Vol 6, No.1, Februari 2026

Faculty of Economics and Business

Review of Applied Accounting Research

http://jurnalnasional.ump.ac.id/index.php/RAAR/

IMPLEMENTASI DAN EVALUASI KEAMANAN BIOMETRIK DALAM SISTEM PEMBAYARAN DIGITAL: STUDI KASUS FINGERPRINT DAN PENGENALAN WAJAH

Syamsul Bakhtiar[1], Juli Riyanto Tri Wijaya[2], Muhammad Rizqi Alriansyah Manurung[3]*, Nurul Hidayah[4]

Affiliation:
[1]Program Studi Magister Akuntansi Fakultas Ekonomi dan Bisnis, Universitas Jenderal Soedirman
[2]Program Studi Akuntansi Fakultas Ekonomi dan Bisnis, Universitas Pancasakti Tegal
[3]Program Studi Akuntansi Fakultas Ekonomi dan Bisnis, Universitas Muhammadiyah Gresik
[4]Program Studi Akuntansi Fakultas Ekonomi dan Bisnis, Universitas Muhammadiyah Cirebon

***Correspondence*:**
muhammad.rizqialriansyah@umg.ac.id

ABSTRAK
Perkembangan pembayaran digital di Indonesia (dompet digital dan mobile banking) meningkatkan penggunaan autentikasi biometrik (fingerprint dan pengenalan wajah) untuk login dan otorisasi transaksi. Namun, literatur sistem informasi dan fintech masih banyak memperlakukan biometrik sebagai fitur yang generik, sehingga bukti empiris tentang bagaimana kualitas implementasi biometrik yang dirasakan pengguna membentuk kepercayaan dan memengaruhi evaluasi keamanan dalam konteks Indonesia masih terbatas. Studi ini mengintegrasikan Technology Acceptance Model (TAM) (kualitas sistem/kemudahan autentikasi) dan trust–risk framework (kepercayaan sebagai mekanisme penurun persepsi risiko) untuk memodelkan hubungan implementasi biometrik, kepercayaan pengguna, dan evaluasi keamanan. Data dikumpulkan melalui survei kuantitatif terhadap 100 pengguna pembayaran digital di Indonesia yang mengaktifkan autentikasi biometrik, menggunakan skala Likert 1–5, dan dianalisis dengan PLS-SEM (SmartPLS). Hasil menunjukkan implementasi biometrik berpengaruh positif signifikan terhadap evaluasi keamanan (β=0,473; p<0,001) dan kepercayaan pengguna juga berpengaruh positif signifikan (β=0,435; p<0,001), dengan daya jelaskan model yang kuat (R^2=0,762). Kontribusi teoretis penelitian ini menegaskan peran implementasi biometrik sebagai security assurance dalam kerangka TAM–trust–risk pada konteks negara berkembang, serta memberi implikasi praktis bagi tata kelola keamanan dan perlindungan data biometrik di Indonesia.
Kata kunci: Biometrik, Pembayaran Digital, Keamanan Sistem, Fingerprint, Pengenalan Wajah

PENDAHULUAN

Perkembangan teknologi digital telah mendorong transformasi besar dalam sistem pembayaran, dari yang awalnya berbasis uang tunai menjadi sistem pembayaran digital yang lebih cepat, efisien, dan dapat diakses kapan saja. Seiring dengan meningkatnya penggunaan dompet digital, e-wallet, dan layanan mobile banking, kebutuhan akan sistem keamanan yang lebih andal pun semakin mendesak. Dalam konteks ini, teknologi biometrik seperti fingerprint (sidik jari) dan pengenalan wajah (face recognition) menjadi solusi yang

Office Address:
Jl. K.H. Ahmad Dahlan, Dukuhwaluh, Kec. Kembaran, Kabupaten Banyumas, Jawa Tengah 53182

e-ISSN : 2807-8969

© 2021 raar. all rights reserved

mutakhir dan dianggap mampu meningkatkan lapisan keamanan dalam proses otentikasi pengguna (Hartono et al., 2022; Yu et al., 2025). Teknologi biometrik memungkinkan verifikasi identitas yang lebih akurat karena berbasis pada karakteristik fisik unik dari setiap individu, sehingga sulit untuk dipalsukan atau digunakan oleh pihak yang tidak berwenang.

Meskipun adopsi teknologi biometrik dalam sistem pembayaran digital terus meningkat, persoalan keamanan dan keandalan teknologi ini masih menjadi perdebatan di berbagai kalangan. Penelitian oleh Cho et al. (2024) menunjukkan bahwa sistem pengenalan biometrik dapat mengalami ancaman berupa spoofing, yaitu pemalsuan data biometrik seperti sidik jari palsu atau rekayasa citra wajah. Oleh karena itu, penerapan sistem ini harus disertai dengan evaluasi keamanan yang ketat untuk memastikan bahwa data pribadi pengguna terlindungi dengan baik dan tidak rentan terhadap kebocoran atau penyalahgunaan. Budiman et al. (2025) menekankan bahwa dalam dunia digital, risiko kebocoran data semakin meningkat, terutama dalam sistem yang menangani data sensitif seperti rekam medis dan biometrik. Dengan demikian, penguatan keamanan sistem biometrik dalam aplikasi pembayaran digital menjadi krusial, baik dari sisi teknis maupun kebijakan perlindungan data.

Studi sebelumnya yang dilakukan oleh Mahadini et al. (2024) membuktikan bahwa sistem fingerprint telah digunakan secara luas dalam sistem administrasi layanan kesehatan, seperti identifikasi pasien BPJS, yang dinilai mampu mempercepat proses layanan sekaligus menghindari duplikasi data. Namun demikian, penggunaan fingerprint dalam konteks sistem pembayaran digital menuntut standar keamanan yang lebih tinggi karena berkaitan langsung dengan transaksi keuangan. Sementara itu, teknologi pengenalan wajah juga mengalami peningkatan pemanfaatan dalam berbagai sektor, termasuk perbankan dan fintech. Menurut Setiyawan & Tjahyanti (2024), efektivitas sistem pengenalan wajah dapat ditingkatkan melalui teknik pengolahan citra untuk mengurangi kesalahan verifikasi. Akan tetapi, perlu evaluasi menyeluruh terhadap keandalannya, terutama dalam berbagai kondisi pencahayaan dan sudut wajah pengguna.

