
**PENGALAMAN PENGGUNA DAN KEPERCAYAAN TERHADAP KEAMANAN *OTP*
DALAM SISTEM AUTENTIKASI DOMPET *DIGITAL***

Heri Wiranto^{1*}, Afwa Mufti Salis²

¹Program Studi Ilmu Komputer, Fakultas Psikologi, Bisnis, dan Teknologi, Universitas Yayasan Pendidikan Imam Bonjol Majalengka, Majalengka, Jawa Barat, Indonesia

²Program Studi Sistem Informasi, Fakultas Rekayasa Industri, Universitas Telkom, Bandung, Jawa Barat, Indonesia

*email: heriwiranto@univypib.ac.id

Received: 2025-04-25 Accepted: 2025-06-13 Published: 2025-06-28

Abstrak

Penelitian ini bertujuan untuk menganalisis hubungan antara pengalaman pengguna (*user experience*) dan kepercayaan (*trust*) terhadap keamanan *One Time Password (OTP)* dalam sistem autentikasi dompet *digital*. Latar belakang penelitian ini adalah meningkatnya adopsi *OTP* dalam transaksi *digital*, namun belum banyak penelitian yang menyoroti pengaruh pengalaman pengguna terhadap kepercayaan terhadap sistem ini. Penelitian ini menggunakan pendekatan kuantitatif dengan desain deskriptif korelasional, melibatkan 100 responden pengguna dompet *digital* yang dipilih melalui teknik *purposive sampling*. Data dikumpulkan menggunakan kuesioner *Likert* skala 4 poin dan dianalisis menggunakan uji korelasi *Rank-Spearman*. Hasil analisis menunjukkan bahwa tidak terdapat hubungan yang signifikan antara pengalaman pengguna dan kepercayaan terhadap keamanan *OTP*, dengan nilai $p = 0,657$ dan koefisien korelasi $\rho = 0,045$. Nilai koefisien determinasi (KD) sebesar 0,2% menunjukkan bahwa kontribusi pengalaman pengguna terhadap kepercayaan sangat kecil. Simpulan dari penelitian ini adalah bahwa meskipun pengalaman pengguna penting dalam aspek lain seperti kepuasan dan loyalitas, kepercayaan terhadap *OTP* kemungkinan lebih dipengaruhi oleh persepsi risiko, pemahaman teknologi, dan edukasi keamanan. Penelitian ini merekomendasikan pendekatan autentikasi yang tidak hanya berfokus pada kenyamanan, tetapi juga pada edukasi dan transparansi sistem keamanan.

Kata kunci: Pengalaman Pengguna, Kepercayaan, Keamanan *OTP*, Dompet *Digital*

Abstract

This study aims to analyze the relationship between user experience and trust in the security of One Time Password (OTP) within digital wallet authentication systems. The research is motivated by the widespread adoption of OTP in digital transactions and the limited studies examining how user experience influences trust in such systems. A quantitative approach with a descriptive correlational design was employed, involving 100 digital wallet users selected via purposive sampling. Data were collected using a 4-point Likert-scale questionnaire and analyzed with the Rank-Spearman correlation test. The results revealed no significant relationship between user experience and trust in OTP security, with a p-value of 0.657 and correlation coefficient $\rho = 0.045$. The coefficient of determination (KD) was 0.2%, indicating a minimal contribution of user experience to trust. The study concludes that while user experience is important for satisfaction and loyalty, trust in OTP is likely more influenced by perceived risk, technological literacy, and security education. This study recommends authentication strategies that go beyond usability, incorporating educational and transparency measures to foster user trust.

Keywords: User Experience, Trust, OTP Security, Digital Wallets.

How to cite (in APA style): Wiranto, H., & Mufti Salis, A. (2025). Pengalaman pengguna dan kepercayaan terhadap keamanan OTP dalam sistem autentikasi dompet digital. *Jurnal Pendidikan Informatika Dan Sains*, 14(1), 75–83. <https://doi.org/10.31571/saintek.v14i1.8897>

Copyright (c) 2025 Heri Wiranto, Afwa Mufti Salis

DOI: 10.31571/saintek.v14i1.8897

PENDAHULUAN

Keamanan data menjadi aspek krusial dalam penggunaan layanan berbasis internet, terutama di era *digital* yang semakin berkembang pesat (Suryawijaya, 2023). Dengan meningkatnya jumlah transaksi *digital*, kebutuhan akan sistem autentikasi yang andal dan aman semakin meningkat. Salah satu metode autentikasi yang banyak digunakan adalah *One Time Password (OTP)*. *OTP* berfungsi sebagai kode verifikasi sementara yang dikirimkan kepada pengguna untuk memastikan identitas mereka sebelum mengakses layanan tertentu (Raihan et al., 2024). Penerapan *OTP* telah menjadi standar dalam berbagai sistem keamanan (Alfarizi et al., 2024), terutama dalam layanan perbankan, *e-commerce*, dan dompet *digital* sebagai bentuk perlindungan terhadap ancaman keamanan siber.

