

Dampak Keamanan Digital Banking terhadap Kualitas Pelayanan

Resi Juariah Susanto

Program Studi S1 Manajemen, Universitas Ekuitas Indonesia, Indonesia

Penulis Korespondensi: resi.juariah@gmail.com

Abstract. *This research examines the implications of the rapid development of digital banking technology on user security and analyzes how banking service quality influences the level of security and convenience experienced by customers when using digital banking services. The increasing adoption of digital financial services has created significant opportunities for improving transaction efficiency and accessibility, while also introducing various cybersecurity risks and challenges related to data privacy and consumer protection. From an operational management perspective, service quality is a critical element that must be managed consistently and sustainably to achieve customer satisfaction, strengthen trust, and enhance long-term customer loyalty. This study employs a qualitative literature review approach by collecting, reviewing, and analyzing books, scientific journals, government regulations, and other relevant publications concerning digital banking security and banking service quality. The findings indicate that high-quality banking services supported by robust security systems, effective risk management, and reliable digital infrastructure contribute significantly to improving customer confidence and reducing perceived security risks. Therefore, banks should continuously strengthen cybersecurity measures, enhance service quality, and implement customer-oriented digital innovations to ensure secure, efficient, and reliable digital banking services. The results of this study are expected to enrich the literature on digital banking and provide practical recommendations for banking institutions, policymakers, and future researchers.*

Keywords: Digital Banking; Operations Management; Security; Service Quality; Technology.

Abstrak. Penelitian ini mengkaji implikasi perkembangan pesat teknologi perbankan digital terhadap keamanan pengguna serta menganalisis bagaimana kualitas layanan perbankan memengaruhi tingkat keamanan dan kenyamanan yang dirasakan nasabah dalam menggunakan layanan perbankan digital. Meningkatnya adopsi layanan keuangan digital telah menciptakan peluang yang signifikan untuk meningkatkan efisiensi transaksi dan aksesibilitas, namun juga menghadirkan berbagai risiko keamanan siber serta tantangan yang berkaitan dengan privasi data dan perlindungan konsumen. Dari perspektif manajemen operasional, kualitas layanan merupakan elemen penting yang harus dikelola secara konsisten dan berkelanjutan guna mencapai kepuasan nasabah, memperkuat kepercayaan, serta meningkatkan loyalitas pelanggan dalam jangka panjang. Penelitian ini menggunakan pendekatan kualitatif melalui studi literatur dengan mengumpulkan, menelaah, dan menganalisis berbagai buku, jurnal ilmiah, peraturan pemerintah, serta publikasi lain yang relevan mengenai keamanan perbankan digital dan kualitas layanan perbankan. Hasil penelitian menunjukkan bahwa layanan perbankan yang berkualitas tinggi, didukung oleh sistem keamanan yang kuat, manajemen risiko yang efektif, serta infrastruktur digital yang andal, berkontribusi secara signifikan dalam meningkatkan kepercayaan nasabah dan mengurangi persepsi terhadap risiko keamanan. Oleh karena itu, perbankan perlu terus memperkuat langkah-langkah keamanan siber, meningkatkan kualitas layanan, serta menerapkan inovasi digital yang berorientasi pada nasabah untuk memastikan layanan perbankan digital yang aman, efisien, dan andal. Hasil penelitian ini diharapkan dapat memperkaya literatur mengenai perbankan digital serta memberikan rekomendasi praktis bagi institusi perbankan, pembuat kebijakan, dan peneliti selanjutnya.

Kata Kunci: Digital Banking; Keamanan; Kualitas Pelayanan; Manajemen Operasi; Teknologi.

1. LATAR BELAKANG

Perkembangan teknologi digital pada era saat ini berlangsung sangat cepat dan memberikan dampak signifikan terhadap berbagai sektor kehidupan, khususnya dalam pemenuhan kebutuhan masyarakat. Pemanfaatan teknologi telah mengubah pola aktivitas masyarakat, termasuk dalam hal transaksi keuangan yang kini tidak lagi bergantung pada pembayaran tunai. Salah satu wujud dari perkembangan tersebut adalah teknologi finansial (fintech), yaitu integrasi teknologi ke dalam sistem keuangan yang melahirkan berbagai layanan, produk, serta model bisnis baru. Kehadiran fintech memberikan pengaruh positif

terhadap peningkatan efisiensi, stabilitas sistem keuangan, keandalan serta keamanan sistem pembayaran. Di antara berbagai jenis fintech, transaksi digital menjadi salah satu yang mengalami pertumbuhan paling pesat dalam beberapa tahun terakhir (Siswanti, 2022).

