JURNAL BISNIS MAHASISWA
Journal homepage: https://jurnalbisnismahasiswa.com
E-ISSN: 2807-2219

Faktor keamanan data dan risiko dalam penggunaan dompet digital: Systematic literature review

Data security factors and risks in using digital wallets: Systematic literature review

Adinda Rahma Dinna*, Arsymanda Nafisa Putri, Mega Zhafarina Purwono
Program Studi Manajemen, Fakultas Ekonomi dan Bisnis, Universitas Kebangsaan Republik Indonesia, Kota Bandung, Indonesia

Abstrak

Tujuan – Penelitian ini bertujuan untuk menyintesis bukti empiris mengenai faktor keamanan data dan risiko penggunaan dompet digital guna memetakan tren riset terkait faktor dominan keamanan data, risiko siber yang signifikan, serta interaksi persepsi aman bagi keberlanjutan adopsi dompet digital.

Desain/metodologi/pendekatan – Penelitian ini menggunakan pendekatan *Systematic Literature Review* (SLR) yang berpedoman pada protokol PRISMA 2020. Data dikumpulkan dari basis data Scopus, ScienceDirect, dan Google Scholar dengan rentang publikasi 2020–2026, yang kemudian diseleksi secara ketat hingga menghasilkan 19 artikel utama untuk dikaji menggunakan teknik analisis tematik.

Temuan – Hasil sintesis menunjukkan bahwa autentikasi biometrik, *two-factor authentication* (2FA), dan enkripsi *end-to-end* merupakan faktor teknis utama yang mampu menurunkan persepsi risiko, meskipun prosedur keamanan yang terlalu ketat dapat mengganggu kenyamanan pengguna. Risiko digital telah berevolusi menjadi ancaman siber lintas batas seperti *phishing*, pencurian identitas, *malware*, pengambilalihan akun, hingga celah privasi akibat *model opacity* pada sistem deteksi penipuan berbasis kecerdasan buatan. Keberlanjutan adopsi dompet digital sangat dibentuk oleh interaksi antara literasi digital pengguna, reputasi platform, serta kejelasan kebijakan perlindungan data.

Keterbatasan penelitian – Keterbatasan dalam penelitian ini mencakup ketiadaan *quality appraisal* formal terhadap metodologi setiap artikel yang dianalisis serta jumlah literatur akhir yang disintesis relatif terbatas (n=19). Selain itu, variasi konteks ekonomi dan regulasi di setiap negara yang diteliti berpotensi memengaruhi hasil penelitian di masing-masing literatur.

Implikasi – Penyedia layanan dompet digital disarankan untuk tidak hanya berfokus pada enkripsi sistem, tetapi juga pada transparansi komunikasi kepada pengguna dan penciptaan keseimbangan antara keamanan dan kemudahan penggunaan (usability). Terdapat pula urgensi bagi regulator untuk menyinkronkan regulasi perlindungan data yang kuat dengan edukasi literasi digital yang disesuaikan berdasarkan profil risiko kelompok pengguna.

Kebaruan – Penelitian ini memberikan sintesis terhadap literatur yang selama ini terfragmentasi antara perspektif adopsi teknologi secara teoretis dengan kajian teknis infrastruktur keamanan siber, serta secara holistik menghubungkan regulasi pelindungan data nasional dengan perilaku keamanan pengguna dompet digital.

Kata Kunci: Keamanan Data, Risiko Digital, Dompet Digital, Systematic Literature Review, Persepsi Aman

Abstract

Purpose *– This study aims to synthesize empirical evidence regarding data security factors and risks in using digital wallets to map research trends related to dominant data security factors, significant cyber risks, and the interaction of perceived security on the sustainability of digital wallet adoption.*

Design/methodology/approach *– This research employs a Systematic Literature Review (SLR) approach guided by the PRISMA 2020 protocol. Data were collected from the Scopus, ScienceDirect, and Google Scholar*

databases with a publication range between 2020 and 2026, and were strictly selected to yield 19 primary articles analyzed using thematic analysis.

Findings *– The synthesis results show that biometric authentication, two-factor authentication (2FA), and end-to-end encryption are the main technical factors capable of reducing perceived risk, although overly strict security procedures can disrupt user convenience. Digital risks have evolved into cross-border cyber threats such as phishing, identity theft, malware, account takeovers, and privacy loopholes due to model opacity in AI-based fraud detection systems. The sustained adoption of digital wallets is heavily shaped by the interaction between users' digital literacy, platform reputation, and the clarity of data protection policies.*

Research limitations *– The limitations of this study include the absence of a formal quality appraisal regarding the methodology of each analyzed article and a relatively limited number of synthesized final literatures (n=19). Furthermore, variations in economic contexts and regulations across the studied countries potentially affect the results in their respective literatures.*

Implications *– Digital wallet providers are advised to focus not only on system encryption but also on communication transparency to users and striking a balance between security and usability. There is also an urgency for regulators to synchronize strong data protection regulations with systematic digital literacy education tailored to the risk profiles of specific user groups.*

Originality *– This study provides a synthesis of literature that was previously fragmented between theoretical technology adoption perspectives and technical cybersecurity infrastructure studies, holistically linking national data protection regulations with the security behaviors of digital wallet users.*

Keywords: *Data Security, Digital Risk, Digital Wallet, Systematic Literature Review, Perceived Security*

Histori Artikel:
Diterima: 17 Juni 2026, Direvisi: 8 Juli 2026, Disetujui: 11 Juli 2026, Dipublikasikan: 31 Juli 2026.