Namun, meskipun *OTP* dirancang untuk meningkatkan keamanan (Rahmadsyah et al., 2025), pengguna sering kali mengalami berbagai kendala dalam penggunaannya. Beberapa permasalahan umum yang dihadapi meliputi keterlambatan pengiriman kode, kesalahan dalam memasukkan *OTP*, serta kekhawatiran terhadap penyalahgunaan data pribadi (Ramadhan, 2024). Hal ini dapat memengaruhi pengalaman pengguna, yang pada akhirnya berdampak pada tingkat kepercayaan mereka terhadap sistem keamanan *OTP*. Pengguna yang merasa bahwa proses penggunaan *OTP* cenderung merepotkan atau menimbulkan rasa tidak aman berpotensi enggan menggunakan layanan *digital* yang mengandalkan metode autentikasi ini. Hal ini sejalan dengan temuan (Robaniyah & Kurnianingsih, 2021) yang menunjukkan bahwa persepsi kemudahan penggunaan dan kepercayaan berpengaruh signifikan terhadap minat penggunaan aplikasi pembayaran *digital* seperti *OVO*.

Beberapa penelitian sebelumnya telah mengkaji berbagai aspek terkait *OTP*. Wibawa et al. (2024) meneliti implementasi *Time-Based OTP* menggunakan *Python* dan *Flask*, yang tidak hanya meningkatkan keamanan autentikasi tetapi juga menawarkan kemudahan integrasi, sehingga berpotensi meningkatkan pengalaman pengguna serta kepercayaan terhadap keamanan sistem *OTP* (Wibawa et al., 2024). Khasanah et al. (2023) mengembangkan sistem *Computer-Based Test (CBT)* dengan keamanan *OTP* berbasis algoritma SHA-256. Hasil penelitian menunjukkan bahwa *OTP* meningkatkan kepercayaan pengguna terhadap keamanan sistem *login* dengan membatasi akses hanya pada pemegang token yang valid (Khasanah et al., 2023). Ramadhan (2024) menganalisis sentimen opini pengguna terhadap keamanan *OTP* pada dompet *digital OVO* di media sosial *Twitter*. Hasilnya menunjukkan bahwa kekhawatiran pengguna terhadap keamanan *OTP* memengaruhi tingkat kepercayaan dan pengalaman pengguna dalam bertransaksi *digital* (Ramadhan, 2024).

Kesenjangan penelitian ini menunjukkan bahwa meskipun *OTP* telah diadopsi secara luas, pemahaman mengenai bagaimana pengalaman pengguna secara langsung memengaruhi kepercayaan terhadap keamanan *OTP* dalam layanan dompet *digital* masih terbatas. Padahal, dalam konteks dompet *digital*, kepercayaan terhadap sistem keamanan sangat menentukan apakah pengguna bersedia melakukan transaksi secara rutin atau bahkan tetap menggunakan layanan tersebut dalam jangka panjang (Agustiningrum & Andjarwati, 2021). Penelitian lain sebelumnya juga menunjukkan bahwa di sektor perbankan, persepsi terhadap keamanan dan kepercayaan terbukti menjadi prediktor signifikan terhadap niat penggunaan aplikasi (Almaiah et al., 2023), sementara beberapa studi menunjukkan bahwa *OTP* turut memperkuat kepercayaan dan kepuasan pengguna dalam pembayaran *digital* (Muhtasim et al., 2022). Namun jika pengguna memiliki pengalaman yang buruk dalam penggunaan *OTP*, seperti sering mengalami kegagalan verifikasi atau merasa prosesnya terlalu rumit, mereka dapat kehilangan kepercayaan terhadap sistem (Tanera, 2023), yang berpotensi membuat

mereka beralih ke metode pembayaran lain atau bahkan berhenti menggunakan layanan dompet *digital* sepenuhnya.

