Jurnal Publikasi Sistem Informasi dan Manajemen Bisnis
Volume.4, Nomor. 2 Mei 2025
e-ISSN: 2808-8980; p-ISSN: 2808-9383, Hal 409-418
DOI: https://doi.org/10.55606/jupsim.v4i2.4524
Available online at : https://journalcenter.org/index.php/jupsim

Keamanan dan Privasi dalam Keuangan Digital

Siti Khoiriah[1*], Annisa Salsabila[2], Daniel David Camberra[3], Erwan Syafri[4], Haqiqi Lina Layyin[5], Riangga Fathurrahman[6], Masno Marjohan[7]
[1-7] Universitas Pamulang, Tangerang Selatan – Indonesia
Email : Stkhoiriah23@gmail.com [1]

Alamat : Jl. Raya Puspitek, Buaran, Kec. Pamulang, Kota Tangerang Selatan, Banten 15310
Korespondensi penulis: stkhoiriah23@gmail.com *

Abstract. *The rapid digitalization of the financial sector in Indonesia has significantly improved access to financial services but also raised serious concerns regarding the security and privacy of user data. Low levels of digital awareness among the public, coupled with uneven adoption of protective technologies such as encryption and blockchain, have intensified these vulnerabilities. This study aims to identify cybersecurity threats and risks in digital financial systems, evaluate the effectiveness of data protection technologies, and analyze the role of regulations and user education in strengthening data protection mechanisms. A systematic literature review was conducted using a qualitative descriptive approach, drawing on 20 national academic sources published between 2018 and 2025. The findings are grouped into four key themes: (1) technical and human-related security risks, (2) variation in the application of protective technologies, (3) institutional disparities in readiness for compliance with the 2022 Personal Data Protection Law, and (4) low privacy literacy among younger users. The study concludes that effective data protection requires synergy between regulation, technology, and digital literacy education. This research highlights the need for strict digital security audits and integrated privacy awareness campaigns within formal education and small business training programs.*

Keywords: *Digital Security, Data Privacy, Fintech, Digital Finance, Data Encryption*

Abstrak. Pesatnya digitalisasi sektor keuangan di Indonesia membawa kemudahan akses layanan keuangan namun juga menimbulkan risiko serius terhadap keamanan dan privasi data pengguna. Minimnya kesadaran digital masyarakat dan belum meratanya penerapan teknologi proteksi seperti enkripsi dan blockchain semakin memperparah kerentanan ini. Penelitian ini bertujuan untuk mengidentifikasi ancaman dan risiko keamanan siber pada sistem keuangan digital, mengevaluasi efektivitas teknologi pengamanan, serta menganalisis peran regulasi dan edukasi pengguna dalam memperkuat sistem perlindungan data. Metode yang digunakan adalah studi literatur sistematis dengan pendekatan deskriptif kualitatif terhadap 20 sumber ilmiah nasional terbitan 2018–2025. Hasil penelitian mengelompokkan empat tema utama yaitu: (1) risiko keamanan teknis dan human error, (2) variasi penerapan teknologi proteksi, (3) ketimpangan kesiapan lembaga terhadap UU PDP 2022, dan (4) rendahnya literasi privasi di kalangan pengguna muda. Temuan ini menunjukkan bahwa pendekatan perlindungan data yang efektif harus mencakup sinergi antara regulasi, teknologi, dan edukasi literasi digital. Penelitian ini berimplikasi pada perlunya audit keamanan digital yang ketat serta kampanye literasi privasi yang terintegrasi ke dalam pendidikan formal dan pelatihan UMKM.

Kata kunci: Keamanan Digital, Privasi Data, Fintech, Keuangan Digital, Enskripsi Data

1. LATAR BELAKANG

Digitalisasi sektor keuangan di Indonesia telah melahirkan banyak inovasi seperti *mobile banking*, dompet digital, pinjaman *peer-to-peer*, hingga *Central Bank Digital Currency (CBDC)*. Inovasi-inovasi ini memudahkan akses masyarakat terhadap layanan keuangan, namun seiring dengan itu muncul pula tantangan besar dalam bentuk kebocoran data, penyalahgunaan identitas, dan peretasan sistem. Laporan Badan Siber dan Sandi Negara (BSSN) mencatat peningkatan serangan siber terhadap lembaga keuangan digital sebesar 30% antara tahun 2020–2023 (BSSN, 2023).