***Penulis Korespondensi:**
adindarahmadinna9@gmail.com

DOI:
https://doi.org/10.60036/jbm.1302

PENDAHULUAN

Perkembangan Transformasi digital telah mengubah lanskap sistem pembayaran global secara drastis dalam satu dekade terakhir, di mana integrasi *financial technology* menjadi penggerak utama dalam efisiensi ekonomi yang berkelanjutan di seluruh dunia (Rodriguez et al., 2026). Peningkatan adopsi dompet digital, terutama setelah pandemi COVID-19 berlangsung, telah menjadi instrumen strategis yang mengubah pola transaksi masyarakat menuju ekosistem non-tunai yang sangat masif guna mendukung perluasan inklusi keuangan global (Herget et al., 2021). Meskipun layanan pembayaran berbasis aplikasi ini berkembang sangat pesat di berbagai negara berkembang dan maju, tantangan mengenai aspek keamanan data dan privasi pengguna tetap menjadi masalah yang mendesak untuk segera diatasi oleh seluruh pemangku kepentingan. Fenomena integrasi teknologi finansial yang cepat ini memerlukan analisis mendalam terkait implikasi risiko keamanan siber dalam jangka panjang, terutama menyangkut ketahanan sistem yang harus mampu melindungi data pribadi nasabah dari berbagai potensi ancaman yang terus berkembang setiap waktu.

Pertumbuhan industri fintech yang sangat signifikan di berbagai kawasan, termasuk Asia dan Amerika Latin, membawa dampak positif bagi efisiensi transaksi, tetapi hal tersebut juga diiringi dengan meningkatnya ancaman keamanan siber yang nyata dan semakin canggih (Vásquez-Vásquez et al., 2026). Risiko kejahatan digital kini telah bergeser secara struktural dari ancaman fisik menuju serangan siber yang kompleks, seperti *phishing*, pencurian identitas digital, *malware*, hingga pengambilalihan akun pengguna yang terdaftar secara resmi pada sebuah platform (Jain et al., 2023). Pengguna yang tidak memiliki literasi risiko finansial yang mumpuni

serta pemahaman teknologi yang rendah sangat rentan terpapar oleh tindak kejahatan tersebut, sehingga perlindungan data pribadi menjadi faktor kritikal yang menentukan keberlanjutan bisnis fintech di masa depan (Nova et al., 2026). Pengelolaan risiko yang bersifat adaptif dan proaktif sangat diperlukan untuk melindungi kepentingan seluruh pengguna, mengingat kerugian finansial yang ditimbulkan dari kebocoran data dapat merusak reputasi penyedia layanan secara permanen di mata publik yang semakin waspada (Karangara & Manta, 2024).

Keamanan data menjadi aspek fundamental yang menentukan tingkat kepercayaan pengguna dalam bertransaksi, karena sistem transaksi digital melibatkan pertukaran informasi sensitif yang bersifat sangat pribadi dan rahasia bagi setiap individu (Presilia & Marwahdiyanti, 2025). Berbagai studi empiris menunjukkan bahwa penerapan autentikasi biometrik yang mutakhir, enkripsi *end-to-end*, dan tokenisasi transaksi merupakan standar yang sangat krusial guna memitigasi celah keamanan yang mungkin dimanfaatkan oleh pelaku kejahatan siber untuk menyusup ke dalam sistem pembayaran (Karangara & Manta, 2024). Penyedia layanan dompet digital dituntut untuk memberikan transparansi penuh mengenai kebijakan pengelolaan dan penyimpanan data kepada setiap nasabah, sehingga reputasi platform dapat terjaga dengan baik di tengah kompetisi industri yang sangat ketat (Karangara & Manta, 2024). Kepercayaan pengguna yang terbangun secara kuat melalui jaminan keamanan sistem akan berkontribusi langsung pada peningkatan loyalitas serta keberlanjutan penggunaan suatu aplikasi pembayaran dalam jangka waktu yang sangat panjang di masa mendatang (Javeed et al., 2026).

Namun, literatur terkini menunjukkan adanya kontradiksi yang cukup menarik dalam temuan perilaku adopsi teknologi pembayaran oleh pengguna saat ini, di mana beberapa studi menganggap bahwa aspek keamanan adalah penentu utama dalam memengaruhi niat penggunaan layanan (Karsim et al., 2024). Sebaliknya, penelitian lain menemukan bahwa persepsi keamanan tidak selalu berkorelasi secara signifikan terhadap keputusan adopsi, terutama pada kelompok generasi muda yang sering kali lebih mengutamakan kemudahan navigasi dan manfaat instan yang ditawarkan oleh aplikasi (Zuniatami & Mahardhika, 2025). Perbedaan temuan ini menunjukkan bahwa persepsi aman bersifat sangat subjektif bagi setiap individu, yang sangat dipengaruhi oleh tingkat literasi digital, latar belakang pendidikan, serta pengalaman buruk terkait gangguan sistem yang pernah dialami sebelumnya (Javeed et al., 2026). Kompleksitas perilaku pengguna yang beragam ini menuntut adanya kajian literatur lebih lanjut yang mampu menyatukan perspektif psikologi perilaku dengan infrastruktur keamanan teknologi informasi secara komprehensif (Rodriguez et al., 2026).