Berdasarkan kesenjangan penelitian yang telah diidentifikasi, penelitian ini bertujuan untuk menganalisis hubungan antara pengalaman pengguna dan kepercayaan terhadap keamanan *OTP* dalam layanan dompet *digital*. Dengan meningkatnya penggunaan dompet *digital* dalam berbagai transaksi keuangan, penting untuk memahami faktor-faktor yang memengaruhi kepercayaan pengguna terhadap sistem keamanan *OTP*. Hasil penelitian ini diharapkan dapat memberikan kontribusi terhadap pengembangan sistem autentikasi *digital*, khususnya dalam konteks dompet *digital*, dengan menekankan pentingnya pemahaman terhadap persepsi pengguna terkait kepercayaan dan pengalaman penggunaan. Dengan mengidentifikasi lemahnya hubungan antara *user experience* dan *trust* terhadap keamanan *OTP*, penelitian ini membuka ruang bagi pengembangan pendekatan autentikasi yang tidak hanya mengutamakan kenyamanan, tetapi juga memperhatikan transparansi dan edukasi keamanan sebagai faktor pendukung kepercayaan. Temuan ini sejalan dengan studi (Robaniyah & Kurnianingsih, 2021), yang menunjukkan bahwa kemudahan dan persepsi keamanan memengaruhi intensi penggunaan layanan *digital* secara signifikan.

METODE

Dalam pelaksanaannya, penelitian ini mengadopsi metode kuantitatif serta desain korelasional yang bersifat deskriptif. Pendekatan ini bertujuan untuk mengidentifikasi dan menganalisis hubungan antara pengalaman pengguna (*user experience*) dan kepercayaan terhadap keamanan *OTP* dalam layanan dompet *digital*. Survei dalam bentuk kuesioner digunakan untuk mengumpulkan data, yang kemudian dianalisis menggunakan metode *Rank Spearman* untuk mengukur korelasi antar variabel.

Populasi dan Sampel

Penentuan jumlah sampel dalam penelitian ini menggunakan rumus *Cochran* karena populasi yang menjadi sasaran relatif besar dan tidak diketahui secara pasti jumlah pastinya. Rumus *Cochran* digunakan untuk menghitung ukuran sampel minimum yang diperlukan agar hasil penelitian dapat digeneralisasikan terhadap populasi dengan tingkat kepercayaan dan *margin of error* tertentu. Dalam penelitian ini, digunakan *margin of error* sebesar 10% dan tingkat kepercayaan 95% ($z = 1,96$), yang sesuai untuk penelitian eksploratif awal.

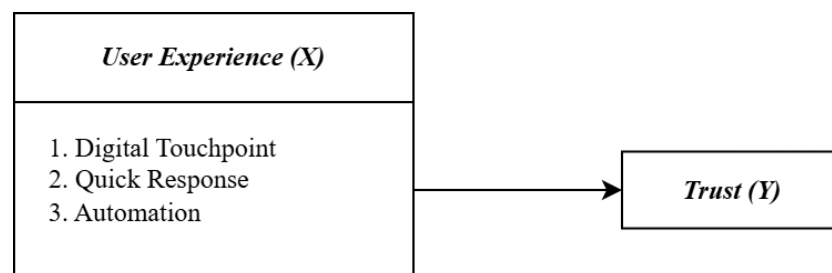
Populasi target dalam penelitian ini adalah masyarakat Indonesia yang menggunakan dompet *digital*, tanpa dibatasi oleh satu merek aplikasi tertentu. Oleh karena itu, pendekatan ini dipilih untuk memberikan ruang generalisasi pada berbagai *platform* dompet *digital* seperti *DANA*, *OVO*, *GoPay*, dan *ShopeePay*. Perhitungan jumlah sampel minimum menggunakan rumus *Cochran* (Persamaan 1).

$$n_0 = \frac{z^2 \cdot p \cdot (1 - p)}{e^2} \quad (1)$$

Persamaan 1, diketahui n_0 adalah ukuran sampel minimum, z adalah skor z pada tingkat kepercayaan 95% (1,96), p adalah proporsi responden dalam populasi (diasumsikan 0,5 karena tidak diketahui secara pasti) dan e adalah *margin of error* (0,10 atau 10%). Pengambilan sampel dilakukan secara *purposive* berdasarkan kriteria inklusi yang telah ditetapkan, yaitu : 1) Responden telah menggunakan dompet *digital* selama minimal 5 bulan terakhir sejak penelitian dilakukan, 2) Responden telah menggunakan *OTP* yang dikirim melalui *SMS*, *email*, atau aplikasi autentikasi (*Authy*, *Google Authenticator*, dsb.), 3) Responden telah menggunakan *OTP* dalam transaksi yang beragam, seperti pembayaran *e-commerce*, transfer saldo, pembayaran tagihan, dan transaksi *offline* dengan *QRIS*. Dengan demikian, jumlah sampel minimum adalah 96 orang. Untuk mengantisipasi potensi bias atau data tidak lengkap, peneliti menggunakan sampel sebanyak 100 responden.

