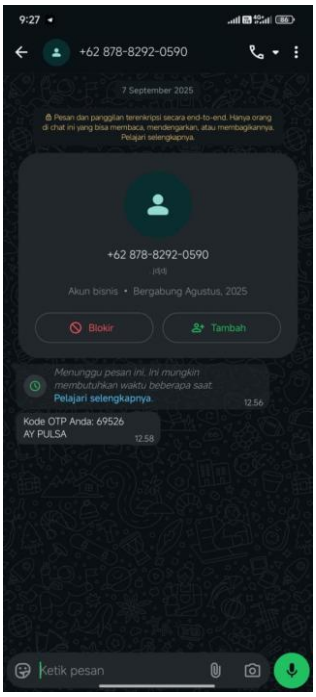
c. Menerima Kode OTP

Teknik dokumentasi digunakan untuk mengumpulkan berbagai bukti fisik maupun digital yang berkaitan dengan implementasi OTP pada aplikasi AY Pulsa. Bukti yang dihimpun meliputi screenshot proses pengiriman kode OTP melalui WhatsApp maupun email, rekaman tampilan antarmuka saat pengguna melakukan login, flowchart alur autentikasi, catatan teknis dari owner aplikasi, serta arsip pembaruan sistem keamanan. Seluruh dokumen tersebut berfungsi untuk memastikan bahwa proses yang diamati benar-benar terjadi, valid, dan sesuai dengan kondisi operasional aplikasi yang sesungguhnya. penggunaan dokumentasi sebagai metode penguatan data lazim digunakan dalam penelitian autentikasi digital karena dapat memberikan verifikasi visual terhadap proses teknis yang tidak selalu dapat dijelaskan secara verbal oleh narasumber. Dalam penelitian mengenai pengiriman OTP melalui WhatsApp API, misalnya, dokumentasi berupa tangkapan layar dan arsip catatan teknis terbukti penting dalam mengonfirmasi konsistensi sistem dan mendukung temuan dari observasi serta wawancara (Hayuningtyas, 2025b). selain itu, dokumentasi juga membantu memvalidasi alur teknis autentikasi dengan membandingkan proses aktual dengan standar keamanan yang direkomendasikan dalam literatur, khususnya ketika menilai kerentanan OTP terhadap manipulasi jaringan atau kesalahan implementasi (Bartłomiejczyk & El Fray, 2024). Dengan demikian, teknik dokumentasi tidak hanya berperan sebagai pelengkap data, tetapi juga sebagai bukti empiris yang memperkuat tingkat kredibilitas hasil penelitian.

Jurnal Minfo Polgan
Volume 14, Nomor 2, Desember 2025 e-ISSN : 2797-3298
DOI : https://doi.org/10.33395/jmp.v14i2.15724 p-ISSN : 2089-9424



Gambar. 5 Kode Diterima melalui Email



Gambar 6 Kode Diterima Melalui WhatsApp

4. Teknik Analisis Data

Analisis data dalam penelitian ini menggunakan model interaktif Miles & Huberman yang terdiri atas tiga tahap utama: reduksi data, penyajian data, dan penarikan kesimpulan. Model ini digunakan secara berulang sehingga peneliti dapat memahami data secara mendalam dan menemukan pola yang berkaitan dengan efektivitas implementasi OTP dalam meningkatkan keamanan aplikasi AY Pulsa. Pendekatan ini banyak digunakan dalam penelitian keamanan digital untuk mengidentifikasi pola risiko dan respons pengguna terhadap mekanisme autentikasi (Wiranto & Salis, 2025).

a. Reduksi

pada tahap reduksi data, seluruh informasi dari wawancara, observasi sistem, dan dokumentasi diseleksi serta dikelompokkan berdasarkan tema penelitian. Reduksi meliputi pemetaan kondisi keamanan aplikasi sebelum penerapan OTP, proses implementasi OTP, kendala teknis seperti keterlambatan pengiriman kode, serta dampak OTP terhadap penurunan risiko akses ilegal. Proses penyederhanaan data ini memusatkan analisis pada aspek-aspek yang benar-benar relevan dengan tujuan penelitian. penelitian terdahulu menegaskan pentingnya reduksi data dalam studi autentikasi