Kesenjangan penelitian (*research gap*) saat ini terletak pada kebutuhan mendesak untuk menyintesis bukti empiris yang ada, terkait bagaimana faktor risiko keamanan spesifik diinteraksikan dengan literasi digital dalam penggunaan sistem pembayaran yang semakin terintegrasi. Literatur yang berkembang saat ini cenderung terfragmentasi antara perspektif adopsi teknologi secara teoretis, dengan kajian teknis mengenai infrastruktur keamanan siber yang dilakukan secara terpisah tanpa melihat keterkaitannya (Zhao, 2025). Belum banyak sintesis sistematis yang mampu menghubungkan regulasi pelindungan data nasional dengan perilaku keamanan pengguna secara holistik, sehingga arah pengembangan kebijakan pelindungan data sering kali kurang tepat sasaran bagi kebutuhan masyarakat luas (Shahen & Sharaf, 2026). Keterbatasan sintesis inilah yang menjadi dasar urgensi dilakukannya penelitian melalui metode tinjauan sistematis, agar dapat memberikan gambaran utuh mengenai ekosistem pembayaran digital yang aman, efisien, dan tetap menjaga hak-hak privasi pengguna dalam dinamika ekonomi modern (Shahen & Sharaf, 2026).

Penelitian ini bertujuan untuk menjawab tantangan tersebut melalui pendekatan *Systematic Literature Review* (SLR) yang ketat, guna menyintesis faktor-faktor keamanan dan risiko penggunaan dompet digital berdasarkan data publikasi ilmiah terkini dari berbagai basis data bereputasi (Shahen & Sharaf, 2026; Vásquez-Vásquez et al., 2026). Kami berfokus pada pemetaan

tren riset yang menjawab tiga pertanyaan penelitian yang spesifik, yakni mengenai faktor keamanan data dominan, risiko siber yang signifikan bagi pengguna, serta interaksi persepsi aman bagi keberlanjutan adopsi (Javeed et al., 2026; Karsim et al., 2024). Penelitian ini diharapkan dapat memberikan panduan komprehensif bagi penyedia layanan dompet digital dalam merancang sistem yang lebih resilien, serta memberikan masukan berharga bagi regulator dalam menyusun kebijakan pelindungan data pribadi yang lebih inklusif dan adaptif. Sistematika sintesis dalam penelitian ini akan memperjelas posisi penelitian dalam diskursus teknologi finansial global yang sedang bergerak sangat dinamis seiring dengan perkembangan pesat kecerdasan buatan dalam deteksi penipuan (Shahen & Sharaf, 2026).

Adapun struktur penulisan artikel ini dimulai dari tinjauan metodologi pencarian artikel yang sangat ketat menggunakan pedoman PRISMA, yang kemudian dilanjutkan dengan analisis tematik hasil sintesis dari berbagai literatur ilmiah yang telah terpilih (Shahen & Sharaf, 2026). Pembahasan artikel akan mengelompokkan temuan utama untuk memetakan hubungan kausalitas antara keamanan sistem dan perilaku pengguna, sehingga *research gap* yang selama ini ada dapat terisi dengan argumen ilmiah yang sangat solid dan dapat dipertanggungjawabkan (Javeed et al., 2026; Vásquez-Vásquez et al., 2026). Di bagian akhir artikel, peneliti menyajikan simpulan, implikasi manajerial bagi penyedia layanan, serta saran bagi penelitian mendatang terkait arah pengembangan sistem pembayaran yang lebih aman, resilien, dan juga sangat tepercaya. Harapannya, artikel ini mampu memberikan kontribusi signifikan terhadap pengembangan ekosistem pembayaran digital di Indonesia yang tidak hanya berfokus pada inovasi teknologi, tetapi juga pada keamanan data masyarakat sebagai aset paling berharga dalam era ekonomi digital (Nova et al., 2026). Oleh karena itu, penelitian ini dilakukan untuk menyintesis bukti empiris terkait keamanan data dan risiko dompet digital guna menjawab pertanyaan penelitian berikut:

1. RQ1: Faktor-faktor keamanan data apa saja yang paling dominan memengaruhi kepercayaan pengguna dompet digital?
2. RQ2: Apa saja risiko keamanan digital yang paling signifikan diidentifikasi dalam literatur terkini?
3. RQ3: Bagaimana interaksi antara persepsi aman, literasi digital, dan reputasi platform membentuk keberlanjutan adopsi dompet digital?

METODE

Penelitian ini menggunakan pendekatan *Systematic Literature Review* (SLR) yang dirancang untuk memberikan tinjauan sistematis, transparan, dan dapat direproduksi atas literatur terkait keamanan dompet digital. Sebagai metodologi penelitian, pendekatan ini dipilih karena kemampuannya dalam mengumpulkan bukti empiris secara komprehensif, memetakan keadaan pengetahuan saat ini, dan memberikan dasar bagi agenda penelitian di masa depan (Snyder, 2019). Seluruh prosedur operasional dalam penelitian ini berpedoman pada protokol PRISMA 2020 (*Preferred Reporting Items for Systematic Reviews and Meta-Analyses*), yang memastikan bahwa proses identifikasi, penyaringan, hingga seleksi akhir dilakukan secara objektif (Page et al., 2021).