Jenis dan Sumber Data

Jenis data yang digunakan dalam studi ini adalah data primer yang diperoleh secara langsung melalui kuesioner daring (*online survey*). Penyusunan kuesioner mengacu pada skala *Likert* dengan empat kategori jawaban, dengan rentang skor: angka 1 untuk sangat tidak setuju, 2 untuk tidak setuju, 3 untuk setuju, dan 4 untuk sangat setuju. Kuesioner terdiri dari tiga bagian utama, yaitu: Karakteristik responden (usia, jenis kelamin, jenis dompet *digital* yang digunakan, frekuensi penggunaan), Pengalaman pengguna (*User Experience*) sebagai variabel independen (X) dimana dapat diukur melalui indikator *Digital Touchpoint*, *Quick Response*, dan *Automation* (Rahayu & Faulina, 2022). Kepercayaan terhadap keamanan *OTP* sebagai variabel dependen (Y) yang dapat diukur melalui indikator Keyakinan pada Layanan, Kualitas Layanan, dan Keamanan Layanan (Efrianto & Tresnawaty, 2021). Model penelitian ditampilkan pada Gambar 1.



Gambar 1. Model Penelitian

Berdasarkan model penelitian pada gambar 1, dirumuskan hipotesis sebagai berikut: H_0 : pengalaman pengguna (*user experience*) tidak berpengaruh terhadap kepercayaan (*trust*) keamanan *OTP* pada dompet *digital*. H_1 : pengalaman pengguna (*user experience*) berpengaruh terhadap kepercayaan (*trust*) keamanan *OTP* pada dompet *digital*. Data yang telah dikumpulkan selanjutnya dianalisis dengan menggunakan uji *Rank Spearman*.

Instrumen dan Pengujian Validitas Reliabilitas

Instrumen yang digunakan dalam penelitian ini adalah kuesioner dengan skala *Likert* 4 poin, yang terdiri dari dua variabel utama, yaitu pengalaman pengguna (*user experience*) sebagai variabel independen (X) dan kepercayaan terhadap keamanan *OTP* (*trust*) sebagai variabel dependen (Y). Skala *Likert* yang digunakan memiliki rentang nilai dari 1 (sangat tidak setuju) hingga 4 (sangat setuju). Penyusunan kuesioner ini dilakukan melalui proses adaptasi dan pengembangan dari beberapa penelitian terdahulu, dengan penyesuaian terhadap konteks dompet *digital* dan sistem autentikasi *OTP*. Penyesuaian dilakukan untuk memastikan relevansi indikator dengan pengalaman nyata pengguna dalam menggunakan layanan dompet *digital* seperti *DANA*, *OVO*, *GoPay*, dan *ShopeePay*.

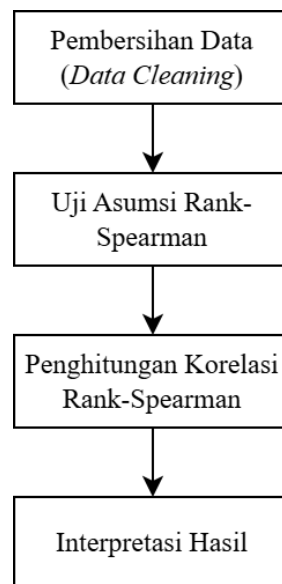
Variabel pengalaman pengguna diukur melalui tiga konstruk utama, yaitu *digital touchpoint*, *quick response*, dan *automation* (Rahayu & Faulina, 2022). Konstruk *digital touchpoint* mencakup aspek seperti kemudahan navigasi dan aksesibilitas aplikasi; *quick response* mengacu pada seberapa cepat sistem merespons tindakan pengguna; sedangkan *automation* berhubungan dengan otomatisasi proses layanan, termasuk pengiriman *OTP*. Masing-masing konstruk terdiri dari 3 hingga 5 item pernyataan. Sementara itu, variabel kepercayaan terhadap keamanan *OTP* mencakup tiga konstruk, yaitu keyakinan pada layanan, kualitas layanan, dan keamanan layanan (Efrianto & Tresnawaty, 2021). Keyakinan pada layanan mengukur sejauh mana pengguna percaya pada sistem keamanan yang diterapkan; kualitas layanan menilai konsistensi dan keandalan pengiriman *OTP*; dan keamanan layanan berkaitan dengan perlindungan data pribadi dan penerapan sistem autentikasi berlapis.

Masing-masing konstruk tersebut juga terdiri dari beberapa item pernyataan yang disusun berdasarkan prinsip-prinsip kepercayaan dalam layanan *digital*.