Dalam konteks transaksi berbasis digital, aspek keamanan menjadi perhatian utama. Rahardjo (dalam Aini et al., 2019) menjelaskan bahwa keamanan transaksi online berkaitan dengan upaya pencegahan terhadap tindakan penipuan, atau setidaknya meminimalkan peluang terjadinya kecurangan dalam sistem berbasis informasi. Hal ini menjadi krusial mengingat informasi digital tidak memiliki bentuk fisik, sehingga rentan terhadap penyalahgunaan apabila tidak dikelola dengan sistem pengamanan yang memadai.

Penerapan teknologi digital dalam layanan keuangan juga membawa perubahan terhadap pola transaksi perbankan. Adopsi layanan digital diketahui mampu menurunkan intensitas transaksi melalui teller, khususnya untuk kebutuhan transfer, penyetoran, dan penarikan dana (Sharma, 2019). Melalui perbankan online, nasabah dapat melakukan pembayaran berbagai tagihan secara mandiri. Namun demikian, transaksi digital menuntut pengguna untuk membagikan data pribadi, sehingga menimbulkan ketidakpastian terkait perlindungan privasi nasabah dalam penggunaan layanan keuangan digital (James et al., 2020).

Berbagai layanan perbankan digital, seperti akses rekening, layanan pinjaman, dan layanan treasury, memiliki tantangan yang berbeda-beda. Penggunaan ATM dan mobile banking sebagai sarana transaksi keuangan juga memengaruhi pengalaman emosional pengguna. Pappu et al. (2018) mengungkapkan adanya keluhan terkait kegagalan mesin ATM yang tetap memotong saldo nasabah meskipun uang tunai tidak keluar. Selain itu, isu perlindungan privasi dan keamanan data menjadi perhatian serius, khususnya terkait risiko peretasan kata sandi. Kato (2019) menjelaskan bahwa peretas sering menyamar sebagai petugas bank dengan mengirimkan pesan palsu melalui email atau pesan singkat, yang bertujuan untuk mengelabui nasabah agar memberikan informasi penting melalui tautan tertentu. Fenomena tersebut menunjukkan bahwa keamanan layanan perbankan digital masih menjadi tantangan, sehingga penting untuk menelaah dampak penggunaan layanan perbankan digital terhadap nasabah, baik dalam akses rekening, layanan pinjaman, maupun layanan keuangan lainnya.

Perbankan digital didefinisikan sebagai istilah umum yang merujuk pada pengembangan layanan dan distribusi produk perbankan melalui berbagai media elektronik, seperti telepon, ATM, internet, dan saluran digital lainnya (Putra & Wiratnoko, 2021). Sejalan dengan hal tersebut, Kurnia (2020) menyatakan bahwa tuntutan kemudahan transaksi secara digital mendorong perbankan untuk terus melakukan inovasi dan pengembangan layanan.

Regulasi terkait penyelenggaraan teknologi finansial telah diatur dalam Peraturan Bank Indonesia Nomor 19/12/PBI/2017. Lebih lanjut, perkembangan teknologi mendorong bank bertransformasi menuju digital banking, yaitu layanan perbankan yang memungkinkan nasabah melakukan seluruh aktivitas perbankan melalui smartphone, mulai dari pembukaan rekening hingga transaksi keuangan lainnya, sebagaimana diatur dalam Peraturan Otoritas Jasa Keuangan Nomor 12/POJK.03/2018.

2. KAJIAN TEORITIS

Bagian ini menguraikan teori-teori relevan yang mendasari topik penelitian dan memberikan ulasan tentang beberapa penelitian sebelumnya yang relevan dan memberikan acuan serta landasan bagi penelitian ini dilakukan. Jika ada hipotesis, bisa dinyatakan tidak tersurat dan tidak harus dalam kalimat tanya. Putri et al. (2023) mengkaji bentuk perlindungan nasabah Bank Syariah Indonesia (BSI) terhadap risiko kebocoran data pribadi dalam penggunaan layanan digital banking di tengah pesatnya perkembangan ekonomi digital. Transformasi perbankan digital di Indonesia ditunjukkan oleh meningkatnya nilai transaksi digital banking yang mencapai Rp5,1 kuadriliun pada Agustus 2023. Walaupun layanan digital banking menawarkan kemudahan serta efisiensi bagi nasabah, di sisi lain terdapat risiko keamanan yang cukup tinggi, terutama terkait ancaman siber. Gangguan layanan yang terjadi pada Mei 2023 akibat maintenance system dan serangan siber menjadi bukti bahwa sistem perbankan digital memerlukan penguatan ketahanan keamanan guna melindungi data dan kenyamanan nasabah.