Received: Maret 15, 2025; Revised: April 22, 2025; Accepted: Mei 17, 2025; Published: Juni 20, 2025

Di sisi lain, menurut (Ajiyanda et al., 2024) literasi pengguna terhadap pentingnya privasi dan keamanan data masih rendah. Hal ini diperparah oleh lemahnya implementasi regulasi perlindungan data pribadi sebelum disahkannya UU PDP Tahun 2022. Selain itu, beberapa platform keuangan digital belum mengadopsi teknologi pengamanan mutakhir seperti kriptografi simetris maupun blockchain (Fajriyah & Purwanti, 2025).

Studi oleh (Pebriani et al., 2025) menunjukkan bahwa koperasi digital masih rentan terhadap kebocoran data akibat lemahnya proteksi akses administratif. Sejalan dengan itu, riset (Kamalia & Purwitasari, 2024) menyoroti rendahnya kepercayaan mahasiswa terhadap e-wallet, terutama dalam hal pengelolaan data oleh penyedia layanan. Oleh karena itu, penelitian ini menjadi penting untuk mengkaji berbagai pendekatan dan strategi dalam mengamankan sistem keuangan digital yang semakin kompleks.

Tujuan dari penelitian literatur ini yaitu untuk mengidentifikasi faktor-faktor risiko terhadap keamanan dan privasi di sistem keuangan digital, menelaah efektivitas teknologi proteksi seperti blockchain, enkripsi, dan otentikasi dua faktor, mengevaluasi peran regulasi dan edukasi pengguna dalam meningkatkan resiliensi sistem.

2. KAJIAN TEORITIS

Dalam konteks digital, keamanan informasi *(information security)* adalah perlindungan terhadap informasi dan sistem dari akses, penggunaan, pengungkapan, gangguan, modifikasi, atau perusakan yang tidak sah. Sementara itu, privasi data *(data privacy)* mengacu pada hak individu untuk mengontrol pengumpulan, penggunaan, dan distribusi informasi pribadi mereka.

Pendekatan teknis keamanan digital mencakup: autentikasi (password, OTP, biometrik), enkripsi *(data at rest & in transit)*, firewall dan IDS/IPS, manajemen identitas dan akses (IAM), blockchain sebagai model distribusi ledger (Fajriyah & Purwanti, 2025). Sementara itu, privasi berfokus pada: minimasi data, penggunaan sesuai tujuan *(purpose limitation)*, kontrol pengguna terhadap data mereka, hak untuk dilupakan *(right to be forgotten)* yang mulai diterapkan pada beberapa platform digital.

Beberapa teori yang sering digunakan dalam menganalisis perilaku pengguna dan keamanan digital antara lain:

1. *Protection Motivation Theory (PMT)*

   Dikembangkan oleh Rogers 1975, PMT menjelaskan bahwa motivasi perlindungan seseorang timbul dari persepsi ancaman *(severity & vulnerability)* dan kemampuan coping *(response efficacy & self-efficacy).* Dalam konteks digital banking, pengguna akan lebih

berhati-hati apabila mereka merasa datanya rentan atau ancaman peretas besar (Putri et al., 2025).

2. *Theory of Planned Behavior (TPB)*

   Menurut Ajzen dalam (Seni & Ratnadi, 2017) mengungkapkan bahwa niat seseorang untuk bertindak dipengaruhi oleh sikap terhadap perilaku, norma subjektif, dan kontrol perilaku. TPB berguna dalam menjelaskan intensi pengguna untuk menggunakan sistem keuangan digital yang dianggap aman.