Kuesioner yang digunakan dalam penelitian ini terlebih dahulu melalui tahap pengujian validitas dan reliabilitas. Uji validitas dilakukan menggunakan *Pearson Product Moment*, sedangkan reliabilitas diuji dengan *Cronbach's Alpha* menggunakan SPSS versi 25. Suatu item dikatakan valid apabila *r*-hitung lebih besar dari *r*-tabel, dan reliabel apabila nilai *Cronbach's Alpha* melebihi angka 0,70

Metode Analisis Data

Metode analisis data dalam penelitian ini dilakukan melalui beberapa tahapan. Tahap pertama adalah pembersihan data (*data cleaning*), yaitu mengeliminasi data yang tidak memenuhi kelengkapan atau tidak sesuai dengan syarat inklusi yang ditentukan. Setelah itu, uji asumsi *Rank Spearman* diterapkan untuk menilai apakah data memenuhi ketentuan yang diperlukan untuk pengujian korelasi non-parametrik. Setelah itu, dilakukan penghitungan korelasi *Rank Spearman* guna mengukur tingkat hubungan antara pengalaman pengguna dan kepercayaan terhadap keamanan *OTP*. Selain menggunakan uji korelasi *Rank Spearman* untuk menganalisis hubungan antara variabel pengalaman pengguna dan kepercayaan terhadap keamanan *OTP*, peneliti mempertimbangkan penggunaan uji regresi linier sebagai teknik analisis pendukung. Namun, berdasarkan hasil uji awal, data tidak memenuhi asumsi dasar regresi seperti linearitas dan distribusi normal dari residual. Oleh karena itu, analisis regresi tidak dilakukan, dan korelasi *Rank Spearman* tetap digunakan karena lebih sesuai untuk data yang bersifat ordinal dan tidak terdistribusi normal secara sempurna. Terakhir, hasil analisis diinterpretasikan dengan menilai kekuatan hubungan berdasarkan koefisien korelasi yang berkisar antara -1 hingga 1 serta signifikansi hubungan menggunakan *p-value* dengan tingkat kepercayaan 95% ($\alpha = 0,05$). Tahapan tersebut dapat dilihat pada Gambar 2.



Gambar 2. Alur Metode Analisis Data

HASIL DAN PEMBAHASAN

Uji validitas dilakukan dengan membandingkan nilai korelasi empiris (*r* hitung) dan nilai kritis (*r* tabel) pada tingkat signifikansi 5%, berdasarkan data dari seratus responden. Sebuah item dikatakan valid apabila nilai *r* hitung lebih besar daripada *r* tabel yang bernilai 0,1946. Berdasarkan hasil uji

validitas yang ditampilkan dalam Tabel 1, seluruh item dalam kuesioner menunjukkan hasil valid. Dengan demikian, seluruh pernyataan dinyatakan valid berdasarkan kriteria pengujian yang digunakan, di mana nilai korelasi empiris (r hitung) untuk setiap butir pernyataan lebih besar dari nilai korelasi tabel (r tabel) sebesar 0,1946 pada tingkat signifikansi 5%. Sehingga semua butir pernyataan dianggap valid dan pernyataan-pernyataan tersebut dapat dipertimbangkan dan digunakan dalam penelitian selanjutnya.

Tabel 1. Hasil Uji Validitas

Variabel	Indikator	R_{hitung}	R_{tabel}	Hasil
<i>User Experience</i>	x 1	0,622	0,1946	Valid
	x 2	0,614	0,1946	Valid
	x 3	0,612	0,1946	Valid
<i>Trust</i>	y 1	0,458	0,1946	Valid
	y 2	0,614	0,1946	Valid
	y 3	0,590	0,1946	Valid

Setelah proses pengujian validitas dilakukan, tahap berikutnya adalah melakukan uji reliabilitas. Menurut Heale dan Twycross, suatu instrumen dinyatakan reliabel apabila nilai *Cronbach's Alpha* mencapai 0,70 atau lebih. Hasil uji reliabilitas yang ditampilkan dalam Tabel 2 menunjukkan bahwa seluruh item dalam instrumen penelitian ini memenuhi standar reliabilitas. Hasil ini mengindikasikan bahwa kuesioner yang digunakan mampu menghasilkan data yang konsisten, baik ketika diujikan dalam waktu berbeda maupun dengan rancangan pengukuran yang tidak sama.