Dari sudut pandang pengguna, kepercayaan terhadap sistem biometrik sangat dipengaruhi oleh sejauh mana privasi dan data mereka terlindungi. Siti Khoiriah et al. (2025) dalam studinya menjelaskan bahwa keamanan dan privasi merupakan isu utama dalam keuangan digital. Penggunaan biometrik tanpa jaminan keamanan yang memadai dapat memicu ketidakpercayaan masyarakat terhadap layanan pembayaran digital. Untuk itu, penting dilakukan evaluasi terhadap infrastruktur keamanan, algoritma pendeteksi ancaman, serta sistem enkripsi yang digunakan dalam penyimpanan dan transmisi data biometrik. Tidak hanya itu, partisipasi aktif dari regulator dan penyedia layanan juga diperlukan dalam membangun sistem yang transparan dan bertanggung jawab (Rengganis & Susanto, 2023).

Penerapan sistem keamanan berbasis biometrik dalam aplikasi digital payment seperti dompet elektronik dan sistem pembayaran berbasis QR Code (QRIS) juga memerlukan pendekatan desain sistem yang adaptif terhadap kebutuhan pengguna. Menurut Muninggar & Rahardiansah (2024), integrasi teknologi QRIS dan sistem otentikasi biometrik dapat mendorong efisiensi pembayaran sekaligus meningkatkan keamanan. Hal ini menjadi semakin penting dalam konteks digitalisasi keuangan di Indonesia yang mengalami percepatan pesat, seiring dengan meningkatnya transaksi non-tunai dan meningkatnya jumlah pengguna aktif dompet digital (Lira, 2025; Setiyawan, 2024). Namun demikian, meskipun teknologi terus berkembang, banyak tantangan praktis dalam implementasi, seperti biaya infrastruktur, interoperabilitas perangkat, serta literasi digital masyarakat.

Meskipun hubungan antara implementasi biometrik, kepercayaan pengguna, dan evaluasi keamanan telah banyak dibahas dalam literatur sistem informasi dan fintech, studi-studi sebelumnya umumnya menempatkan biometrik sebagai "fitur" yang bersifat generik dan kurang membedakan kualitas implementasi (misalnya akurasi autentikasi, mekanisme anti-spoofing/liveness detection, prosedur fallback saat autentikasi gagal, serta perlindungan data biometrik). Selain itu, temuan empiris di negara berkembang dengan tingkat adopsi pembayaran digital yang tinggi dan karakteristik risiko siber yang khas masih relatif terbatas, khususnya dalam konteks ekosistem pembayaran digital Indonesia yang melibatkan beragam penyedia layanan, variasi desain kontrol keamanan, serta ekspektasi pengguna terhadap privasi dan keamanan. Oleh karena itu, kebutuhan riset bukan lagi sekadar menguji apakah biometrik "ada" atau "tidak ada", melainkan bagaimana implementasi biometrik yang dirasakan pengguna membentuk mekanisme psikologis berupa kepercayaan dan pada akhirnya memengaruhi evaluasi keamanan sistem pembayaran digital.

Berdasarkan gap tersebut, kontribusi baru penelitian ini terletak pada tiga hal. Pertama, penelitian ini memposisikan kepercayaan pengguna sebagai mekanisme (mediator) yang menjelaskan bagaimana implementasi biometrik diterjemahkan menjadi evaluasi keamanan, sehingga memperkaya pemahaman kausal (bukan sekadar hubungan langsung) dalam konteks pembayaran digital. Kedua, penelitian ini menekankan aspek kualitas implementasi biometrik (fingerprint dan/atau face recognition) sebagai konstruk yang lebih operasional dan relevan bagi desain kontrol keamanan, sehingga hasilnya dapat diturunkan menjadi rekomendasi teknis yang konkret. Ketiga, secara praktis penelitian ini menawarkan implikasi tata kelola keamanan untuk penyedia layanan dan pemangku kepentingan (misalnya kebijakan penguatan autentikasi, mitigasi spoofing, proteksi data biometrik, serta kontrol audit dan kepatuhan), sehingga temuan tidak hanya berkontribusi pada literatur akademik fintech, tetapi juga pada penguatan pengendalian dan akuntabilitas keamanan sistem pembayaran digital di Indonesia.

Berdasarkan paparan tersebut, penelitian ini dilakukan dengan tujuan untuk mengetahui bagaimana implementasi dan evaluasi keamanan pada sistem pembayaran digital dengan fokus pada penggunaan teknologi fingerprint dan pengenalan wajah. Penelitian ini akan mengkaji proses penerapan teknologi biometrik dalam sistem pembayaran digital, mengevaluasi tingkat keamanan yang ditawarkan, serta menilai potensi risiko dan kelemahan sistem tersebut. Dengan pendekatan studi kasus, penelitian ini diharapkan dapat memberikan gambaran empiris mengenai efektivitas, efisiensi, dan keandalan sistem biometrik dalam menghadirkan solusi pembayaran digital yang aman dan terpercaya. Selain itu, penelitian ini juga bertujuan untuk memberikan rekomendasi praktis bagi pengembang aplikasi, pembuat kebijakan, dan institusi keuangan terkait optimalisasi sistem biometrik untuk keamanan transaksi digital.