Tahap awal penelitian dimulai dengan perumusan pertanyaan penelitian yang tajam guna membatasi cakupan kajian agar tetap relevan dengan fenomena keamanan teknologi finansial. Peneliti menetapkan tiga pertanyaan utama yang akan dijawab melalui sintesis literatur, yaitu faktor keamanan dominan, risiko signifikan, serta interaksi persepsi aman. Perumusan ini sangat krusial dalam metodologi SLR karena menjadi acuan utama dalam menentukan kriteria inklusi dan eksklusi artikel yang akan dianalisis. Peneliti memposisikan tinjauan literatur ini bukan sekadar ringkasan, melainkan metodologi formal yang menuntut ketelitian dalam mengumpulkan dan menganalisis data sekunder agar validitas temuan tetap terjaga (Snyder, 2019).

Tahap identifikasi dilakukan melalui penelusuran pustaka pada basis data ilmiah Scopus, ScienceDirect, dan Google Scholar dengan rentang publikasi 2020–2026 (Booth et al., 2016).

Strategi pencarian menggunakan kata kunci kombinasi Boolean ("digital wallet" OR "e-wallet") AND ("data security" OR "perceived risk") guna menjaring artikel yang memiliki relevansi tematik tinggi dengan fokus penelitian. Penggunaan beberapa basis data ilmiah dilakukan untuk menjamin keberagaman sumber referensi serta memperluas cakupan studi yang relevan dengan isu keamanan transaksi digital di berbagai konteks regional (Kitchenham et al., 2009). Strategi ini memastikan bahwa semua artikel yang terjaring memiliki kontribusi teoretis atau empiris yang nyata terhadap topik yang diangkat.

Proses seleksi dilakukan melalui tahap *screening* judul dan abstrak untuk membuang duplikasi serta literatur yang tidak relevan dengan fokus keamanan data dan risiko digital. Peneliti melakukan pembersihan data dengan menghapus artikel duplikat menggunakan perangkat lunak bibliografi guna menjamin bahwa setiap unit analisis bersifat unik. Tahap ini dirancang secara sistematis untuk memisahkan literatur yang relevan dengan literatur yang tidak membahas topik keamanan siber secara spesifik, guna memastikan kualitas data yang akan disintesis tetap terjaga secara konsisten (Okoli, 2015). Kehati-hatian dalam tahap ini sangat penting untuk meminimalkan bias seleksi yang sering terjadi dalam peninjauan literatur tradisional.

Tahap kelayakan (*eligibility*) melibatkan pembacaan teks lengkap (*full-text*) dari setiap artikel yang telah lolos tahap penyaringan untuk menentukan kecocokan dengan tujuan riset. Kriteria inklusi utama mencakup artikel jurnal ilmiah yang membahas aspek keamanan data, persepsi risiko, serta perilaku adopsi dompet digital, dengan kriteria eksklusi bagi publikasi prosiding, buku, atau artikel yang tidak tersedia dalam akses penuh. Melalui proses penyaringan yang ketat ini, sebanyak 19 artikel ilmiah terpilih ditetapkan sebagai data primer untuk disintesis lebih lanjut. Snyder (2019) menekankan bahwa kriteria inklusi dan eksklusi yang ketat sangat penting dilakukan untuk menjaga fokus kajian literatur penelitian agar tidak melebar ke topik yang kurang relevan (Snyder, 2019).

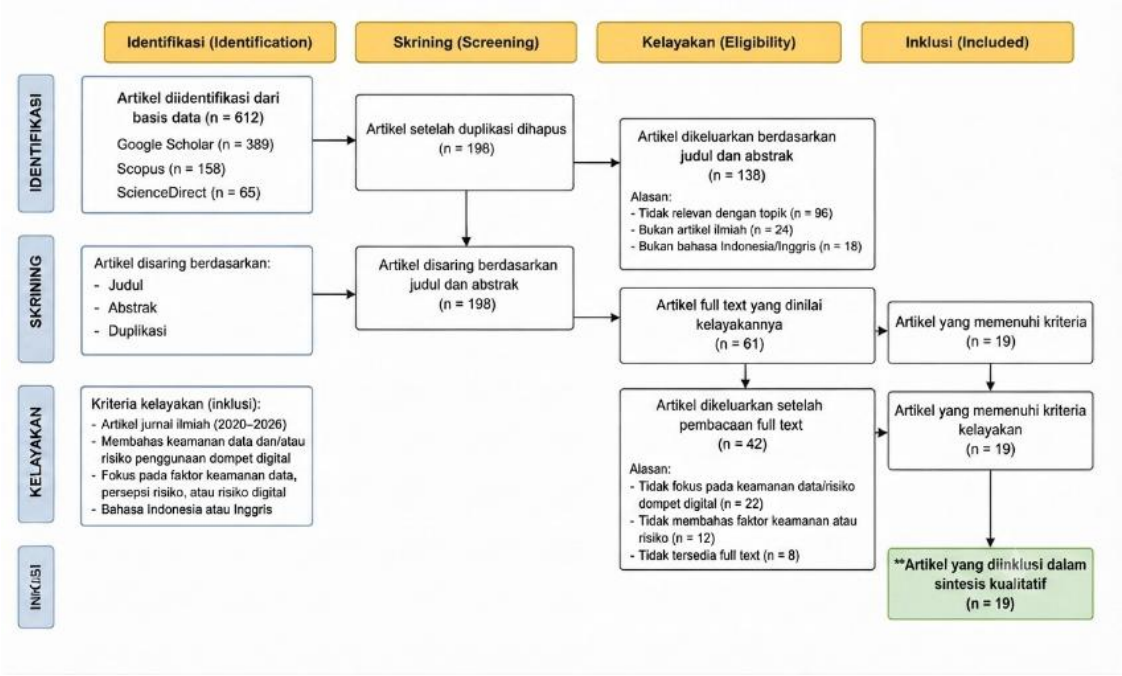
Setelah artikel terpilih, peneliti melakukan ekstraksi data menggunakan matriks sintesis yang mencakup variabel penulis, tahun, negara studi, metode penelitian, serta temuan utama terkait keamanan data dan risiko digital. Teknik analisis data yang digunakan adalah analisis tematik (*thematic analysis*) untuk mengelompokkan pola dan tema dominan dari hasil penelitian terdahulu secara sistematis (Braun & Clarke, 2012). Proses ekstraksi data ini menjadi kunci utama dalam menjamin *traceability*, di mana setiap klaim yang disajikan dalam bab pembahasan memiliki rujukan langsung dari subset artikel yang mendukungnya secara kredibel. Teknik ini memungkinkan peneliti untuk mengidentifikasi kesenjangan penelitian yang ada dalam literatur terkini.