Penelitian yang dilakukan oleh Kurnia (2020) menunjukkan bahwa variabel fitur, kemudahan penggunaan, keamanan, dan promosi memiliki pengaruh secara parsial terhadap keputusan nasabah dalam menggunakan layanan digital banking Jenius. Selain itu, keempat variabel tersebut juga terbukti berpengaruh secara simultan terhadap keputusan penggunaan digital banking. Dari hasil analisis yang dilakukan, kemudahan penggunaan menjadi faktor yang paling dominan memengaruhi keputusan nasabah. Aplikasi yang mudah dipahami, mudah dioperasikan, memiliki tampilan menarik, serta bersifat user friendly terbukti mampu meningkatkan minat nasabah untuk memanfaatkan layanan digital banking Jenius.

Sari et al. (2022) mengungkapkan bahwa variabel keamanan, kepercayaan, manfaat, dan promosi secara parsial berpengaruh terhadap keputusan penggunaan dompet elektronik ShopeePay, sementara variabel kemudahan tidak menunjukkan pengaruh secara parsial. Namun demikian, secara simultan seluruh variabel yang terdiri dari keamanan, manfaat, kepercayaan, promosi, dan kemudahan terbukti memengaruhi keputusan penggunaan e-wallet

ShopeePay. Temuan penelitian tersebut juga menyimpulkan bahwa manfaat merupakan variabel yang paling dominan dalam mendorong keputusan pengguna dalam memilih dompet elektronik ShopeePay.

3. METODE PENELITIAN

Bagian ini memuat rancangan penelitian meliputi disain penelitian, populasi/ sampel penelitian, teknik dan instrumen pengumpulan data, alat analisis data, dan model penelitian yang digunakan. Metode yang sudah umum tidak perlu dituliskan secara rinci, tetapi cukup merujuk ke referensi acuan (misalnya: rumus uji-F, uji-t, dll). Pengujian validitas dan reliabilitas instrumen penelitian tidak perlu dituliskan secara rinci, tetapi cukup dengan mengungkapkan hasil pengujian dan interpretasinya. Keterangan simbol pada model dituliskan dalam kalimat. Sugiyono (2019), menjelaskan bahwa metode penelitian adalah cara ilmiah untuk mendapatkan data d

engan tujuan dan kegunaan tertentu, data yang diperoleh melalui penelitian adalah data empiris (teramati) dengan kriteria valid, reliable dan objektif. Metode yang digunakan adalah deskriptif kuantitatif. Metode deskriptif adalah suatu metode yang digunakan agar hasil penelitian dapat digambarkan atau dianalisis tetapi tidak digunakan untuk menghasilkan kesimpulan yang luas.

Rancangan Analisis Data

Rancangan analisis data pada penelitian ini dengan menerapkan Langkah-langkah:

- a. Mencari pengertian mengenai digital banking
 - b. Mencari apa saja yang termasuk ke dalam digital banking
 - c. Mengkaji apa saja yang dampak bagi pengguna
- Mengkaji sejauh mana risiko dari penggunaan digital banking.

4. HASIL DAN PEMBAHASAN

Secara konseptual, keamanan dipahami sebagai kondisi yang terbebas dari ancaman, risiko, atau gangguan yang dapat merusak aspek integritas, kerahasiaan, dan ketersediaan suatu sistem maupun informasi. Keamanan mencakup berbagai langkah protektif untuk melindungi informasi, sistem, serta aset dari potensi ancaman yang dapat merugikan individu, organisasi, bahkan negara. Dalam konteks perbankan, fokus utama keamanan diarahkan pada perlindungan data nasabah, transaksi keuangan, dan sistem perbankan secara menyeluruh guna mencegah peretasan, pencurian data, maupun penipuan daring (Widiana et al., 2023).