Dengan meningkatnya ancaman kejahatan digital seperti pencurian identitas dan penipuan online, studi ini menjadi sangat relevan untuk mendukung penguatan sistem keamanan digital di Indonesia. Rachman & Biduri (2023) menekankan pentingnya pengendalian fraud di era digital melalui penerapan teknologi berbasis otentikasi yang kuat. Di samping itu, Prayitno & Sinosi (2024) menyoroti pentingnya peran pengendalian internal berbasis teknologi dalam mendeteksi dan mencegah penipuan. Oleh karena itu, implementasi fingerprint dan pengenalan wajah dalam sistem pembayaran digital tidak hanya berperan sebagai fitur tambahan, tetapi juga sebagai komponen strategis dalam mendukung integritas sistem keuangan digital nasional. Penelitian ini diharapkan dapat memberikan kontribusi

ilmiah dan praktis terhadap pengembangan sistem pembayaran digital yang aman, inklusif, dan berkelanjutan.

TINJAUAN LITERATUR

Perkembangan sistem pembayaran digital mendorong inovasi dalam metode otentikasi yang lebih aman dan efisien. Salah satu pendekatan mutakhir yang banyak diterapkan adalah teknologi biometrik, seperti fingerprint dan pengenalan wajah. Sistem ini menggunakan karakteristik biologis pengguna sebagai pengenal unik, menggantikan metode tradisional seperti password atau PIN yang rentan terhadap peretasan dan pencurian data (Hartono et al., 2022; Yu et al., 2025).

Penelitian ini membangun kerangka teoretis dengan mengintegrasikan perspektif Technology Acceptance Model (TAM) dan trust–risk framework pada sistem informasi/fintech. Dalam perspektif TAM, desain fitur autentikasi yang meminimalkan friksi transaksi (misalnya autentikasi cepat tanpa mengingat PIN/password) dipahami sebagai elemen kualitas sistem yang meningkatkan pengalaman penggunaan dan penerimaan teknologi. Namun, pada konteks pembayaran digital yang berisiko tinggi, penerimaan tidak cukup dijelaskan oleh aspek utilitarian saja; karena itu, penelitian ini juga menggunakan trust–risk framework yang menempatkan kepercayaan pengguna sebagai mekanisme psikologis kunci yang terbentuk melalui sinyal jaminan keamanan (assurance) dari penyedia layanan, serta melalui persepsi pengguna atas pengelolaan privasi dan data sensitif. Dengan demikian, Implementasi Biometrik (X1) diposisikan sebagai bentuk security assurance (misalnya akurasi autentikasi, perlindungan data biometrik, dan mitigasi spoofing), Kepercayaan Pengguna (X2) sebagai keyakinan terhadap kompetensi–integritas–benevolence penyedia layanan, dan Evaluasi Keamanan (Y) sebagai penilaian pengguna terhadap tingkat perlindungan dan pengurangan risiko pada sistem pembayaran digital.

Berdasarkan kerangka tersebut, hubungan antar-variabel dalam model penelitian dapat dijelaskan secara kausal, bukan sekadar normatif. Implementasi biometrik yang dipersepsikan semakin baik akan meningkatkan keyakinan pengguna bahwa proses autentikasi dan perlindungan data dilakukan secara memadai, sehingga menaikkan evaluasi keamanan secara langsung (jalur X1→Y). Pada saat yang sama, implementasi biometrik juga berperan sebagai sinyal jaminan struktural (structural assurance) yang membangun kepercayaan pengguna terhadap sistem dan penyedia layanan (jalur X1→X2). Kepercayaan ini selanjutnya memperkuat penilaian bahwa sistem aman, karena pengguna meyakini adanya kemampuan dan komitmen penyedia layanan dalam menjaga privasi, mencegah akses tidak sah, serta menangani insiden keamanan secara bertanggung jawab (jalur X2→Y). Dengan logika ini, kepercayaan pengguna berpotensi menjadi mediator yang menjelaskan bagaimana kualitas implementasi biometrik diterjemahkan menjadi evaluasi keamanan, sehingga pengujian hipotesis tidak hanya menguji hubungan langsung, tetapi juga mekanisme penjelas yang mendasarinya.

Menurut Cho et al. (2024), teknologi biometrik memberikan keuntungan signifikan dalam hal kenyamanan dan keamanan. Namun, sistem ini tidak sepenuhnya bebas dari risiko. Salah satu ancaman yang paling sering terjadi adalah spoofing, yaitu pemalsuan data biometrik untuk mengakses sistem secara ilegal. Oleh karena itu, penting bagi pengembang dan penyedia layanan untuk melengkapi sistem biometrik dengan fitur keamanan tambahan, seperti deteksi liveness dan enkripsi data biometrik, untuk mencegah akses tidak sah terhadap informasi sensitif.

Dalam konteks implementasi, studi oleh Mahadini et al. (2024) menunjukkan bahwa penggunaan fingerprint dalam sistem layanan kesehatan seperti BPJS telah membantu meningkatkan efisiensi dan akurasi verifikasi pasien. Hal ini menunjukkan potensi besar biometrik untuk diterapkan dalam sektor lain, termasuk sistem pembayaran digital. Namun, penerapan biometrik di sektor keuangan tentu memerlukan evaluasi risiko yang lebih kompleks, karena melibatkan akses terhadap data finansial dan transaksi bernilai ekonomi tinggi.

Studi Setiyawan & Tjahyanti (2024) menyoroti peran teknik pengolahan citra dalam meningkatkan akurasi pengenalan wajah. Penelitian ini menekankan bahwa pengenalan wajah dapat memberikan hasil verifikasi yang tinggi jika disertai dengan sistem pemrosesan gambar yang baik, seperti pengaturan pencahayaan, sudut pandang, dan resolusi kamera. Hal ini penting, mengingat kegagalan dalam mengenali wajah pengguna dapat berdampak langsung pada kecepatan dan kenyamanan dalam bertransaksi secara digital.

Dari sisi perlindungan data, Budiman et al. (2025) mengingatkan bahwa sistem biometrik harus dirancang dengan keamanan data sebagai prioritas utama. Risiko kebocoran data biometrik dapat berdampak lebih serius dibandingkan data lain, karena karakteristik biometrik seperti sidik jari dan wajah tidak bisa diubah seperti halnya password. Oleh karena itu, pendekatan berbasis privacy by design perlu diterapkan dalam pengembangan sistem pembayaran digital berbasis biometrik.