Sebagai bentuk transparansi metodologis, peneliti mengakui beberapa keterbatasan dalam penelitian ini, terutama mengenai ketiadaan *quality appraisal* formal terhadap metodologi setiap artikel yang dianalisis (Kitchenham et al., 2009). Keterbatasan ini menuntut pembaca untuk mempertimbangkan temuan penelitian dengan penuh kehati-hatian, mengingat adanya variasi konteks ekonomi dan regulasi di setiap negara yang mungkin memengaruhi hasil penelitian di masing-masing literatur. Meskipun demikian, upaya telah dilakukan untuk meminimalkan bias seleksi dengan mengikuti protokol PRISMA 2020 secara konsisten di setiap tahapan penelitian guna memastikan hasil yang objektif (Page et al., 2021). Interpretasi terhadap temuan juga disesuaikan dengan keterbatasan jumlah literatur yang disintesis (n=19).

Seluruh tahapan penelitian mulai dari pencarian hingga ekstraksi data telah didokumentasikan dengan cermat untuk menjamin keterlacakan data (*traceability*) bagi pembaca. Upaya ini dilakukan agar hasil sintesis ini memiliki landasan argumen yang dapat dipertanggungjawabkan dalam diskursus akademik mengenai teknologi finansial global. Pendekatan ini diharapkan dapat memenuhi ekspektasi keterlacakan data dan memberikan kontribusi nyata bagi pengembangan literatur di masa depan yang lebih mendalam serta

terintegrasi. Struktur metodologi yang ketat ini menjadi fondasi bagi validitas hasil analisis tematik yang disajikan dalam bab berikutnya (Snyder, 2019).

Proses seleksi literatur dilakukan secara ketat untuk memastikan bahwa artikel yang dianalisis memiliki relevansi dan kualitas yang memenuhi standar penelitian sistematis. Tahapan ini didokumentasikan ke dalam diagram alur PRISMA 2020 untuk menjamin transparansi serta kemampuan telusur (*traceability*) bagi pembaca dalam memverifikasi setiap langkah pemilihan artikel dari tahap identifikasi hingga tahap inklusi akhir. Alur kerja sistematis tersebut diilustrasikan secara mendetail pada Gambar 1 berikut ini :



Gambar 1. Diagram PRISMA Seleksi Studi

Gambar 1 menunjukkan bahwa dari total 612 artikel yang berhasil diidentifikasi dari berbagai basis data ilmiah, sebanyak 19 artikel telah memenuhi seluruh kriteria inklusi untuk disintesis dalam penelitian ini. Proses eliminasi dilakukan secara objektif dengan mengeluarkan artikel yang tidak relevan, artikel duplikat, serta literatur yang tidak membahas secara spesifik mengenai keamanan data dan risiko digital pada dompet digital. Keseluruhan jumlah artikel akhir (n=19) ini menjadi sumber data primer yang digunakan untuk melakukan analisis tematik, sehingga temuan yang dihasilkan memiliki landasan empiris yang kuat dan dapat dipertanggungjawabkan secara akademik.

HASIL DAN PEMBAHASAN

Hasil

Penelitian ini menyintesis 19 artikel ilmiah terpilih (2020-2026) untuk memetakan faktor keamanan dan risiko penggunaan dompet digital. Untuk memastikan keterlacakan (*traceability*) dan memenuhi standar SLR, data dikelompokkan ke dalam karakteristik studi (Tabel 1) dan tema analisis utama.