Tabel 2. Hasil Uji Reliabilitas

Variabel	<i>Reliability Coefficient</i>	<i>Cronbach's Alpha</i>	Hasil
<i>User Experience</i>	15 Pertanyaan	0,925	Reliabel
<i>Trust</i>	15 Pertanyaan	0,806	Reliabel

Setelah tahap pengumpulan data selesai dilakukan, langkah berikutnya adalah melakukan analisis hubungan antar variabel dengan menggunakan uji korelasi *Rank Spearman*. Analisis ini bertujuan untuk menilai tingkat keterkaitan antara variabel *user experience* dan *trust*. Tabel 3 menyajikan hasil pengolahan data berdasarkan uji korelasi *Rank Spearman*.

Tabel 3. Hasil Analisis Korelasi *Rank Spearman* Antara Variabel *User Experience* terhadap *Trust*

<i>User Experience</i>				
	<i>P-Value</i>	Koefisien Korelasi	Arah	KD
<i>Trust</i>	0,657	0,045	Positif	0,2%

Hasil uji korelasi *Rank Spearman* dalam penelitian ini menunjukkan bahwa tidak terdapat hubungan yang signifikan antara *user experience* dan *trust* terhadap keamanan *OTP* dalam konteks dompet *digital*. Berdasarkan hasil analisis, diperoleh nilai koefisien korelasi sebesar $\rho = 0,045$ dengan nilai $p = 0,657$. Karena nilai p jauh di atas ambang signifikansi 0,05, maka hipotesis nol (H_0) diterima, dan hipotesis alternatif (H_1) ditolak. Hal ini menandakan bahwa secara statistik tidak terdapat hubungan yang berarti antara kedua variabel tersebut.

Meskipun arah hubungan yang terbentuk bersifat positif, nilai korelasinya sangat lemah dan tidak cukup untuk menunjukkan keterkaitan yang kuat antara pengalaman pengguna dan kepercayaan terhadap keamanan *OTP*. Nilai koefisien determinasi (KD) yang diperoleh sebesar 0,2% mengindikasikan bahwa hanya sebagian kecil variasi pada variabel *trust* yang dapat dijelaskan oleh *user experience*. Dengan kata lain, terdapat kemungkinan bahwa kepercayaan pengguna terhadap

sistem keamanan *OTP* lebih banyak dipengaruhi oleh faktor-faktor lain yang tidak diuji dalam penelitian ini, seperti pemahaman terhadap teknologi, persepsi risiko, atau pengalaman negatif sebelumnya.

Hasil analisis yang menunjukkan tidak adanya hubungan signifikan antara pengalaman pengguna dan kepercayaan terhadap keamanan *OTP* juga diperkuat oleh fakta bahwa model regresi tidak dapat dibangun secara valid karena data tidak memenuhi prasyarat analisis regresi. Hal ini menunjukkan bahwa hubungan antar variabel dalam konteks ini lebih kompleks, sehingga tidak cukup hanya dijelaskan oleh pendekatan linier semata. Dengan demikian, penggunaan uji *Rank Spearman* sebagai metode nonparametrik dinilai paling sesuai untuk konteks penelitian ini.

Temuan ini menegaskan bahwa peningkatan pengalaman pengguna, meskipun penting, belum mampu secara signifikan membentuk kepercayaan terhadap mekanisme autentikasi *OTP* jika tidak dibarengi dengan faktor lain seperti jaminan keamanan dan pemahaman risiko oleh pengguna. Oleh karena itu, strategi peningkatan kepercayaan sebaiknya tidak hanya difokuskan pada aspek kenyamanan dan kemudahan penggunaan aplikasi, tetapi juga mencakup aspek edukasi, transparansi sistem keamanan, dan penanganan risiko keamanan secara lebih terbuka.

Meskipun demikian, penting untuk dicatat bahwa *user experience* tetap memiliki peran penting dalam membentuk aspek lain dari perilaku pengguna, seperti kepuasan dan loyalitas. Sejumlah penelitian terdahulu (Agustiono et al., 2022; Faizi et al., 2022; Hernawan & Harimurti, 2021; Nirawati et al., 2020) mengungkap bahwa pengalaman pengguna yang positif berkontribusi terhadap peningkatan kepuasan pengguna dan loyalitas terhadap layanan *digital*. Namun, dalam konteks keamanan *OTP*, hasil penelitian ini memberikan perspektif baru bahwa kepercayaan tidak hanya bergantung pada interaksi pengguna dengan aplikasi, melainkan juga pada persepsi terhadap risiko, integritas sistem, dan edukasi terkait keamanan *digital*.