3. *DeLone & McLean Information System Success Model*

   Model ini menilai kesuksesan sistem informasi berdasarkan kualitas sistem, kualitas informasi, kualitas layanan, penggunaan, kepuasan pengguna, dan dampak net benefit. Menurut (Sulistyawati & Munawir, 2024) privasi dan keamanan dianggap elemen penting dalam kualitas sistem keuangan digital.

Sebelum disahkannya UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi, perlindungan terhadap privasi di Indonesia masih terbatas pada regulasi sektoral. Hal ini mengakibatkan banyak celah hukum, khususnya dalam transaksi elektronik yang melibatkan lembaga fintech (Hendarto, 2024). UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) merupakan undang-undang pertama yang secara komprehensif mengatur perlindungan data pribadi di Indonesia. UU ini mengadopsi banyak prinsip dari GDPR Eropa seperti:

1. Prinsip keabsahan pemrosesan data
2. Hak akses dan koreksi
3. Persetujuan eksplisit

Namun demikian, implementasinya masih menghadapi tantangan dari sisi kesiapan lembaga dan infrastruktur digital (Hendarto, 2024).

Studi oleh (Lestari, 2025) mengidentifikasi beberapa jenis ancaman utama terhadap keuangan digital, yaitu:

1. *Phishing*: upaya mendapatkan kredensial pengguna melalui penipuan.
2. *Malware*: program jahat yang mencuri informasi atau mengontrol perangkat pengguna.
3. *Insider threats*: kebocoran yang berasal dari pihak internal lembaga keuangan.
4. *Identity theft*: pencurian identitas untuk mengakses akun atau layanan.
5. *Social engineering*: manipulasi psikologis agar pengguna memberikan akses tidak sah.

Adapun teknologi yang digunakan untuk mitigasi risiko meliputi:

1. *Blockchain*

   Blockchain menyediakan sistem ledger terdistribusi yang memungkinkan transaksi terekam secara transparan dan tidak dapat diubah. Implementasi ini semakin banyak digunakan pada sektor remittance, lending peer-to-peer, dan smart contract di sektor keuangan (Fajriyaha, 2025).

2. *Artificial Intelligence* dalam Deteksi Kecurangan

   AI dapat digunakan untuk mendeteksi pola anomali dan mencegah fraud secara real-time (Mulyandini & Anggionaldi, 2024). Namun, AI juga membawa tantangan etika terkait privasi algoritmik.

3. Biometrik dan MFA *(Multi-Factor Authentication)*

   Metode autentikasi seperti sidik jari, pengenalan wajah, serta kombinasi password dan OTP menjadi protokol yang diadopsi luas di mobile banking Indonesia.

Literasi digital menjadi salah satu faktor penting dalam memahami risiko dan perlindungan data. Studi oleh (Ajiyanda et al., 2024) menunjukkan bahwa remaja usia sekolah belum sepenuhnya memahami pentingnya enkripsi dan keamanan PIN. Di sisi lain, budaya "asal klik" serta minimnya kebiasaan membaca kebijakan privasi memperparah potensi kebocoran informasi pribadi.

Beberapa studi yang menjadi dasar konseptual penelitian ini antara lain:

1. (Putri et al., 2025) menggunakan *Protection Motivation Theory (PMT)* untuk menjelaskan niat pengguna melindungi data pribadi mereka saat menggunakan aplikasi SeaBank.
2. (Lestari, 2025) mengkaji manfaat dan risiko internet banking serta pentingnya edukasi pengguna.
3. (Simatupang et al., 2024) menekankan bahwa kepercayaan pengguna menjadi penentu utama adopsi layanan digital.
4. (Sudarmanto et al., 2024) dalam bukunya memaparkan pentingnya sistem informasi akuntansi modern dalam mengelola data keuangan secara aman dan efisien.

Studi ini akan memperluas kajian sebelumnya dengan menyajikan sintesis komprehensif dari berbagai pendekatan teknologi dan regulasi terhadap isu keamanan dan privasi dalam konteks keuangan digital Indonesia.