Tabel 1. Ringkasan Karakteristik Studi (n=19)

Variabel	Distribusi	Artikel Terkait (Contoh)
Metode	Kuantitatif (8), Kualitatif/SLR (11)	Angel-Rodriguez et al. (2026); Nova et al. (2026)

Variabel	Distribusi	Artikel Terkait (Contoh)
Fokus	Keamanan Data (9), Risiko/Adopsi (10)	Javeed et al. (2026); Zuniatami & Mahardhika (2025)
Cakupan	Global (Asia, Eropa, Latin America)	Vásquez-Vásquez et al. (2026); Herget et al. (2021)

Sumber: Data diolah peneliti (2026)

Faktor Keamanan Data dan Teknologi Perlindungan

Sintesis literatur menunjukkan bahwa kepercayaan pengguna adalah variabel psikologis yang dimediasi oleh ketangguhan sistem keamanan. Penggunaan autentikasi biometrik, *two-factor authentication* (2FA), dan enkripsi *end-to-end* diidentifikasi sebagai standar teknis utama yang mampu menurunkan persepsi risiko. Nova et al. (2026) menegaskan bahwa tokenisasi data dan protokol TLS menjadi mekanisme krusial dalam memitigasi risiko pencurian data di tingkat server. Namun, terdapat variasi hasil mengenai pengaruh keamanan terhadap niat penggunaan; sementara beberapa studi menyatakan keamanan sebagai determinan utama, Zuniatami & Mahardhika (2025) justru menemukan bahwa pada segmen Gen Z di Indonesia, fitur keamanan yang terlalu ketat dapat dianggap sebagai hambatan kenyamanan jika tidak didukung antarmuka intuitif. Hal ini mengindikasikan bahwa persepsi keamanan dipengaruhi oleh keseimbangan antara fungsionalitas teknis dan pengalaman pengguna.

Lanskap Risiko Digital dan Tantangan Keamanan Siber

Risiko dalam penggunaan dompet digital kini berevolusi menjadi ancaman siber lintas batas yang mencakup *phishing*, pencurian identitas, *malware*, dan insiden pengambilalihan akun (*account takeover*). Zhao (2025) menyoroti risiko baru berupa *model opacity* pada sistem deteksi penipuan berbasis AI, yang sering kali menimbulkan celah privasi data yang tidak disadari oleh pengguna. Literatur juga menekankan bahwa kelemahan internal organisasi, seperti manajemen insiden yang buruk dan transparansi kebijakan privasi yang rendah, menjadi kerentanan yang sama signifikannya dengan ancaman eksternal. Temuan dari berbagai konteks ekonomi berkembang di Asia dan Amerika Latin secara konsisten menunjukkan bahwa institusi yang kurang matang secara regulasi menjadi faktor risiko kontekstual yang signifikan dalam menghambat adopsi dompet digital yang aman.

Literasi Risiko, Persepsi Aman, dan Keberlanjutan Adopsi

Analisis menunjukkan bahwa persepsi keamanan pengguna (*perceived security*) dibentuk oleh interaksi antara literasi digital dan transparansi platform. Literasi digital berfungsi sebagai mediator; pengguna dengan literasi yang lebih tinggi memiliki kecemasan siber yang lebih rendah dan lebih mampu mengidentifikasi upaya *social engineering*. Javeed et al. (2026) dan Vásquez-Vásquez et al. (2026) menyimpulkan bahwa reputasi platform dan kejelasan kebijakan perlindungan data pribadi adalah faktor yang paling efektif dalam membangun loyalitas pengguna jangka panjang. Hasil sintesis ini mempertegas bahwa keberlanjutan adopsi dompet digital bukan sekadar masalah inovasi teknologi, melainkan proses sosioteknis yang memerlukan integrasi antara edukasi publik, kepatuhan terhadap regulasi, dan penguatan sistem keamanan siber yang transparan.

Pembahasan

Sintesis terhadap 19 artikel yang dianalisis menegaskan bahwa keamanan data pada dompet digital merupakan fenomena sosioteknis yang kompleks, di mana teknologi perlindungan siber harus diimbangi dengan strategi manajemen risiko berbasis literasi pengguna. Secara teoretis, hasil ini mempertegas bahwa model adopsi teknologi tradisional seperti TAM atau UTAUT

perlu mengintegrasikan variabel "kepercayaan terintegrasi" (*trust-integrated framework*) sebagai variabel mediasi yang menentukan keberlanjutan penggunaan. Sejalan dengan studi Angel-Rodriguez et al. (2026), transisi dari transaksi berbasis tunai menuju dompet digital tidak bersifat linier, melainkan sangat bergantung pada persepsi risiko yang dirasakan masyarakat, khususnya di negara berkembang.

Lebih jauh, temuan mengenai lanskap risiko menunjukkan adanya pergeseran dari ancaman siber konvensional menuju tantangan yang lebih canggih seperti *model opacity* pada sistem deteksi penipuan yang diidentifikasi oleh Zhao (2025). Hal ini menuntut adanya pergeseran paradigma dalam tata kelola keamanan perusahaan; dari model keamanan yang bersifat statis menuju model yang adaptif dan *context-aware*. Kesenjangan yang ditemukan menunjukkan bahwa penyedia dompet digital sering kali terjebak dalam *trade-off* antara kemudahan penggunaan (*usability*) dan keamanan, yang justru membuka celah bagi serangan rekayasa sosial karena pengguna merasa terbebani oleh prosedur keamanan yang terlalu kompleks, sebagaimana diulas oleh Javeed et al. (2026).

Implikasi penting dari penelitian ini adalah perlunya sinkronisasi antara regulasi perlindungan data yang kuat dan edukasi literasi digital yang sistematis. Temuan mengenai peran literasi sebagai mediator menunjukkan bahwa edukasi tidak boleh bersifat seragam, melainkan harus disesuaikan dengan profil risiko kelompok pengguna, selaras dengan temuan Zuniatami & Mahardhika (2025) mengenai perbedaan respon antar antargenerasi. Strategi mitigasi yang diusulkan dalam literatur tidak hanya berfokus pada enkripsi sistem, tetapi juga pada transparansi komunikasi kepada pengguna mengenai bagaimana data mereka dilindungi, sebuah aspek yang ditekankan oleh Vásquez-Vásquez et al. (2026) sebagai kunci loyalitas.