Perkembangan teknologi digital turut meningkatkan risiko kebocoran data, khususnya di sektor perbankan. Kebocoran data pribadi bukanlah fenomena baru, namun dampaknya semakin serius seiring meningkatnya ketergantungan pada sistem digital. Terbukanya informasi sensitif seperti nomor rekening, data identitas, atau informasi kartu kredit dapat menimbulkan berbagai konsekuensi negatif. Insiden tersebut dapat terjadi akibat serangan siber, kelemahan sistem internal, maupun kelalaian dalam pengelolaan data. Selain memicu risiko pencurian identitas dan penyalahgunaan keuangan, kebocoran data juga berpotensi menurunkan tingkat kepercayaan nasabah serta merusak reputasi institusi perbankan. Meskipun Indonesia tercatat sebagai salah satu negara dengan tingkat keamanan siber terbaik di kawasan ASEAN menurut National Cyber Security Index (NCSI), tantangan tetap ada. Oleh karena itu, Putri et al. (2023) menganalisis perlindungan nasabah BSI melalui kajian terhadap kebijakan keamanan, respons terhadap serangan siber, serta mekanisme perlindungan data nasabah.

Kepercayaan masyarakat terhadap keamanan layanan perbankan digital sangat dipengaruhi oleh pengalaman individu dalam menggunakan teknologi tersebut. Sari dan Fitri (2025) menjelaskan bahwa individu yang pernah mengalami atau mengetahui kasus kejahatan siber cenderung memiliki tingkat kewaspadaan lebih tinggi dan tingkat kepercayaan yang lebih rendah terhadap sistem perbankan digital. Sebaliknya, nasabah yang memperoleh edukasi memadai dan tidak memiliki pengalaman negatif cenderung lebih percaya dalam menggunakan layanan digital. Faktor usia dan tingkat pendidikan turut memengaruhi persepsi keamanan, di mana generasi muda umumnya lebih adaptif terhadap teknologi dibandingkan kelompok usia yang lebih tua. Oleh karena itu, peningkatan literasi digital dan edukasi keamanan menjadi aspek penting yang harus diperkuat, baik oleh masyarakat maupun oleh pihak perbankan, guna menciptakan ekosistem perbankan digital yang aman dan terpercaya.

Privasi dan keamanan data juga menjadi faktor utama yang menghambat adopsi layanan fintech. Stewart (2018) menyebutkan bahwa risiko penggunaan fintech lebih diperhatikan oleh pengguna dibandingkan kualitas produk itu sendiri. Oleh sebab itu, perlindungan terhadap kepentingan masyarakat harus menjadi prioritas utama. Penyelenggara layanan fintech dituntut untuk memperkuat tata kelola serta sistem keamanan teknologi yang digunakan. Selain itu, edukasi mengenai penggunaan layanan secara bijaksana dan rasional perlu dilakukan secara berkelanjutan. Peran regulator, seperti Bank Indonesia dan Otoritas Jasa Keuangan (OJK), menjadi sangat penting dalam memastikan penyelenggaraan layanan keuangan digital berjalan secara adaptif, proaktif, dan didukung oleh regulasi yang memadai.

Ariani (2017) menyatakan bahwa keamanan memiliki pengaruh signifikan terhadap minat penggunaan layanan digital. Apabila aspek keamanan dan kerahasiaan data tidak dikelola dengan baik oleh penyedia layanan, maka minat pengguna terhadap layanan tersebut cenderung menurun. Hal ini menunjukkan bahwa kepercayaan pengguna sangat bergantung pada sejauh mana penyedia layanan mampu menjamin keamanan informasi yang dikelola.

Kamil (2020) mengemukakan bahwa keamanan data dan informasi mencakup empat aspek utama, yaitu privasi atau kerahasiaan data, integritas informasi, autentikasi keaslian data, serta ketersediaan sistem dan informasi saat dibutuhkan. Keempat aspek tersebut saling berkaitan dan menjadi fondasi utama dalam menjaga keamanan sistem informasi digital, khususnya dalam layanan keuangan.

Siswanti (2022) menemukan bahwa tingkat keamanan penggunaan fintech berpengaruh positif dan signifikan terhadap minat masyarakat dalam menggunakan layanan tersebut. Keamanan dipersepsikan sebagai kondisi di mana pengguna merasa terlindungi dari risiko yang dapat menimbulkan kerugian. Semakin tinggi tingkat keamanan yang dirasakan, maka semakin besar pula minat masyarakat untuk memanfaatkan layanan fintech dalam aktivitas transaksinya.

Penelitian Matandatu (2025) menunjukkan bahwa tingkat pengetahuan keamanan siber dan perilaku praktik keamanan pengguna mobile banking berpengaruh signifikan terhadap persepsi risiko ancaman siber. Pengguna yang memahami risiko phishing, pentingnya pembaruan aplikasi, serta kelemahan penggunaan kata sandi yang sama cenderung lebih sadar terhadap potensi ancaman. Penerapan langkah protektif seperti penggunaan autentikasi dua faktor, penggantian kata sandi secara berkala, serta dukungan lingkungan sosial dan edukasi turut memperkuat kesadaran keamanan. Temuan ini menegaskan bahwa peningkatan keamanan mobile banking perlu mengintegrasikan edukasi berkelanjutan, teknologi yang mudah digunakan, serta dukungan sosial yang memadai.