Lebih lanjut, Siti Khoiriah et al. (2025) menegaskan pentingnya kesadaran dan kepercayaan pengguna terhadap sistem digital berbasis biometrik. Keamanan bukan hanya soal teknologi, tetapi juga melibatkan faktor psikologis dan sosial. Pengguna harus diyakinkan bahwa data biometrik mereka tidak akan disalahgunakan, dan bahwa sistem yang mereka gunakan benar-benar aman. Kepercayaan pengguna ini sangat menentukan keberhasilan adopsi teknologi baru di masyarakat.

Menurut Muninggar & Rahardiansah (2024), integrasi sistem pembayaran digital dengan teknologi QRIS dan biometrik dapat meningkatkan efisiensi sekaligus menjaga keamanan transaksi. Namun, perlu ada pengujian menyeluruh terhadap kompatibilitas perangkat, kecepatan respons sistem, dan resistensi terhadap serangan siber sebelum sistem ini diterapkan secara luas. Hal serupa juga diungkapkan oleh Lira (2025), yang mencatat bahwa adopsi digital banking di sektor syariah juga menghadapi tantangan dalam penerapan teknologi pengenalan identitas berbasis biometrik, terutama dalam hal kesiapan infrastruktur dan literasi digital masyarakat.

Sementara itu, dari sisi regulasi dan pengawasan, Rengganis & Susanto (2023) menyoroti perlunya evaluasi terhadap sistem anti-money laundering (AML) yang mengandalkan teknologi digital. Sistem pembayaran yang menggunakan biometrik perlu terintegrasi dengan kebijakan keamanan nasional agar dapat mendeteksi dan mencegah aktivitas ilegal, termasuk pencucian uang dan penipuan. Penelitian Prayitno & Sinosi (2024) juga mendukung hal ini dengan menyebutkan bahwa pengendalian internal berbasis teknologi sangat penting dalam deteksi fraud di era digital.

Dengan mempertimbangkan berbagai studi tersebut, dapat disimpulkan bahwa implementasi dan evaluasi teknologi biometrik dalam sistem pembayaran digital memerlukan pendekatan multidimensi, mencakup aspek teknis, keamanan data, kepercayaan pengguna, kesiapan infrastruktur, dan dukungan kebijakan. Fingerprint dan

pengenalan wajah bukan hanya alat otentikasi, tetapi juga merupakan bagian integral dari ekosistem keamanan digital masa depan.

METODE PENELITIAN

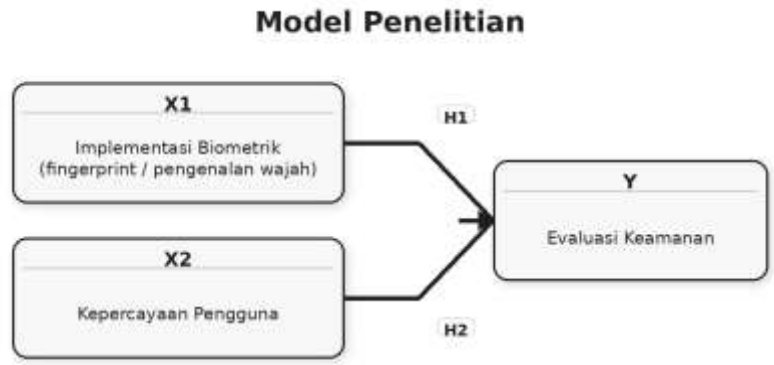
Penelitian ini menggunakan pendekatan kuantitatif dengan metode survei, di mana data primer diperoleh melalui penyebaran kuesioner kepada 100 responden yang memiliki pengalaman menggunakan sistem pembayaran digital berbasis biometrik, seperti fingerprint dan pengenalan wajah. Instrumen penelitian disusun dalam bentuk pernyataan tertutup dengan skala Likert 1–5, dari "sangat tidak setuju" hingga "sangat setuju". Penelitian ini mengkaji tiga variabel utama, yaitu implementasi teknologi biometrik (X1) sebagai variabel independen, kepercayaan pengguna (X2) sebagai variabel independen, dan evaluasi keamanan sistem pembayaran digital (Y) sebagai variabel dependen. Setiap variabel diukur melalui beberapa indikator yang dikembangkan dari teori dan studi terdahulu. Instrumen penelitian disusun dalam bentuk pernyataan tertutup menggunakan skala Likert 1–5. Ringkasan indikator untuk setiap konstruk disajikan pada tabel berikut. Indikator dikembangkan dan diadaptasi dari literatur terkait keamanan biometrik, perlindungan data, dan kepercayaan pengguna dalam layanan pembayaran digital (Hartono et al., 2022; Cho et al., 2024; Budiman et al., 2025; Siti Khoiriah et al., 2025).

Konstruk	Kode	Indikator Pernyataan
Implementasi Biometrik (X1)	IB1	Autentikasi biometrik memudahkan proses login/otorisasi transaksi.
	IB2	Autentikasi biometrik pada aplikasi jarang gagal dan hasilnya akurat.
	IB3	Proses autentikasi biometrik berlangsung cepat/responsif.
	IB4	Sistem biometrik memiliki perlindungan terhadap pemalsuan (mis. liveness/anti-spoofing).
	IB5	Data biometrik pengguna diproses/disimpan dengan perlindungan yang memadai (mis. enkripsi/keamanan data).
Kepercayaan Pengguna (X2)	TR1	Saya percaya penyedia layanan menjaga kerahasiaan dan privasi data saya.
	TR2	Saya percaya sistem mampu melindungi saya dari akses tidak sah/penipuan.
	TR3	Saya percaya penyedia layanan bertanggung jawab jika terjadi masalah keamanan.
	TR4	Saya percaya data biometrik tidak akan disalahgunakan oleh pihak lain.
	TR5	Saya percaya kebijakan keamanan/privasi penyedia layanan jelas dan dapat dipercaya.
Evaluasi Keamanan (Y)	SE1	Saya merasa aman menggunakan biometrik untuk autentikasi pembayaran digital.
	SE2	Risiko akun/transaksi diakses pihak tidak berwenang menjadi lebih rendah dengan biometrik.
	SE3	Sistem pembayaran digital berbasis biometrik dinilai sulit untuk dibobol/diserang.
	SE4	Saya menilai perlindungan keamanan dan privasi pada sistem sudah memadai.
	SE5	Secara keseluruhan, sistem pembayaran digital yang saya gunakan aman untuk transaksi.