3. METODE PENELITIAN

Penelitian ini menggunakan pendekatan deskriptif kualitatif berbasis studi pustaka sistematis, dengan fokus pada identifikasi, klasifikasi, dan analisis mendalam terhadap publikasi ilmiah yang membahas isu keamanan dan privasi dalam sistem keuangan digital di Indonesia. Penelitian ini bertujuan menghasilkan sintesis konseptual dan pemetaan fenomena dari berbagai perspektif ilmiah, teknologi, dan regulasi yang relevan dengan konteks Indonesia.

A. Jenis dan Desain Penelitian

Penelitian ini merupakan studi literatur sistematis *(systematic literature review)* yang tidak hanya mengumpulkan dan merangkum hasil studi terdahulu, tetapi juga menyusun hubungan antar-konsep secara teoritis. Studi literatur ini menekankan validitas isi dan kontekstual, dengan mengutamakan sumber yang relevan, mutakhir, dan berasal dari jurnal nasional terakreditasi, prosiding ilmiah, maupun buku akademik. Desain penelitian mencakup empat tahap utama:

1) Identifikasi literatur yang relevan.
2) Evaluasi kualitas dan kelayakan sumber.
3) Koding dan klasifikasi tematik.
4) Sintesis temuan ke dalam struktur konseptual dan argumentatif.

B. Sumber Data

Data sekunder dikumpulkan dari:

- Jurnal ilmiah nasional.
- Repositori perguruan tinggi.
- Prosiding seminar nasional.
- Buku ilmiah yang terbit dalam lima tahun terakhir.
- Laporan resmi lembaga seperti OJK, BSSN, BI, Kominfo.

Pencarian dilakukan melalui portal publish or perish yang terindeks Google Scholar, Garuda Ristekdikti, dan Sinta. Kata kunci yang digunakan: "keamanan digital", "privasi data", "fintech", "bank digital", "UU PDP", "perlindungan konsumen digital", "digital finance Indonesia".

C. Teknik Pengumpulan dan Pengolahan Data

Pengumpulan data dilakukan melalui tahapan berikut:

- Seleksi Awal: Membaca judul dan abstrak untuk menentukan relevansi.
- Evaluasi Isi: Membaca keseluruhan dokumen dan mencatat poin penting menggunakan lembar review.

- Koding Tematik: Mengelompokkan literatur berdasarkan topik dominan (keamanan, privasi, teknologi, regulasi, perilaku pengguna).
- Validasi Sumber: Memastikan kredibilitas melalui penerbit, akreditasi jurnal, dan tahun terbit.

Instrumen bantu yang digunakan:

- Mendeley Desktop: untuk manajemen referensi.
- Microsoft Excel: untuk matriks klasifikasi dan pengkodean data.

D. Teknik Analisis Data

Analisis data dilakukan dengan metode analisis isi tematik *(thematic content analysis)*, yaitu:

1) Menyaring konten artikel yang berkaitan langsung dengan keamanan dan privasi.
2) Menyusun peta tematik dari isu-isu dominan yang muncul.
3) Mengidentifikasi pola, perbedaan, dan kesenjangan (gap) dalam literatur.
4) Menyajikan sintesis dalam bentuk narasi konseptual dan tabel ringkasan.

Setiap publikasi yang dianalisis akan diberi skor relevansi berdasarkan:

1) Kedalaman analisis privasi/keamanan.
2) Kekuatan argumentasi teoritis.
3) Kontribusi pada konteks Indonesia.

E. Validitas dan Kredibilitas

Validitas data dijaga melalui:

1) Triangulasi sumber (lebih dari satu jurnal untuk setiap sub-topik utama).
2) *Peer cross-checking* antar penulis untuk menghindari bias.
3) Audit trail: pencatatan proses seleksi dan justifikasi inklusi literatur.

Reliabilitas dipastikan dengan penggunaan alat bantu (Mendeley, Excel) dan kerangka klasifikasi yang seragam. Hasil analisis disusun secara sistematis agar dapat direplikasi oleh peneliti lain.