Jurnal Minfo Polgan
Volume 14, Nomor 2, Desember 2025 e-ISSN : 2797-3298
DOI : https://doi.org/10.33395/jmp.v14i2.15724 p-ISSN : 2089-9424

digital, karena penelitian OTP sering menghasilkan banyak informasi teknis yang harus disaring agar dapat dianalisis secara sistematis (Bartłomiejczyk & El Fray, 2024).

b. Penyajian Data

tahap selanjutnya adalah penyajian data yang dilakukan melalui narasi deskriptif, tabel temuan, serta diagram alur proses OTP untuk memberikan gambaran visual mengenai mekanisme autentikasi di aplikasi. Penyajian data membantu peneliti melihat hubungan antara masalah keamanan, intervensi melalui OTP, dan perubahan yang terjadi setelah fitur tersebut diterapkan. pendekatan ini sesuai dengan praktik penelitian modern yang menampilkan alur autentikasi digital melalui diagram guna mempermudah interpretasi (Hayuningtyas, 2025b).

c. Penarikan Kesimpulan

Penarikan kesimpulan dilakukan setelah proses verifikasi hasil analisis melalui triangulasi dan pembandingan dengan teori. Berdasarkan temuan di lapangan, penerapan OTP mampu meningkatkan keamanan akun pengguna, mengurangi risiko pembobolan, dan memastikan bahwa hanya pengguna yang memiliki akses ke nomor terdaftar yang dapat masuk ke aplikasi. Hal ini sejalan dengan penelitian yang menunjukkan bahwa OTP meningkatkan keamanan karena bersifat dinamis, acak, dan memiliki masa berlaku terbatas (Mayorga & Yoo, 2025).

5. Validitas Data

Untuk menjamin keakuratan dan keandalan temuan penelitian, digunakan dua teknik utama, yaitu triangulasi dan member check. Kedua teknik ini lazim digunakan dalam penelitian mengenai implementasi autentikasi digital agar data yang diproduksi benar-benar menggambarkan kondisi sistem yang diteliti (Wiranto & Salis, 2025).Poin-Poin Validitas Data

a. Triangulasi
1. Membandingkan dan mengonfirmasi hasil wawancara, observasi sistem, dan dokumentasi teknis.
2. Memastikan konsistensi informasi dari berbagai sumber data.
3. Mengurangi potensi bias peneliti dan meningkatkan keandalan temuan.

b. Member Check
1. Mengirimkan kembali transkrip wawancara kepada owner untuk diperiksa kebenarannya.
2. Mengonfirmasi interpretasi peneliti terkait proses OTP, kendala, dan evaluasi keamanan.
3. Memastikan bahwa hasil analisis sesuai dengan kondisi dan pandangan narasumber.

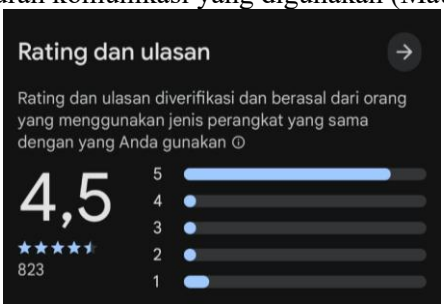
HASIL DAN PEMBAHASAN

Hasil Penelitian

Berdasarkan hasil wawancara dengan pemilik aplikasi AY Pulsa, diperoleh informasi mengenai sejarah perkembangan aplikasi, tujuan pengembangan, sistem keamanan awal, serta implementasi OTP sebagai fitur autentikasi tambahan. Aplikasi AY Pulsa mulai digunakan sejak Agustus 2025 dan dirancang untuk mempermudah transaksi produk digital seperti pulsa dan paket data. Sebelum penerapan OTP, proses login hanya menggunakan kombinasi nama pengguna, nomor HP, email, dan kata sandi. Meskipun belum ditemukan kasus penyalahgunaan akun, pemilik aplikasi memiliki kekhawatiran terhadap potensi risiko akses ilegal apabila pengguna menggunakan kata sandi yang lemah atau sama dengan akun lain, sebuah risiko yang banyak ditemukan pada sistem autentikasi berbasis password saja (Maulana et al., 2025). Pemilik aplikasi kemudian memutuskan untuk menambahkan OTP sebagai lapisan keamanan tambahan karena dinilai mudah diterapkan, tidak memerlukan biaya besar, dan memiliki tingkat keamanan yang tinggi. Setiap proses login akan menghasilkan OTP yang dikirim melalui WhatsApp atau email pengguna, dengan masa berlaku sekitar 20 menit. Penggunaan OTP sebagai faktor autentikasi tambahan ini sejalan dengan temuan penelitian bahwa OTP meningkatkan keamanan secara signifikan dibandingkan penggunaan kata sandi statis saja (Mayorga & Yoo, 2025). Hasil observasi terhadap penggunaan OTP menunjukkan bahwa fitur ini mampu meningkatkan keamanan akses tanpa menimbulkan keluhan dari pengguna. Pengguna memberikan respons positif dan memberikan penilaian baik di Play Store. Temuan ini sejalan dengan penelitian yang menunjukkan bahwa OTP melalui saluran pesan instan memiliki tingkat keberhasilan pengiriman yang tinggi dan