Untuk memperjelas konteks penelitian, responden dalam studi ini adalah pengguna layanan pembayaran digital di Indonesia yang mengaktifkan autentikasi biometrik (fingerprint dan/atau pengenalan wajah) pada aplikasi pembayaran (misalnya dompet digital dan/atau mobile banking) untuk kebutuhan login, otorisasi transaksi, atau konfirmasi pembayaran (termasuk skenario pembayaran berbasis QR/QRIS). Karakteristik responden dicatat untuk

memastikan keterwakilan profil pengguna dan relevansi konteks, meliputi jenis kelamin, rentang usia, pendidikan/pekerjaan, domisili, serta intensitas penggunaan pembayaran digital (frekuensi transaksi dan lama penggunaan fitur biometrik). Ringkasan karakteristik responden disajikan pada Tabel X (atau lampiran), sehingga pembaca dapat menilai cakupan populasi pengguna yang menjadi dasar inferensi temuan penelitian ini.

Pengambilan sampel dilakukan secara purposive sampling dengan kriteria responden yang telah menggunakan sistem pembayaran biometrik dalam enam bulan terakhir. Data yang dikumpulkan dianalisis menggunakan metode Partial Least Square Structural Equation Modeling (PLS-SEM) dengan bantuan software SmartPLS. Analisis dilakukan dalam dua tahap, yaitu pengujian outer model (untuk mengukur validitas dan reliabilitas instrumen) dan inner model (untuk menganalisis hubungan antar variabel laten). Hasil penelitian ini diharapkan dapat memberikan gambaran yang komprehensif tentang efektivitas implementasi dan keamanan biometrik dalam sistem pembayaran digital.



Gambar. Hubungan X1 dan X2 terhadap Y

Gambar diatas menunjukkan model penelitian yang menguji pengaruh Implementasi Biometrik (X1) dan Kepercayaan Pengguna (X2) terhadap Evaluasi Keamanan (Y) pada sistem pembayaran digital. Model ini memformalkan dua hubungan utama: H1 menyatakan bahwa semakin baik implementasi biometrik (misalnya kemudahan, akurasi, dan perlindungan autentikasi), semakin tinggi evaluasi keamanan; sedangkan H2 menyatakan bahwa semakin tinggi kepercayaan pengguna terhadap penyedia layanan dan pengelolaan data, semakin tinggi evaluasi keamanan yang dirasakan. Dengan demikian, evaluasi keamanan diposisikan sebagai konstruk endogen yang dijelaskan oleh faktor teknis (implementasi biometrik) dan faktor psikologis (kepercayaan pengguna).

HASIL PENGUJIAN HIPOTESIS

Tabel 1. Uji Validitas dan Reliabilitas

Variabel	Cronbach Alpha	Composite Reliability	AVE	Interpretasi
Evaluasi Keamanan (Y)	0.944	0.958	0.819	Valid dan sangat reliabel
Implementasi Biometrik (X1)	0.925	0.944	0.770	Valid dan sangat reliabel
Kepercayaan Pengguna (X2)	0.926	0.944	0.772	Valid dan sangat reliabel

Sumber: Data diolah, PLS 2026

Cronbach's Alpha dan Composite Reliability (CR) masing-masing berada di atas 0,70, bahkan mendekati 0,95 untuk semua variabel (Y, X1, X2), menunjukkan bahwa konstruk memiliki konsistensi internal yang sangat baik. Average Variance Extracted (AVE) juga sangat tinggi, yaitu > 0,77 untuk seluruh konstruk. Ini berarti lebih dari 77% variansi indikator dijelaskan oleh konstruknya, menunjukkan validitas konvergen yang sangat baik. Instrumen pengukuran pada setiap konstruk (Implementasi Biometrik, Kepercayaan Pengguna, dan Evaluasi Keamanan) valid dan reliabel untuk digunakan dalam penelitian ini.

Tabel 2. Uji Validitas Diskriminan (Fornell-Larcker Criterion)

Konstruk	√AVE (Diagonal)	Korelasi dengan konstruk lain	Hasil
Evaluasi Keamanan (Y)	0.905	0.842 (X1), 0.837 (X2)	Valid
Implementasi Biometrik (X1)	0.877	0.848 (X2)	Valid
Kepercayaan Pengguna (X2)	0.879	-	Valid

Sumber: Data diolah, PLS 2026

Nilai diagonal (√AVE) dari masing-masing konstruk lebih tinggi dibandingkan korelasinya dengan konstruk lain:

- √AVE Y = 0.905 > korelasi dengan X1 (0.842) dan X2 (0.837)
- √AVE X1 = 0.877 > korelasi dengan X2 (0.848)

Setiap konstruk dalam model mampu membedakan dirinya dengan konstruk lain, yang berarti tidak terjadi tumpang tindih konsep antar variabel laten.

Tabel 3. Path Coefficient & Signifikansi (Inner Model)

Hubungan	Koefisien	T-Statistik	P-Value	Interpretasi
X1 → Y (Implementasi → Evaluasi)	0.473	4.687	0.000	Signifikan
X2 → Y (Kepercayaan → Evaluasi)	0.435	4.011	0.000	Signifikan

Sumber: Data diolah, PLS 2026

Nilai T-statistik > 1.96 dan P-value < 0.05 menunjukkan bahwa pengaruh keduanya terhadap evaluasi keamanan bermakna secara statistik. Nilai koefisien menunjukkan bahwa semakin baik implementasi biometrik dan semakin tinggi kepercayaan pengguna, semakin tinggi pula persepsi terhadap keamanan sistem pembayaran digital. Hipotesis penelitian terbukti. Kedua variabel independen berpengaruh signifikan terhadap variabel dependen.