Permana et al. (2024) mengungkapkan bahwa perlindungan privasi memiliki pengaruh signifikan terhadap tingkat kepercayaan pengguna aplikasi mobile banking. Sistem keamanan berbasis teknologi seperti OTP, biometrik, dan PIN dinilai mampu meningkatkan rasa aman pengguna. Meskipun demikian, aspek transparansi hukum terkait pengelolaan data pribadi masih memerlukan perhatian lebih lanjut. Generasi muda yang mendominasi pengguna layanan mobile banking menunjukkan tingkat kesadaran keamanan yang tinggi, namun tetap membutuhkan edukasi lanjutan agar dapat memanfaatkan fitur keamanan secara optimal.

Temuan tersebut menegaskan pentingnya inovasi berkelanjutan dalam teknologi keamanan serta penguatan regulasi perlindungan data pribadi. Dengan peningkatan aspek

tersebut, diharapkan kepercayaan pengguna terhadap layanan digital, khususnya mobile banking, dapat terus meningkat. Penelitian ini memberikan panduan strategis bagi penyedia layanan untuk mengembangkan sistem yang tidak hanya aman, tetapi juga adaptif terhadap perkembangan teknologi dan potensi penyalahgunaan.

Ali dan Fitri (2025) menjelaskan bahwa sektor perbankan menghadapi tingkat ancaman siber yang semakin kompleks di era digital. Inovasi teknologi memang meningkatkan efisiensi dan inklusi keuangan, namun rendahnya literasi digital nasabah menjadi tantangan tersendiri. Oleh karena itu, pengguna dituntut untuk lebih waspada serta menerapkan langkah-langkah pengamanan yang tepat dalam bertransaksi secara daring agar terhindar dari potensi kerugian.

Transformasi digital perbankan juga menuntut penerapan sistem keamanan siber yang efektif. Ancaman seperti pencurian data, ransomware, dan serangan DDoS menjadi risiko yang harus diantisipasi secara serius. Perlindungan terhadap data sensitif nasabah dan kelangsungan operasional layanan menjadi prioritas utama untuk mencegah kerugian finansial maupun reputasi. Upaya mitigasi risiko siber perlu dilakukan secara komprehensif melalui pendekatan teknis, kebijakan, serta peningkatan kesadaran pengguna.

Dengan berbagai tantangan tersebut, keberlangsungan layanan digital banking hingga saat ini masih dapat terjaga dengan baik. Tingkat kepercayaan masyarakat terhadap perbankan tetap terpelihara selama institusi perbankan mampu memberikan layanan yang responsif, aman, dan cepat dalam menangani permasalahan yang muncul selama proses digitalisasi berlangsung.

5. KESIMPULAN DAN SARAN

Kesimpulan ditulis secara singkat yaitu mampu menjawab tujuan atau permasalahan penelitian dengan menunjukkan hasil penelitian atau pengujian hipotesis penelitian, **tanpa** mengulang pembahasan. Kesimpulan ditulis secara kritis, logis, dan jujur berdasarkan fakta hasil penelitian yang ada, serta penuh kehati-hatian apabila terdapat upaya generalisasi. Bagian kesimpulan dan saran ini ditulis dalam bentuk paragraf, tidak menggunakan penomoran atau *bullet*. Pada bagian ini juga dimungkinkan apabila penulis ingin memberikan saran atau rekomendasi tindakan berdasarkan kesimpulan hasil penelitian. Demikian pula, penulis juga sangat disarankan untuk memberikan ulasan terkait keterbatasan penelitian, serta rekomendasi untuk penelitian yang akan datang.