Jurnal Minfo Polgan
Volume 14, Nomor 2, Desember 2025 e-ISSN : 2797-3298
DOI : https://doi.org/10.33395/jmp.v14i2.15724 p-ISSN : 2089-9424

mudah digunakan oleh pengguna awam (Hayuningtyas, 2025). Secara umum, pengguna menilai proses login dengan OTP aman, cepat, dan tidak menyulitkan, sehingga meningkatkan tingkat kepercayaan pengguna terhadap aplikasi. Hal ini konsisten dengan temuan yang menunjukkan bahwa pengalaman pengguna berperan penting dalam penerimaan mekanisme autentikasi berbasis OTP (Wiranto & Salis, 2025). Namun demikian, penelitian juga menemukan beberapa kendala teknis, yaitu OTP tidak terkirim apabila nomor pengguna salah, tidak aktif, atau mengalami gangguan jaringan. Masalah ini juga tercatat dalam literatur bahwa keberhasilan OTP sangat bergantung pada keandalan saluran komunikasi yang digunakan (Maulana et al., 2025).



Gambar.7 Rating & Ulasan Pengguna

Gambar.8 Ulasan Kepuasan Pengguna

PEMBAHASAN

Penerapan OTP pada AY Pulsa memberikan penguatan signifikan terhadap keamanan aplikasi. Meskipun tidak terdapat kasus pembajakan akun sebelum OTP diterapkan, langkah preventif ini sejalan dengan prinsip keamanan modern yang menekankan mitigasi risiko sebelum insiden terjadi (Maulana et al., 2025). Berdasarkan teori autentikasi digital, OTP merupakan bentuk two-step verification yang dapat menurunkan kemungkinan akses ilegal meskipun kata sandi pengguna berhasil ditebak atau bocor (Mayorga & Yoo, 2025).

Dalam konteks AY Pulsa, OTP berfungsi sebagai lapisan kedua setelah password sehingga mempersulit upaya penyalahgunaan akun. Pengiriman OTP melalui WhatsApp dan email memberikan fleksibilitas jalur autentikasi serta meningkatkan keandalan pengiriman. Temuan lapangan ini konsisten dengan hasil penelitian yang menunjukkan bahwa WhatsApp memiliki tingkat keberhasilan pengiriman OTP yang lebih tinggi dibandingkan SMS tradisional (Hayuningtyas, 2025).

Hasil wawancara menunjukkan bahwa penerapan OTP tidak hanya meningkatkan

Jurnal Minfo Polgan
Volume 14, Nomor 2, Desember 2025 e-ISSN : 2797-3298
DOI : https://doi.org/10.33395/jmp.v14i2.15724 p-ISSN : 2089-9424

keamanan teknis tetapi juga meningkatkan kepuasan dan kepercayaan pengguna. Peningkatan rating dan ulasan di Play Store mengindikasikan bahwa persepsi keamanan berpengaruh langsung terhadap kualitas pengalaman pengguna. Hal ini sesuai dengan temuan sebelumnya bahwa persepsi keamanan merupakan faktor penting dalam adopsi teknologi autentikasi (Wiranto & Salis, 2025). Selain OTP, AY Pulsa juga menambahkan PIN 4 digit untuk keamanan transaksi internal. Pendekatan ini sejalan dengan praktik standar pada aplikasi keuangan yang menggabungkan multi-layered security untuk melindungi autentikasi dan transaksi secara simultan (Maulana et al., 2025). Sinergi antara OTP dan PIN menjadikan sistem keamanan aplikasi lebih komprehensif.