Terakhir, keberhasilan ekosistem pembayaran digital di berbagai konteks regional memberikan pelajaran bahwa faktor institusional dan regulasi nasional berperan sebagai *enabler* utama bagi keamanan transaksi. Penelitian di masa depan, sebagaimana disarankan oleh Nova et al. (2026), perlu mengeksplorasi bagaimana kecerdasan buatan dapat digunakan untuk mempersonalisasi edukasi keamanan bagi pengguna secara *real-time*. Secara keseluruhan, pembahasan ini menegaskan bahwa keamanan dompet digital adalah upaya kolektif yang memerlukan sinergi antara penyedia platform, regulator, dan tingkat literasi digital masyarakat luas

SIMPULAN

Penggunaan sintesis terhadap 19 artikel yang dianalisis menegaskan bahwa keamanan data pada dompet digital merupakan fenomena sosioteknis yang kompleks, di mana teknologi perlindungan siber harus diimbangi dengan strategi manajemen risiko berbasis literasi pengguna. Secara teoretis, hasil ini mempertegas bahwa model adopsi teknologi tradisional seperti TAM atau UTAUT perlu mengintegrasikan variabel "kepercayaan terintegrasi" (*trust-integrated framework*) sebagai variabel mediasi yang menentukan keberlanjutan penggunaan. Sejalan dengan studi Angel-Rodriguez et al. (2026), transisi dari transaksi berbasis tunai menuju dompet digital tidak bersifat linier, melainkan sangat bergantung pada persepsi risiko yang dirasakan masyarakat, khususnya di negara berkembang.

Lebih jauh, temuan mengenai lanskap risiko menunjukkan adanya pergeseran dari ancaman siber konvensional menuju tantangan yang lebih canggih seperti *model opacity* pada sistem deteksi penipuan yang diidentifikasi oleh Zhao (2025). Hal ini menuntut adanya pergeseran paradigma dalam tata kelola keamanan perusahaan; dari model keamanan yang bersifat statis menuju model yang adaptif dan *context-aware*. Kesenjangan yang ditemukan menunjukkan bahwa penyedia dompet digital sering kali terjebak dalam *trade-off* antara kemudahan penggunaan (*usability*) dan keamanan, yang justru membuka celah bagi serangan rekayasa sosial karena pengguna merasa

terbebani oleh prosedur keamanan yang terlalu kompleks, sebagaimana diulas oleh Javeed et al. (2026).

Implikasi penting dari penelitian ini adalah perlunya sinkronisasi antara regulasi perlindungan data yang kuat dan edukasi literasi digital yang sistematis. Temuan mengenai peran literasi sebagai mediator menunjukkan bahwa edukasi tidak boleh bersifat seragam, melainkan harus disesuaikan dengan profil risiko kelompok pengguna, selaras dengan temuan Zuniatami & Mahardhika (2025) mengenai perbedaan respons antargenerasi. Strategi mitigasi yang diusulkan dalam literatur tidak hanya berfokus pada enkripsi sistem, tetapi juga pada transparansi komunikasi kepada pengguna mengenai bagaimana data mereka dilindungi, sebuah aspek yang ditekankan oleh Vásquez-Vásquez et al. (2026) sebagai kunci loyalitas.

Terakhir, keberhasilan ekosistem pembayaran digital di berbagai konteks regional memberikan pelajaran bahwa faktor institusional dan regulasi nasional berperan sebagai *enabler* utama bagi keamanan transaksi. Penelitian di masa depan, sebagaimana disarankan oleh Nova et al. (2026), perlu mengeksplorasi bagaimana kecerdasan buatan dapat digunakan untuk mempersonalisasi edukasi keamanan bagi pengguna secara *real-time*. Secara keseluruhan, pembahasan ini menegaskan bahwa keamanan dompet digital adalah upaya kolektif yang memerlukan sinergi antara penyedia platform, regulator, dan tingkat literasi digital masyarakat luas.

DAFTAR PUSTAKA

Ahmad, I., Noreen, R., Khalid, T., & Amjad, F. (2026). Balancing innovation and cybersecurity: Exploring digital risks in FinTech adoption. *Contemporary Review of Social Sciences Research*.

Angel-Rodriguez, P., & Vicente-Pascual, J. A. (2026). Exploring the adoption of mobile payments: A hybrid literature review and future research agenda. *Future Business Journal*. https://doi.org/10.1186/s43093-025-00712-6

Booth, A., Sutton, A., & Papaioannou, D. (2016). *Systematic approaches to a successful literature review* (2nd ed.). Sage Publications.

Braun, V., & Clarke, V. (2012). Thematic analysis. In H. Cooper (Ed.), *APA handbook of research methods in psychology* (Vol. 2, pp. 57–71). American Psychological Association.

Dahlberg, T., Guo, J., & Ondrus, J. (2015). A critical review of mobile payment research. *Electronic Commerce Research and Applications, 14*(5), 265–284.

Featherman, M. S., & Pavlou, P. A. (2003). Predicting e-services adoption: A perceived risk facets perspective. *International Journal of Human-Computer Studies, 59*(4), 451–474.

Güngördü Belbağ, A. (2026). Mobile payment adoption during the COVID-19 pandemic: A systematic literature review. *Journal of Financial Services Marketing*.