Dengan demikian, hasil ini memperluas pemahaman mengenai dimensi *trust* dalam sistem autentikasi, khususnya *OTP*, di mana pengalaman pengguna yang positif tidak serta-merta menjamin meningkatnya kepercayaan pengguna terhadap keamanan yang disediakan. Oleh karena itu, perusahaan penyedia dompet *digital* perlu mempertimbangkan strategi tambahan dalam membangun kepercayaan terhadap *OTP*, seperti transparansi mekanisme keamanan, edukasi pengguna mengenai perlindungan data, dan peningkatan teknologi autentikasi berbasis biometrik atau token fisik sebagai alternatif atau pelengkap *OTP*.

Secara keseluruhan, temuan ini menegaskan pentingnya pendekatan multidimensional dalam merancang sistem autentikasi yang tidak hanya nyaman digunakan tetapi juga mampu membangun keyakinan pengguna secara berkelanjutan. Penelitian ini memberikan kontribusi pada literatur dengan menyoroti bahwa dalam sistem keamanan *digital*, aspek kepercayaan tidak dapat disederhanakan hanya berdasarkan pengalaman penggunaan, melainkan harus dipandang sebagai hasil dari interaksi antara persepsi keamanan, edukasi teknologi, serta komunikasi risiko yang efektif kepada pengguna.

SIMPULAN

Berdasarkan hasil analisis korelasi *Rank Spearman*, penelitian ini menyimpulkan bahwa tidak terdapat hubungan yang signifikan antara pengalaman pengguna (*user experience*) dan kepercayaan (*trust*) terhadap keamanan *OTP* dalam sistem autentikasi dompet *digital*. Nilai koefisien korelasi sebesar $\rho = 0,045$ dan nilai $p = 0,657$ menunjukkan bahwa arah hubungan bersifat positif namun sangat lemah, dan tidak signifikan secara statistik. Koefisien determinasi yang rendah, yakni 0,2%, mengindikasikan bahwa pengalaman pengguna hanya menjelaskan sebagian kecil variasi dalam kepercayaan terhadap sistem keamanan *OTP*. Temuan ini menegaskan bahwa aspek kenyamanan atau pengalaman antarmuka dalam penggunaan aplikasi dompet *digital* belum cukup untuk membangun kepercayaan terhadap fitur keamanan seperti *OTP*. Oleh karena itu, perusahaan penyedia layanan dompet *digital* perlu mempertimbangkan strategi tambahan untuk membangun kepercayaan

pengguna secara menyeluruh. Strategi tersebut meliputi peningkatan transparansi mekanisme keamanan, edukasi *digital* terkait perlindungan data, serta optimalisasi teknologi autentikasi berbasis biometrik atau token fisik sebagai pelengkap *OTP*. Dengan pendekatan tersebut, kepercayaan pengguna terhadap sistem keamanan dapat dibangun tidak hanya dari sisi pengalaman penggunaan, tetapi juga dari aspek perlindungan dan pemahaman terhadap risiko. Penelitian ini memberikan kontribusi penting dalam literatur tentang kepercayaan pengguna dalam konteks keamanan *digital*, dan membuka ruang untuk penelitian lanjutan yang mengeksplorasi faktor-faktor lain yang memengaruhi kepercayaan terhadap sistem autentikasi di era *digital*.