KESIMPULAN

Penelitian ini menunjukkan bahwa penerapan OTP pada aplikasi AY Pulsa memberikan dampak positif terhadap keamanan aplikasi dan kepercayaan pengguna. Walaupun sebelum OTP tidak terdapat kasus pembajakan akun, kekhawatiran mengenai potensi penyalahgunaan mendorong developer menambahkan autentikasi tambahan. OTP terbukti efektif karena mudah diterapkan, tidak memerlukan biaya, dan meningkatkan keamanan login secara signifikan (Mayorga & Yoo, 2025).

Respons pengguna terhadap OTP sangat positif, ditunjukkan melalui peningkatan rating dan ulasan aplikasi. Selain mengurangi risiko penyalahgunaan akun bagi pengguna yang menggunakan kata sandi lemah, fitur ini juga memperkuat keamanan sistem secara keseluruhan. Penambahan fitur PIN 4 digit mendukung keamanan transaksi internal sehingga sesuai dengan standar keamanan aplikasi digital modern.

Ke depan, meskipun autentikasi biometrik belum direncanakan, penguatan keamanan internal dan edukasi pengguna terkait pembuatan kata sandi kuat tetap menjadi langkah strategis.

Keterbatasan Penelitian

Penelitian ini memiliki beberapa keterbatasan. Pertama, data berasal dari satu sumber utama yaitu pemilik aplikasi, sehingga pandangan pengguna umum belum tergambarkan secara utuh. Kedua, penelitian tidak mencakup pengujian teknis seperti brute force test, audit server, atau analisis metode enkripsi, padahal aspek tersebut penting untuk mengevaluasi keamanan secara menyeluruh (Bartłomiejczyk & El Fray, 2024). Ketiga, fokus penelitian hanya pada penggunaan OTP pada login tanpa mengkaji keamanan database, manajemen sesi, ataupun perlindungan terhadap serangan jaringan.

Keempat, penelitian tidak membandingkan penerapan OTP di AY Pulsa dengan aplikasi serupa sehingga hasil masih bersifat spesifik. Selain itu, observasi dilakukan dalam waktu terbatas sehingga perubahan perilaku pengguna jangka panjang tidak dapat dipantau. Keterbatasan ini memberikan ruang untuk penelitian lanjutan yang lebih komprehensif.

Implikasi dan Arah Pengembangan ke Depan

Temuan penelitian menunjukkan bahwa implementasi OTP dapat meningkatkan kepercayaan pengguna dan memperkuat autentikasi dua faktor. Untuk pengembangan selanjutnya, AY Pulsa dapat mempertimbangkan metode autentikasi tambahan seperti autentikasi biometrik, PIN dinamis, atau integrasi dengan aplikasi autentikator yang lebih aman dari interception (Bartłomiejczyk & El Fray, 2024).Edukasi pengguna terkait pembuatan kata sandi yang kuat juga perlu ditingkatkan untuk meminimalkan risiko dari sisi pengguna. Selain itu, audit keamanan berkala, penetration testing, serta pemantauan log aktivitas dapat membantu mendeteksi ancaman lebih awal. Penelitian mendatang disarankan melibatkan pengguna sebagai responden untuk memperoleh gambaran yang lebih luas mengenai kenyamanan, efektivitas, dan kendala OTP dalam praktik sehari-hari (Wiranto & Salis, 2025). Dengan mengombinasikan peningkatan teknologi dan pemahaman perilaku pengguna, keamanan aplikasi dapat terus ditingkatkan dan memberikan perlindungan optimal bagi seluruh pengguna AY Pulsa.

REFERENSI

Khairina, N., & Harahap, M. K. (2018). Menjaga Kerahasiaan Data dengan Steganografi Kombinasi LSB-2 dengan

e-ISSN : 2797-3298
p-ISSN : 2089-9424

LSB-3. *SinkrOn - Jurnal & Penelitian Teknik Informatika , 3*(1), 286-288.

Khairina, N., Harahap, M. K., & Lubis, J. H. (2018). The Authenticity of Image using Hash MD5 and Steganography Least Significant Bit . *International Journal Of Information System & Technology, 2*(1), 1-6.