DAFTAR REFERENSI

- Aini, Q., Rahardja, U., Arribathi, A. H., & Santoso, N. P. L. (2019). Penerapan *cloud accounting* dalam menunjang efektivitas laporan neraca pada perguruan tinggi. *CESS (Journal of Computer Engineering, Science and System)*, 4(1), 60–64. <https://doi.org/10.24114/cess.v4i1.12051>
- Ali, A., & Fitri, A. O. (2025). Keamanan perbankan di era digital: Tantangan dan solusinya. *Jurnal Bersama Ilmu Ekonomi*, 1(2), 154–165. <https://doi.org/10.55123/ekonom.v1i2.197>
- Ariani, M. Z. (2017). Pengaruh kualitas layanan, keamanan, dan risiko terhadap minat penggunaan LINE Pay. *Conference on Management and Behavioral Studies*, 457–467.
- James, K., Wolf, R., & David, W. (2020). *Cybersecurity in a digital era*. McKinsey & Company.
- Kamil, I. (2020). Pengaruh kemampuan finansial, kemudahan, dan keamanan terhadap perilaku penggunaan financial technology. *Jurnal Akuntansi dan Keuangan Islam*, 1(2), 98–114. <https://doi.org/10.24042/al-mal.v1i2.6501>
- Kato, C. (2019). Legal framework challenges to e-banking in Tanzania. *PSU Research Review*, 3(2), 101–110. <https://doi.org/10.1108/PRR-06-2018-0016>
- Kurnia, D. (2020). Pengaruh fitur, kemudahan penggunaan, keamanan, dan promosi terhadap keputusan penggunaan digital banking Jenius PT Bank Tabungan Pensiun Nasional. *UG Jurnal*, 14(8).
- Matandatu, S. (2025). Determinasi faktor-faktor kesadaran pengguna mobile banking terhadap ancaman keamanan siber di era digital. *Jejak Digital: Jurnal Ilmiah Multidisiplin*, 1(3), 567–577. <https://doi.org/10.63822/vmtade43>
- Pappu, R., & Saranya, G. (2018). Digital banking services: Customer perspectives. *Journal of Emerging Technologies and Innovative Research*, 5(12), 306–311.
- Permana, K. K., Eprianto, I., Fauzi, A., Minarny, T., Widyarora, S., & Fajriansyah, D. N. (2024). Pengaruh keamanan data pribadi terhadap kepercayaan pengguna di era transformasi digital: Studi kasus pada aplikasi mobile banking. *Orbit: Jurnal Ilmu Multidisiplin Nusantara*, 1(1). <https://doi.org/10.63217/orbit.v1i2.84>
- Putra, W. L., & Wiratnoko, D. (2021). Dampak layanan digital banking terhadap nasabah. *Jurnal Mahasiswa*, 3(1).
- Putri, D. F., Andriani, S., Sari, W. R., & Nabbila, F. L. (2023). Analisis perlindungan nasabah BSI terhadap kebocoran data dalam menggunakan digital banking. *Jurnal Ilmiah Ekonomi dan Manajemen*, 1(4).
- Robinson, K. A., Saldanha, I. J., & Mckoy, N. A. (2011). *Framework for identifying research gaps*. Johns Hopkins University.
- Sari, L. R., Anggraini, R., Kencanawati, M. S., & Sularto, L. (2022). Dampak keamanan, manfaat, kepercayaan, promosi, serta kemudahan pada keputusan pemanfaatan dompet elektronik ShopeePay. *METIK Jurnal*, 6(1). <https://doi.org/10.47002/metik.v6i1.335>
- Sestri, E., & H. (2018). Penggunaan metode *analytic hierarchy process* (AHP) dalam analisis faktor-faktor yang memengaruhi penggunaan transportasi daring. *Seminar Nasional Teknologi Informasi dan Multimedia*, 31–36.

- Sharma, P. (2019). *Impact of digitization on transaction banking in the financial industry*. Leeds University Business School.
- Siswanti, T. (2022). Analisis pengaruh manfaat ekonomi, keamanan, dan risiko terhadap minat penggunaan financial technology (FinTech): Studi kasus pada masyarakat di wilayah Kecamatan Bekasi Timur. *Jurnal Bisnis dan Akuntansi Unsurya*, 7(1), 44–61. <https://doi.org/10.35968/jbau.v7i2.899>
- Stewart, H., & ... (2018). Data security and consumer trust in FinTech innovation in Germany. *Information and Computer Security*, 26(1), 109–128. <https://doi.org/10.1108/ICS-06-2017-0039>
- Sugiyono. (2019). *Metode penelitian pendidikan (Kuantitatif, kualitatif, kombinasi, R&D, dan penelitian pendidikan)*. Alfabeta.
- Widiana, W., Anggara, F. S. A., Purnamasari, S., Nugraha, J. P., Ardianto, R., Harto, B., Nuraeni, Sulistiyo, H., Elsa, Suartini, S., B., S., & Dasman, S. (2023). *Keuangan bisnis digital*. PT Global Eksekutif Teknologi.