4. HASIL DAN PEMBAHASAN

Penelitian ini menghasilkan empat kategori utama dari sintesis literatur, yaitu: (1) ancaman dan risiko keamanan digital, (2) teknologi pengamanan dan mitigasi risiko, (3) regulasi dan kebijakan privasi di Indonesia, serta (4) persepsi pengguna dan faktor sosial-budaya. Tiap kategori dianalisis berdasarkan temuan yang dominan dan ditinjau dalam konteks Indonesia.

Ancaman dan Risiko Keamanan Digital dalam Layanan Keuangan

Berdasarkan analisis 20 literatur ilmiah, ditemukan bahwa sektor keuangan digital di Indonesia menghadapi ancaman keamanan siber yang bersifat teknis dan manusiawi. Beberapa ancaman utama meliputi:

1. **Kelemahan Sistem Internal**

(Pebriani et al., 2025) melaporkan bahwa banyak koperasi digital di Indonesia tidak memiliki sistem cadangan data, firewall aktif, atau otorisasi berlapis. Akses ke panel admin hanya menggunakan password dasar tanpa 2FA, meningkatkan risiko peretasan.

a) **Serangan Siber**

(Lestari, 2025) mencatat peningkatan serangan phishing, malware, dan ransomware terhadap layanan mobile banking dan fintech. Beberapa bank digital mengalami gangguan sistem akibat *distributed denial-of-service (DDoS)*, yang melumpuhkan sistem transaksi selama berjam-jam.

b) **Kelemahan Sistem Internal**

(Pebriani et al., 2025) melaporkan bahwa banyak koperasi digital di Indonesia tidak memiliki sistem cadangan data, firewall aktif, atau otorisasi berlapis. Akses ke panel admin hanya menggunakan password dasar tanpa 2FA, meningkatkan risiko peretasan.

c) **Penyalahgunaan Data Nasabah**

Kasus penjualan data nasabah oleh oknum internal lembaga keuangan digital terungkap dalam investigasi oleh (Hendarto, 2024). Data pribadi digunakan untuk penawaran asuransi, pinjaman pribadi, dan target iklan tanpa persetujuan pengguna.

2. **Teknologi Pengamanan dan Praktik Terbaik di Indonesia**

Dari sisi teknologi, Indonesia mulai mengadopsi beragam metode pengamanan digital, tetapi tingkat implementasi antar institusi masih timpang.

a) ***Multi-Factor Authentication (MFA)***

(Simatupang et al., 2024) menunjukkan bahwa sebagian besar bank digital telah menerapkan kombinasi PIN, OTP, dan biometrik (sidik jari/wajah) sebagai lapisan autentikasi. Namun, sebagian fintech hanya mengandalkan OTP via SMS yang masih rentan terhadap SIM swap dan intercept.

b) **Implementasi Enkripsi dan Blockchain**

(Sudarmanto et al., 2024) menyatakan bahwa enkripsi AES-256 mulai diterapkan dalam penyimpanan data transaksi dan saldo. Beberapa startup fintech seperti Pintek dan Dana Syariah mulai menjajaki penerapan blockchain dalam pelacakan transaksi dan validasi identitas (Fajriyah & Purwanti, 2025).

c) Deteksi Penipuan berbasis AI

(Mulyandini, 2024) mengembangkan model kecerdasan buatan untuk memonitor pola transaksi mencurigakan *(fraud pattern recognition)* pada layanan e-wallet, dan berhasil mendeteksi penipuan 24% lebih cepat dibanding sistem manual.

3. Perkembangan Regulasi Privasi dan Keamanan

Salah satu hambatan utama dalam perlindungan keamanan digital adalah ketertinggalan regulasi yang komprehensif sebelum hadirnya UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (PDP).

a) Keterbatasan Hukum Sebelumnya

Sebelum UU PDP, regulasi perlindungan data tersebar dalam PP No. 71/2019, POJK No. 12/2021, dan UU ITE. Menurut (Hasibuan et al., 2024), kelemahan utama adalah lemahnya sanksi, kurangnya pengawasan terhadap fintech, dan tidak adanya mekanisme class action bagi korban kebocoran data.

b) Implikasi UU PDP 2022

UU PDP mewajibkan lembaga keuangan digital untuk:

- Menyediakan dasar hukum pemrosesan data.
- Melindungi hak pengguna terhadap akses dan koreksi.
- Menyediakan insiden response center.