Herget, N., Krey, P. S., & Caccamo, M. (2021). Mobile payment adoption during the COVID-19 pandemic in Germany. *Digitala Vetenskapliga Arkivet*, May, 1–94. http://hj.diva-portal.org/smash/get/diva2:1559437/FULLTEXT01.pdf

Jain, R., Kumar, S., Sood, K., Grima, S., & Rupeika-Apoga, R. (2023). A systematic literature review of the risk landscape in fintech. *Risks, 11*(2). https://doi.org/10.3390/risks11020036

Javeed, A., Elghuweel, M. E., & Khan, M. Y. (2026). Beyond convenience and security: A trust-integrated framework for digital wallet adoption. *Future Business Journal, 12*(143), 16. https://doi.org/10.1186/s43093-026-00845-2

Karangara, R., & Manta, O. (2024). Cybersecurity & data privacy in fintech. *Preprints*. https://doi.org/10.20944/preprints202401.2194.v2

Karsim, K., Rini, R., Ronaldo, R., Anam, S., & Judijanto, L. (2024). The perception of security and risk, ease of use, and benefits are the determining factors in adopting a digital wallet. *Journal of Management: Small and Medium Enterprises (SMEs), 17*(2), 525–535.

Kitchenham, B., Brereton, P., Budgen, D., Turner, M., Bailey, J., & Linkman, S. (2009). Systematic literature reviews in software engineering – A systematic literature review. *Information and Software Technology, 51*(1), 7–15. https://doi.org/10.1016/j.infsof.2008.09.009

Lestari, F. T., & Hidayati, S. A. (2026). The influence of trust in fintech and perceived security on the decision to use e-wallets among students in Mataram City. *Al-Kharaj: Journal of Islamic Economic and Business*.

Lim, C. Y. (2025). *The mediating effect of trust on factors influencing the intention to use FinTech applications among urban working professionals in Malaysia* [Unpublished manuscript/thesis]. University of Wales Trinity Saint David.

Makri, M. (2026). Digital payment adoption among higher education students in India: A systematic literature review. *Diginomics*.

Nova, N. I., Nabila, S., Paiza, P. R., & Sinaga, N. (2026). Analisis keamanan sistem pembayaran digital terhadap perlindungan data pengguna. *RIGGS: Journal of Artificial Intelligence and Digital Business, 4*(4), 8985–8991. https://doi.org/10.31004/riggs.v4i4.5119

Okoli, C. (2015). A guide to conducting a standalone systematic literature review. *Communications of the Association for Information Systems, 37*(1), 879–910.

Oliveira, T., Thomas, M., Baptista, G., & Campos, F. (2016). Mobile payment: Understanding the determinants of customer adoption and intention to recommend the technology. *Computers in Human Behavior, 61*, 404–414. https://doi.org/10.1016/j.chb.2016.03.030

Padma Kiran, K., & Vedala, N. S. (2025). Exploring behavioral intentions of consumers towards different digital payment services through the interplay of perceived risks and adoption factors. *Humanities and Social Sciences Communications*. https://doi.org/10.1057/s41599-025-05468-6

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., et al. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *BMJ, 372*, n71. https://doi.org/10.1136/bmj.n71

Pizzan-Tomanguillo, N. P., & Pereyra-Gonzales, T. V. (2024). Evolution and trends in digital wallet research: A bibliometric analysis in Scopus and Web of Science. *Publications, 12*(4).

Presilia, P. Y., & Marwahdiyanti, F. (2025). The influence of system security technology and data privacy on user trust and satisfaction in digital wallet applications: Systematic literature review. *[Nama Jurnal Tidak Diketahui], 1*(1), 42–52.

Rajpal, S., & Manglani, A. (2026). Drivers of FinTech adoption: Insights from a global review of recent literature. *Accounting Research Journal*.

Rodriguez, P. A., Antonio, J., Pascual, V., Shahen, A. M., Sharaf, M. F., Javeed, A., Elghuweel, M. E., Khan, M. Y., Tinggi, S., Ekonomi, I., Prasetya, E., Behavior, F., Nova, N. I., Nabila, S., Paiza, P. R., Sinaga, N., Vásquez-Vásquez, L. M., Alvarado-Cáceres, E. J., Caicedo-Mendoza, J. A., … Rupeika-Apoga, R. (2026). Cybersecurity & data privacy in fintech. *Journal of Risk and Financial Management, 17*(2), 1–29. https://doi.org/10.31004/riggs.v4i4.5119

Shahen, A. M., & Sharaf, M. F. (2026). Digital payments as a conceptual pathway linking COVID-19 and financial inclusion: A PRISMA-based systematic review and bibliometric analysis. *Journal of Theoretical and Applied Electronic Commerce Research, 21*(4), 1–29.

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research, 104*, 333–339. https://doi.org/10.1016/j.jbusres.2019.07.039

Vásquez-Vásquez, L. M., Alvarado-Cáceres, E. J., Caicedo-Mendoza, J. A., & Fernández-Bedoya, V. H. (2026). From cash to digital wallets: A PRISMA-based systematic review of microentrepreneur adoption in Asia and Latin America. *Journal of Risk and Financial Management, 19*(3), 1–29. https://doi.org/10.3390/jrfm19030232

Zhao, B. (2025). FinTech and risk management: Exploring opportunities, challenges, and regulatory responses. *SHS Web of Conferences, 225*, 02024.