Tabel 4. R-Square (Kekuatan Penjelasan)

Variabel Endogen	R^2	Interpretasi
Evaluasi Keamanan (Y)	0.762	Sangat kuat (>0.75)

Sumber: Data diolah, PLS 2026

Nilai R^2 sebesar 0.762 menunjukkan bahwa 76.2% variasi dalam Evaluasi Keamanan dapat dijelaskan oleh kombinasi Implementasi Biometrik (X1) dan Kepercayaan Pengguna (X2). Model struktural memiliki daya prediksi yang sangat kuat terhadap variabel dependen, sehingga cukup andal untuk digunakan dalam pengambilan kesimpulan kebijakan atau praktik.

Tabel 5. Effect Size (f^2)

Hubungan	f^2	Interpretasi
X1 → Y	0.264	Sedang
X2 → Y	0.224	Sedang

Sumber: Data diolah, PLS 2026

Nilai f^2 antara 0.15–0.35 dikategorikan sebagai pengaruh sedang. Hal ini berarti baik implementasi maupun kepercayaan pengguna memiliki kontribusi nyata dan penting terhadap persepsi keamanan. Setiap variabel independen memiliki kontribusi yang berarti secara praktis, bukan hanya secara statistik.

Semua pengujian dalam model ini memenuhi kriteria statistik yang disarankan. Instrumen terbukti valid dan reliabel, hubungan antar variabel signifikan, dan model mampu menjelaskan sebagian besar variabilitas dalam persepsi keamanan. Ini menunjukkan bahwa penerapan biometrik serta kepercayaan pengguna adalah faktor penting dalam menciptakan sistem pembayaran digital yang aman dan terpercaya.

Pembahasan

Temuan bahwa implementasi biometrik (X1) berpengaruh positif terhadap evaluasi keamanan (Y) dapat dijelaskan melalui perspektif TAM dan teori keamanan sistem informasi. Dalam kerangka TAM, autentikasi biometrik mengurangi friksi penggunaan (tidak perlu mengingat PIN/password, proses lebih cepat), sehingga meningkatkan persepsi kemudahan dan kualitas sistem yang kemudian diterjemahkan pengguna sebagai sistem yang "lebih aman dan lebih andal". Dari sisi keamanan, biometrik juga berfungsi sebagai security assurance karena dianggap lebih sulit ditiru dibanding kredensial tradisional, terutama bila diiringi mekanisme anti-spoofing/liveness detection. Karena itu, ketika pengguna menilai implementasi biometrik berjalan konsisten (mudah dipakai, jarang gagal, responsif), evaluasi keamanan cenderung meningkat bukan hanya karena "ada biometrik", melainkan karena implementasinya memberi sinyal kontrol keamanan yang nyata.

Selanjutnya, pengaruh positif kepercayaan pengguna (X2) terhadap evaluasi keamanan (Y) konsisten dengan trust–risk framework, yang menempatkan kepercayaan sebagai mekanisme psikologis untuk menurunkan ketidakpastian dan persepsi risiko pada transaksi digital. Dalam konteks pembayaran digital, pengguna tidak memiliki akses untuk memverifikasi keamanan teknis secara langsung; akibatnya, mereka mengandalkan keyakinan bahwa penyedia layanan kompeten menjaga privasi, melindungi data sensitif, dan mampu menangani risiko keamanan. Ketika kepercayaan meningkat, pengguna cenderung menilai sistem lebih aman karena mereka mempersepsikan adanya komitmen dan kemampuan penyedia layanan dalam mencegah akses tidak sah serta melindungi data biometrik dan finansial.

Nilai effect size (f^2) yang berada pada kategori sedang untuk jalur X1→Y dan X2→Y menunjukkan bahwa evaluasi keamanan bukan semata hasil "kontrol teknis" atau semata "keyakinan psikologis", melainkan kombinasi keduanya. Secara teoretis, hal ini mendukung argumen bahwa keamanan pada fintech bersifat sosio-teknis: kontrol autentikasi (biometrik) menyediakan jaminan struktural, sementara kepercayaan memperkuat interpretasi pengguna terhadap jaminan tersebut. Dengan kata lain, implementasi biometrik yang baik cenderung menaikkan evaluasi keamanan, namun dampak tersebut menjadi lebih bermakna ketika pengguna juga percaya pada tata kelola dan akuntabilitas penyedia layanan dalam pengelolaan data biometrik.

Meski demikian, literatur juga menunjukkan potensi kontradiksi: biometrik dapat meningkatkan keamanan, tetapi sekaligus memunculkan kekhawatiran privasi dan risiko kebocoran data (terutama karena data biometrik tidak dapat "diganti" seperti password) serta risiko spoofing pada skenario tertentu. Kontradiksi ini membantu menjelaskan mengapa sebagian studi menemukan efek biometrik tidak selalu linear positif—khususnya ketika kepercayaan terhadap pengelolaan data rendah atau ketika pengguna menilai teknologi (misalnya face recognition) lebih invasif dibanding fingerprint. Dalam studi ini,

arah hubungan yang tetap positif mengindikasikan bahwa pada sampel pengguna yang sudah mengadopsi biometrik, manfaat keamanan dan kenyamanan cenderung lebih dominan daripada kekhawatiran privasi; namun temuan ini juga menegaskan pentingnya transparansi, proteksi data, dan komunikasi keamanan agar peningkatan keamanan teknis tidak berbalik menjadi penurunan kepercayaan.