Namun, dalam praktiknya, (Simatupang et al., 2024) menyebutkan bahwa lembaga keuangan belum semua siap secara teknis dan struktural untuk memenuhi standar kepatuhan penuh. Banyak dari mereka masih mengandalkan sistem pihak ketiga *(outsourcing).*

4. Persepsi Pengguna dan Kesadaran Risiko

Aspek non-teknis seperti perilaku pengguna dan literasi digital sangat berpengaruh dalam efektivitas perlindungan data.

a) Rendahnya Kesadaran Pengguna

Penelitian Kamalia (2024) menemukan bahwa 67% mahasiswa pengguna e-wallet tidak mengganti PIN default, dan 48% menggunakan tanggal lahir sebagai sandi. Pengguna juga cenderung menyetujui terms & conditions tanpa membacanya.

b) Generasi Z dan Trust Digital

Sabilla (2024) mengkaji persepsi Gen Z terhadap mobile banking dan menemukan bahwa perceived security menjadi faktor penentu utama dalam minat penggunaan aplikasi. Jika keamanan diragukan, maka loyalitas terhadap aplikasi turun drastis.

c) Literasi Privasi di Pelajar dan Koperasi

(Ajiyanda et al., 2024) dalam kegiatan edukasi di SMK menemukan bahwa siswa umumnya tidak mengetahui risiko berbagi informasi kartu ATM atau NIK kepada pihak ketiga. Literasi ini menjadi penting mengingat generasi muda merupakan target utama digital banking dan e-wallet.

5. KESIMPULAN DAN SARAN

Penelitian ini mengungkap bahwa keamanan dan privasi dalam sistem keuangan digital di Indonesia merupakan isu yang semakin penting di tengah pesatnya digitalisasi layanan keuangan. Berdasarkan hasil telaah terhadap 20 literatur ilmiah dan sumber resmi, dapat disimpulkan bahwa ancaman keamanan digital seperti *phishing, malware*, dan kebocoran data sangat nyata, baik dari aspek teknis maupun faktor internal organisasi keuangan digital. Teknologi pengamanan seperti enkripsi, multi-factor authentication, dan blockchain mulai diterapkan, namun belum merata di seluruh lembaga keuangan dan fintech. Regulasi perlindungan data mengalami perkembangan melalui hadirnya UU PDP Tahun 2022, namun masih terdapat celah dalam pengawasan, implementasi teknis, dan penegakan sanksi. Persepsi dan kesadaran pengguna masih rendah, terutama di kalangan generasi muda dan pelaku usaha mikro, sehingga meningkatkan risiko kebocoran data akibat kelalaian pribadi. Temuan ini memperkuat bahwa keamanan dan privasi bukan hanya persoalan teknologi, melainkan juga berkaitan dengan literasi, budaya digital, dan kepatuhan terhadap regulasi.

Lembaga keuangan digital perlu menerapkan standar keamanan siber nasional, termasuk audit berkala, sertifikasi sistem informasi, dan penggunaan teknologi keamanan berbasis AI dan blockchain. Pemerintah dan regulator seperti OJK, BSSN, serta Kominfo perlu memperkuat pengawasan dan melakukan pendekatan berbasis risiko terhadap layanan digital, terutama fintech berbasis komunitas. Dibutuhkan pula kurikulum literasi digital yang menyentuh aspek privasi di sekolah, universitas, dan pelatihan koperasi atau UMKM. Penelitian lanjutan direkomendasikan untuk mengeksplorasi efektivitas teknologi pengamanan dalam konteks daerah dan segmen pengguna marginal, serta dampak UU PDP terhadap perilaku industri keuangan digital.