REFERENSI

- Agustiningrum, D., & Andjarwati, A. L. (2021). Pengaruh kepercayaan, kemudahan, dan keamanan terhadap keputusan pembelian di marketplace. *Jurnal Ilmu Manajemen*, 9(3), 896–906. <https://doi.org/10.26740/jim.v9n3.p896-906>
- Agustiono, Listyorini, S., & Nugraha, H. S. (2022). Pengaruh customer experience terhadap customer loyalitas pelanggan melalui kepuasan pelanggan sebagai variabel intervening (studi pada masyarakat Semarang pengguna LinkAja). *Jurnal Ilmu Administrasi Bisnis*, 11(2), 244–256. <https://doi.org/doi.org/10.14710/jiab.2022.34564>
- Alfarizi, S., Sumaryana, Y., & Sundari, S. S. (2024). Rancang bangun sistem informasi jual beli motor menggunakan one time password (OTP) dan Mailtrap API. *Jurnal Informatika Dan Teknik Elektro Terapan*, 12(2), 1115–1122. <https://doi.org/10.23960/jitet.v12i2.4137>
- Almaiah, M. A., Al-Otaibi, S., Shishakly, R., Hassan, L., Lutfi, A., Alrawad, M., Qatawneh, M., & Alghanam, O. A. (2023). Investigating the role of perceived risk, perceived security and perceived trust on smart m-banking application using SEM. *Sustainability (Switzerland)*, 15(13), 1–17. <https://doi.org/10.3390/su15139908>
- Efrianto, G., & Tresnawaty, N. (2021). Pengaruh privasi, keamanan, kepercayaan dan pengalaman terhadap penggunaan fintech di kalangan masyarakat Kabupaten Tangerang Banten. *Jurnal Ilmiah Akuntansi Dan Ekonomi*, 6(1), 53–72. <https://doi.org/10.54964/liabilitas.v6i1.71>
- Faizi, N., Febrilia, I., & Rahmi. (2022). Analisis pengaruh customer experience dan e-service quality terhadap customer satisfaction pada pengguna transportasi online di Jakarta. *Jurnal Bisnis, Manajemen, Dan Keuangan*, 3(2), 391–403. <https://doi.org/doi.org/10.21009/jbmk.0302.05>
- Hernawan, M., & Harimurti, C. (2021). Pengaruh customer experience dan kepuasan pelanggan terhadap loyalitas pelanggan Smartfren. *Jurnal Administrasi Bisnis*, 1(4), 61–77. <https://doi.org/doi.org/10.31334/jambis.v1i4.1808>
- Khasanah, N. I., Mujiyanto, A. H., & Widoyoningrum, S. (2023). Peningkatan sistem keamanan one time password (OTP) pada token aplikasi computer based test (CBT) menggunakan algoritma SHA-256. *INOVATE - Jurnal Ilmiah Inovasi Teknologi Informasi*, 8(1), 18–27. <https://ejournal.unhasy.ac.id/index.php/innovate/article/view/5084>
- Muhtasim, D. A., Tan, S. Y., Hassan, M. A., Pavel, M. I., & Susmit, S. (2022). Customer satisfaction with digital wallet services: An analysis of security factors. *International Journal of Advanced Computer Science and Applications*, 13(1), 195–206. <https://doi.org/10.14569/IJACSA.2022.0130124>
- Nirawati, L., Pratiwi, A. D., Mutiahana, A., & Afida, E. A. (2020). Pengaruh kepercayaan konsumen dan pengalaman pelanggan (customer experience) terhadap loyalitas pelanggan pada aplikasi Shopee. *Jurnal Syntax Transformation*, 1(9), 624–631. <https://doi.org/doi.org/10.46799/jst.v1i9.157>
- Rahayu, S., & Faulina, S. T. (2022). Pengaruh digital customer experience dalam menciptakan customer satisfaction dan customer loyalty di era digital. *Jesya (Jurnal Ekonomi & Ekonomi Syariah)*, 5(1), 1–13. <https://doi.org/10.36778/jesya.v5i1.568>
- Rahmadsyah, M., Ananda, Y., Nasution, A. A., & Arif, A. (2025). Rancang bangun sistem akses

- kendaraan roda dua dengan sistem kode one time password (OTP) dan e-KTP berbasis Arduino Uno. *Journals of Telecommunication and Electrical Scientific (JTELS)*, 02(01), 58–65. <https://doi.org/https://doi.org/10.24010/jtels.v2i01.1064>
- Raihan, F., Renaldy, R., & Putra, H. R. (2024). Sistem keamanan data web layanan kesehatan dengan metode multi factor authentication (MFA). *Seminar Nasional Sains dan Teknologi (SENS)*, 9(9), 460–467. <https://conference.upgris.ac.id/index.php/sens/article/view/6871>
- Ramadhan, D. Y. (2024). Analisis sentimen opini keamanan kode one time password dompet digital dalam media sosial menggunakan metode lexicon based dan support vector machine learning [Undergraduate thesis, Universitas Islam Negeri Syarif Hidayatullah].
- Robaniyah, L., & Kurnianingsih, H. (2021). Pengaruh persepsi manfaat, kemudahan penggunaan dan keamanan terhadap minat menggunakan aplikasi OVO. *Image: Jurnal Riset Manajemen*, 10(1), 53–62. <https://doi.org/10.17509/image.v10i1.32009>
- Suryawijaya, T. W. E. (2023). Memperkuat keamanan data melalui teknologi blockchain: Mengeksplorasi implementasi sukses dalam transformasi digital di Indonesia. *Jurnal Studi Kebijakan Publik*, 2(1), 55–68. <https://doi.org/10.21787/jskp.2.2023.55-68>
- Tanera, L. (2023). Tantangan dalam menghadapi perkembangan teknologi dan transformasi digital dalam bisnis waralaba. *Jurnal Multilingual*, 3(3), 1412–4823. <https://doi.org/doi.org/10.26499/multilingual.v3i3.459>
- Wibawa, S., Suryanto, S., & Ningsih, R. (2024). Perlindungan data digital dengan time-based one-time password (TOTP). *INSANtek: Jurnal Inovasi dan Sains Teknik Elektro*, 5(1), 30–36. <https://doi.org/10.31294/insantek.v5i1.3495>