KESIMPULAN, KETERBATASAN DAN SARAN

Penelitian ini memiliki keterbatasan penting, yaitu evaluasi keamanan diukur melalui persepsi responden (self-reported security perception) sehingga temuan merefleksikan penilaian subjektif pengguna, bukan audit teknis keamanan sistem secara langsung. Konsekuensinya, hasil dapat dipengaruhi oleh bias persepsi (misalnya pengalaman pribadi, tingkat literasi digital, atau paparan informasi keamanan di media). Untuk meminimalkan potensi bias metode umum, pengisian kuesioner dilakukan secara anonim dan instruksi menekankan bahwa tidak ada jawaban benar/salah; namun demikian, penelitian lanjutan disarankan untuk mengombinasikan pendekatan survei dengan indikator objektif (misalnya uji keamanan aplikasi, log insiden/keluhan, atau evaluasi kontrol keamanan) serta memperluas konteks pada jenis aplikasi/sektor yang lebih spesifik agar generalisasi temuan menjadi lebih kuat. Berdasarkan hasil analisis dengan metode PLS-SEM, dapat disimpulkan bahwa implementasi teknologi biometrik, baik melalui fingerprint maupun pengenalan wajah, berpengaruh signifikan terhadap evaluasi keamanan sistem pembayaran digital. Disarankan agar pengembang aplikasi pembayaran digital terus meningkatkan kualitas implementasi fitur biometrik dengan memastikan keandalan teknis, perlindungan privasi, dan transparansi dalam pengelolaan data biometrik pengguna. Selain itu, penting untuk membangun edukasi dan literasi digital yang mendorong kepercayaan publik terhadap teknologi biometrik, agar adopsinya semakin luas dan keamanannya dapat dinikmati secara maksimal oleh masyarakat.

Penelitian ini menegaskan kontribusi teoretis dengan mengintegrasikan TAM dan trust–risk framework, yakni memposisikan implementasi biometrik sebagai security assurance yang tidak hanya meningkatkan evaluasi keamanan secara langsung, tetapi juga memperkuatnya melalui mekanisme kepercayaan pengguna sehingga memperkaya pemahaman sosio-teknis keamanan fintech. Secara metodologis, studi ini memiliki keterbatasan karena evaluasi keamanan diukur berbasis persepsi responden (self-reported), desain cross-sectional membatasi inferensi dinamika kausal dari waktu ke waktu, ukuran dan teknik sampel dapat membatasi generalisasi, serta belum dilakukan multi-group analysis untuk membandingkan fingerprint vs face recognition. Perkembangan sistem pembayaran digita

Sebagai rekomendasi kebijakan, pemerintah dan otoritas terkait seperti Bank Indonesia serta Kementerian Komunikasi dan Informatika perlu menetapkan regulasi yang jelas dan tegas mengenai standar keamanan penggunaan teknologi biometrik dalam sistem pembayaran digital. Kebijakan tersebut harus mencakup aspek perlindungan data biometrik, prosedur audit teknologi, kewajiban penyedia layanan untuk menerapkan enkripsi dan deteksi liveness, serta mekanisme pengawasan terhadap potensi penyalahgunaan data. Selain itu, diperlukan kolaborasi antara regulator, penyedia teknologi, dan lembaga keuangan untuk memastikan bahwa penerapan biometrik tidak hanya efisien, tetapi juga memenuhi prinsip keadilan, privasi, dan keamanan konsumen.

REFERENSI

Ancelin Feodora Anthony, C., Lumban Gaol, N. A., Purba, N. N., Raudina, C., Maulana, A., & Universitas Pembangunan Nasional Veteran Jakarta. (2023). Peranan audit internal dalam pengendalian fraud di era digital. Accounting Student Research Journal, 2(1).

Anwar, M., Rahmatullah, A., & Others. (2025). Pelayanan informasi pajak kendaraan bermotor terhadap wajib pajak melalui E-SIGNAL di Kabupaten Jember. Menulis: Jurnal Penelitian. https://padangjurnal.web.id/index.php/menulis/article/view/179

Budiman, A., Isa, M., & Soekiswati, S. (2025). Analisis risiko dan tindakan pencegahan kebocoran data rekam medis elektronik pasien di RS P Surakarta. Ranah Research: Journal of https://jurnal.ranahresearch.com/index.php/R2J/article/view/1421

Caseba, F. L., & Dewayanto, T. (2024). Penerapan artificial intelligence, big data, dan blockchain dalam fintech payment terhadap risiko penipuan komputer. Diponegoro Journal of Accounting. https://ejournal3.undip.ac.id/index.php/accounting/article/view/46058

Cho, S. J., Kim, K., Park, S., & Bae, G. (2024). Method and apparatus that detects spoofing of biometric information. US Patent. https://patents.google.com/patent/US11915525B2/en

Destarianto, P. P., Hartadi, D. R., Pratita, D. G., & Others. (2024). Diseminasi sistem payment gateway dengan blockchain pada aplikasi DiKantin sebagai produk unggulan TEFA. National Conference. https://ocs.polije.ac.id/index.php/nacosvi/article/view/161

Febria, D. (2020). Pengaruh leverage, profitabilitas dan kepemilikan manajerial terhadap manajemen laba. SEIKO: Journal of Management & Business, 3(2), 65. https://doi.org/10.37531/sejaman.v3i2.568

Hartono, N., Rizaldy, A., & Lestari, N. A. (2022). Studi literatur sistem keamanan biometrik untuk verifikasi dan transaksi dompet digital. Journal SHIFT, 2(2).

Hendrayana, I. G., Suprayitno, D., Judijanto, L., & Kosadi, F. (2024). E-Money: Panduan lengkap penggunaan dan manfaat e-money dalam era digital. Google Books. https://books.google.com

Herina, M. I., Putri, N. S., & Pramestirani, S. M. (2024). Kemudahan dan keamanan transaksi e-commerce. Jurnal Star. http://jurnalstar.digitechuniversity.ac.id/index.php/jurnalstar/article/view/168

Junaeni, I. (2020). Pengaruh indikator keuangan perusahaan terhadap harga saham dalam kelompok Jakarta Islamic Indeks. Owner, 4(1), 216. https://doi.org/10.33395/owner.v4i1.220

Lira, A. E. T. (2025). Digital banking: Inovasi dan implementasi di industri perbankan syariah Kota Makassar. Jurnal Perubahan Ekonomi. https://oaj.jurnalhst.com/index.php/jpe/article/view/8923

Mahadini, A. S., Setianingsih, E. L., & Others. (2024). Implementasi kebijakan sistem fingerprint pasien khusus rawat jalan BPJS Kesehatan di Rumah Sakit PKU Muhammadiyah Gombong. Journal of Public Policy. https://ejournal3.undip.ac.id/index.php/jppmr/article/view/47162

Manajerial, K., Dan, U. P., Laba, M., Perusahaan, P., & Dan, P. (2020). Real estate managerial ownership, leverage, profitability, firm size and earnings management in properti and real estate companies. Jurnal Ekonomi dan Manajemen, 5(1), 49–61.