DAFTAR REFERENSI

Ajiyanda, F., Sakti, D. V. S. Y., Santika, R. R., Permana, I., & Gandung, T. (2024). Peningkatan literasi digital dan keamanan data pribadi pada siswa SMK Triguna 1956. Jurnal Manajemen dan Teknologi, 5(1), 10–15. https://doi.org/10.29207/jamtekno.v5i1.5892

Fajriyah, A., & Purwanti. (2025). Pengaruh implementasi teknologi blockchain terhadap pengamanan dan keandalan pelaporan keuangan pada sistem informasi akuntansi dalam era digitalisasi. Jurnal Sistem Informasi dan Akuntansi, 12(1), 1567–1572.

Hasibuan, D. H., Harianto, D., & Utara, U. S. (2024). Pelindungan konsumen di bidang sistem pembayaran dalam pandangan sosiologi hukum. Jurnal Sosial, 5(2), 61–73. https://doi.org/10.53695/js.v5i2.1163

Hendarto, I. S. (2024). Implikasi pengaruh minimnya pengaturan perlindungan privasi data pribadi nasabah pada perbankan digital. Journal Justiciabellen (JJ), 4(2), 129–140.

Kamalia, S., & Purwitasari, F. (2024). Persepsi mahasiswa akuntansi terhadap penggunaan e-wallet sebagai alat tukar. Equilibrium: Jurnal Ekonomi dan Pembelajaran, 20(2), 180–187. https://doi.org/10.30742/equilibrium.v20i2.4027

Lestari, P. A. (2025). Transformasi digital bank syariah di era teknologi: Perkembangan, tantangan dan peluang menuju pertumbuhan berkelanjutan. Jurnal Sistem Informasi dan Teknologi (JSEIT), 5(2), 62–71. https://doi.org/10.31764/jseit.v5i2

Mulyandini, V. C. (2024). Peran kecerdasan buatan dalam mendeteksi kecurangan keuangan: Studi kasus pada proses audit forensik. Jurnal Akuntansi dan Teknologi, 16(2), 1–11. https://doi.org/10.31253/aktek.v16i2.3431

Pebriani, R. A., Yustini, T., Sari, R., & Kholis, N. (2025). Smart cooperative. Jurnal Abdimas Ekonomi dan Bisnis, 5(1), 58–65. https://doi.org/10.31294/3vcwad78

Putri, D. Y., Suratno, T., & Noverina, Y. (2025). Kesadaran privasi data dan kepercayaan pengguna aplikasi SeaBank menggunakan protection motivation theory. JATI: Jurnal Aktualisasi Teknologi Informasi, 9(4), 6207–6214. https://doi.org/10.36040/jati.v9i4.14019

Seni, N. N. A., & Ratnadi, N. M. D. (2017). Theory of planned behavior untuk memprediksi niat berinvestasi. E-Jurnal Ekonomi dan Bisnis Universitas Udayana, 6(12), 4043–4068.

Simatupang, S., Sinaga, O. S., Manurung, S., Ambarita, M. H., & Mokodongan, E. N. (2024). Bank digital dan kepercayaan konsumen. Jurnal Ilmiah Satyagraha, 7(2), 156–164. https://doi.org/10.47532/jis.v7i2.1090

Sudarmanto, E., Alamsyah, S., Hamdani, Sunaryo, D., Erviani, H., Kimsen, Kismanah, I., Erdawati, L., Kaswoto, J., Rahardja, L., Khorida, & Rachmania, D. (2024). Sistem informasi akuntansi kontemporer. Minhaj Pustaka. https://doi.org/10.62083/fpyy8k92

Sulistyawati, U. S., & Munawir. (2024). Decoding big data: Mengubah data menjadi keunggulan kompetitif dalam pengambilan keputusan bisnis. Jurnal Manajemen dan Teknologi (JMT), 1(2), 58–71. https://doi.org/10.35870/jmt.vxix.1114