Parulian Sitorus, S., Riama Sidauruk, S., Alamsyah, Y., Sun, A., & Akbar Ritonga, A. (2023). Cyber Forensik Digital. *Jurnal Arjuna : Aplikasi Riset Jaringan Dan Komputer*, *1*(1), 7–10. https://doi.org/10.5281/zenodo.11077724

Aloul, F. (2010). *Multi-factor authentication for mobile devices*. International Journal of Computer Science & Information Technology, 2(3), 15–23.

App-based Detection of SMS OTP Vulnerabilities in Banking Systems. (2024). *Journal of Cybersecurity Engineering*, 12(2), 77–89.

Bartłomiejczyk, M., & El Fray, I. (2024). *Security gaps in SMS OTP authentication: A technical and user-centric analysis*. International Journal of Digital Forensics, 9(1), 45–62.

Bhatia, S. (2019). *Mobile application security: A layered defense approach*. Journal of Information Security Studies, 8(2), 110–125.

Bonneau, J., Preibusch, S., & Anderson, R. (2012). *A systematic analysis of password security issues in online systems*. ACM Computing Surveys, 45(3), 1–35.

Creswell, J. W. (2021). *Qualitative inquiry and research design: Choosing among five approaches* (4th ed.). SAGE Publications.

Das, A., Bonneau, J., Caesar, M., Borisov, N., & Wang, X. (2014). *The tangled web of password reuse*. Network & Distributed System Security Symposium, 1–12.

Fitriyansyah, M., & Hazri, A. (2020). *Analisis keamanan sistem login berbasis password statis dan OTP*. Jurnal Teknologi Keamanan Informasi, 6(1), 33–42.

Florêncio, D., & Herley, C. (2007). *A large-scale study of web password habits*. Proceedings of the 16th International Conference on World Wide Web, 657–666.

Hayuningtyas, R. (2025a). *Implementasi OTP melalui WhatsApp API pada aplikasi digital*. Jurnal Sistem Informasi Terapan, 13(1), 21–34.

Hayuningtyas, R. (2025b). *Studi delay pengiriman OTP dan dampaknya terhadap pengalaman pengguna*. Jurnal Keamanan Siber Indonesia, 5(2), 88–102.

Implementasi One Time Password Menggunakan WhatsApp API pada Aplikasi Mobile. (2025). *Jurnal Teknologi Informasi dan Komunikasi Digital*, 9(1), 55–68.

Kaspersky. (2018). *The future of authentication: OTP and multi-factor security*. Kaspersky Security Report.

Maulana, F., Putra, A., & Rahman, T. (2025). *Keamanan autentikasi pada aplikasi digital berbasis transaksi*. Jurnal Informatika dan Keamanan Siber, 7(1), 14–27.

Mayorga, R., & Yoo, S. (2025). *Evaluating two-factor authentication effectiveness in mobile applications*. International Journal of Cybersecurity, 11(2), 90–108.

Meng, W. (2020). *Multi-factor authentication systems and OTP mechanisms in modern cybersecurity*. Cybersecurity Intelligence Review, 4(3), 50–63.

Rahayuda, I. G. B., & Santiari, N. P. (2023). *Evaluasi keamanan OTP Firebase menggunakan SAST dan IAST*. Jurnal Teknologi dan Rekayasa Perangkat Lunak, 4(2), 79–93.

Stallings, W. (2017). *Information security: Principles and practice* (3rd ed.). Pearson.

Wiranto, B., & Salis, R. (2025a). *Pengaruh pengalaman pengguna terhadap persepsi keamanan OTP*. Jurnal Interaksi Digital, 8(1), 30–44.

Wiranto, B., & Salis, R. (2025b). *User experience evaluation of OTP-based authentication in mobile banking*. Journal of Human-Centered Computing, 12(1), 22–37.

Wiranto, B., & Salis, R. (2025c). *User trust and behavior in OTP authentication systems*. Journal of Cyber Behavior Studies, 10(2), 55–70.

Wibawa, A., Suryanto, A., & Ningsih, D. (2024). *Keamanan autentikasi TOTP pada aplikasi digital*. Jurnal Keamanan Informasi Indonesia, 6(1), 44–59.

Yin, R. K. (2018). *Case study research and applications: Design and methods* (6th ed.). SAGE Publications.