Mulumbot, F. J., & Sumanti, E. (2020). The effect of information asymmetry and corporate governance mechanism on earnings management. Klabat Accounting Review, 1(1), 27–40.

Muninggar, R. A., & Rahardiansah, T. (2024). Pemberdayaan hukum pembayaran digital melalui penggunaan teknologi Quick Response Code Indonesian Standard (QRIS). Jurnal Pembangunan Hukum Indonesia. https://ejournal2.undip.ac.id/index.php/jphi/article/view/23794

Prayitno, A., & Maryam Sinosi, S. (2024). Peran pengendalian internal berbasis teknologi dalam mendukung akuntansi forensik untuk mendeteksi fraud di era digital. Economics and Digital Business Review, 5.

Putri, I. P., Kesuma, H. D., Amelia, N. M. P., Sutrisna, R., & Others. (2025). Transformasi digital melalui sistem kepegawaian terintegrasi pada kantor berita di Palembang. Abdimas Galuh. https://jurnal.unigal.ac.id/index.php/abdimasgaluh/article/view/18042

Rachman, D. S., & Biduri, S. (2023). Pencegahan fraud di era digital. Jurnal Akuntansi Keuangan dan Bisnis, 16(2). https://jurnal.pcr.ac.id/index.php/jakb/

Rengganis, F. D., & Susanto, D. S. (2023). Evaluation of the anti-money laundering programs implementation in Indonesia. Integritas: Jurnal Antikorupsi, 9(2), 229–240. https://doi.org/10.32697/integritas.v9i2.973

Rohayati, E. (2020). Pengaruh asimetri informasi dan ukuran perusahaan terhadap manajemen laba pada sub sektor industri rokok yang terdaftar di Bursa Efek Indonesia periode 2013–2017. Eksis: Jurnal Ilmiah Ekonomi dan Bisnis, 10(2), 116. https://doi.org/10.33087/eksis.v10i2.173

Safitri, N., Arlan, A. S., & Urahmah, N. (2025). Efektivitas aplikasi Jamsostek Mobile (JMO) dalam proses pencairan jaminan hari tua (JHT). Al Iidara Balad. https://jurnal.stiaamuntai.ac.id/index.php/aliidarabalad/article/view/941

Sakti, A. F. A., Ramadhan, A. Y., Munir, B., & Others. (2025). Analisis prinsip perlindungan berbasis kemampuan pada sistem operasi Android. Scientica: Jurnal Ilmiah Sains dan Teknologi, 9(1). https://jurnal.researchideas.org/index.php/scientica/article/view/351

Sari, N. P., & Khafid, M. (2020). Peran kepemilikan manajerial dalam memoderasi pengaruh profitabilitas, leverage, ukuran perusahaan, kebijakan dividen terhadap manajemen laba pada perusahaan BUMN. Jurnal Ilmu Ekonomi, 7(2).

Setiyawan, I. N. Y., & Tjahyanti, L. (2024). Optimasi sistem pengenalan wajah dengan teknik pengolahan citra untuk meningkatkan akurasi dan efisiensi. KOMTEKS, 7(1). https://ejournal.unipas.ac.id/index.php/Komteks/article/view/2294

Setiyawan, Y. N. (2024). Evaluasi kualitas layanan dompet digital OVO dengan metode E-Servqual, IPA-Kano, dan QFD. Skripsi, Institut Teknologi Sepuluh Nopember. https://repository.its.ac.id/110995/

Siti Khoiriah, Salsabila, A., Camberra, D. D., Syafri, E., Layyin, H. L., Fathurrahman, R., & Marjohan, M. (2025). Keamanan dan privasi dalam keuangan digital. Jurnal Publikasi Sistem

Informasi dan Manajemen Bisnis, 4(2), 409–418. https://doi.org/10.55606/jupsim.v4i2.4524

Susilawati, Y., & Aziz, A. (2025). Pengaruh produktivitas kerja dan disiplin kerja terhadap keterpenuhan pembayaran tunjangan kinerja pegawai. Neraca: Jurnal Ekonomi dan Akuntansi. https://jurnal.researchideas.org/index.php/neraca/article/view/93

Syaifullah, S., Haryanto, R., & Others. (2024). Implementation of e-money as student payment at Al-Amien Islamic Boarding School from an Islamic economic perspective. Masyrif: Jurnal Ekonomi dan Perbankan Syariah, 6(1). https://ejournal.unia.ac.id/index.php/masyrif/article/view/1800

Utami, S. E. N., Kusumahadi, T. A., & SE, M. E. (2024). Financial Technology 2. Google Books. https://books.google.com

Wahana, A. (2025). Peran teknologi transparansi dan keamanan dalam Ekonomi 5.0 pada blockchain. Indonesian Research Journal on Education. http://irje.org/irje/article/view/2322

Yu, S., Jia, W., Shu, X., Yuan, X., Gui, J., Tang, J., & Shan, C. (2025). Biometric Recognition: Proceedings of the 18th Chinese Conference, CCBR 2024. Springer. https://books.google.com/books?id=WyVEEQAAQBAJ

Zuhri, S., Juhandi, N., Sudibyo, H. H., & Fahlevi, M. (2020). Determinasi harga saham perusahaan manufaktur subsektor makanan dan minuman. Journal Industrial Engineering & Management Research (JIEMAR), 1(2), 24–34.