

Analisis Persepsi Masyarakat Terhadap Keamanan Dan Risiko *Cyber Crime* Dalam Perbankan Digital

Selvi Novita Sari ^{1*}, Anggun Okta Fitri ²

^{1,2}Perbankan Syariah, Universitas Islam Negeri Raden Intan Lampung>Nama Institusi

^{1*}nselvinovita1611@gmail.com, ²anggunoktafitri@radenintan.ac.id

Abstrak

Perkembangan teknologi informasi telah membawa perubahan signifikan dalam sektor perbankan, terutama dengan hadirnya layanan perbankan digital yang menawarkan kemudahan dan efisiensi dalam bertransaksi. Namun, di balik manfaat tersebut, terdapat tantangan yang berkaitan dengan keamanan data dan risiko kejahatan siber (*cyber crime*). Penelitian ini bertujuan untuk menganalisis persepsi masyarakat terhadap keamanan dan risiko *cyber crime* dalam perbankan digital. Metode yang digunakan dalam penelitian ini adalah studi pustaka (*literature review*) dengan pendekatan deskriptif kualitatif. Hasil penelitian menunjukkan bahwa persepsi masyarakat terhadap keamanan perbankan digital bervariasi, tergantung pada tingkat literasi digital, pengalaman pribadi, serta kepercayaan terhadap sistem keamanan yang diterapkan oleh bank. Sebagian masyarakat merasa aman berkat adanya fitur keamanan seperti enkripsi data, autentikasi dua faktor (2FA), dan pemantauan transaksi secara real-time. Namun, sebagian lainnya masih merasa khawatir akibat meningkatnya kasus kejahatan siber seperti phishing, peretasan akun, dan pencurian data pribadi. Faktor usia, tingkat pendidikan, serta pemahaman mengenai teknologi juga memengaruhi tingkat kepercayaan masyarakat terhadap perbankan digital. Penelitian ini menekankan pentingnya peningkatan literasi digital dan edukasi mengenai keamanan siber untuk mengurangi risiko kejahatan siber dalam perbankan digital.

Kata Kunci : Perbankan Digital, *Siber Cyber Crime*, Persepsi Masyarakat.

Abstract

The development of information technology has brought significant changes to the banking sector, particularly with the emergence of digital banking services that offer convenience and efficiency in transactions. However, behind these benefits lie challenges related to data security and the risks of cybercrime. This study aims to analyze public perceptions of security and cybercrime risks in digital banking. The research method used in this study is a literature review with a qualitative descriptive approach. The findings indicate that public perceptions of digital banking security vary depending on the level of digital literacy, personal experience, and trust in the security systems implemented by banks. Some individuals feel secure due to security features such as data encryption, two-factor authentication (2FA), and real-time transaction monitoring. However, others remain concerned about the rising cases of cybercrime, such as phishing, account hacking, and personal data theft. Factors such as age, education level, and understanding of technology also influence the level of public trust in digital banking. This study highlights the importance of enhancing digital literacy and cybersecurity education to mitigate the risks of cybercrime in digital banking.

Keyword : Digital Banking, Cybercrime, Public Perception.

1. PENDAHULUAN

Perkembangan teknologi informasi yang pesat telah mengubah berbagai aspek kehidupan, termasuk dalam sektor perbankan. Digitalisasi perbankan memungkinkan transaksi keuangan dilakukan dengan lebih cepat, mudah, dan efisien melalui layanan seperti mobile banking, internet banking, dan dompet digital (Zamzami AL & Fauzi AL. 2024). Keberadaan perbankan digital ini memberikan kemudahan bagi masyarakat dalam mengakses layanan keuangan tanpa harus datang langsung ke kantor bank. Di balik kemudahan tersebut, terdapat tantangan besar yang berkaitan dengan

keamanan data dan risiko kejahatan siber atau *cyber crime* (Moh Riskiyadi, Alexander A, & Tarjo 2021). Perbankan digital menjadi sasaran empuk bagi pelaku kejahatan siber yang memanfaatkan celah keamanan untuk mencuri data pribadi, informasi keuangan, atau bahkan melakukan pencurian dana nasabah. Beberapa bentuk serangan yang sering terjadi antara lain *phishing*, *malware*, *ransomware*, dan serangan peretasan (*hacking*) (Alvin T & Agus Zainul A. 2023). Masyarakat sebagai pengguna layanan perbankan digital memiliki persepsi yang beragam terhadap keamanan sistem ini.

Kepercayaan masyarakat terhadap keamanan perbankan digital sangat dipengaruhi oleh faktor literasi digital dan pengalaman pribadi. Pengguna yang memiliki pemahaman lebih baik tentang teknologi cenderung lebih berhati-hati dalam bertransaksi, misalnya dengan tidak sembarangan membagikan data pribadi atau menggunakan jaringan internet yang tidak aman (Bimo CU dan Atep AR. 2024). Mereka yang memiliki pengalaman buruk seperti terkena *scam* atau penipuan digital cenderung lebih skeptis terhadap keamanan layanan perbankan digital.

Kasus-kasus kejahatan *cyber* di sektor perbankan terus meningkat dari tahun ke tahun. Berdasarkan laporan berbagai lembaga keamanan siber, jumlah serangan siber terhadap perbankan digital meningkat seiring dengan meningkatnya jumlah pengguna layanan digital banking (Muhammad Irwan Padli, 2024). Hal ini menunjukkan bahwa sistem keamanan perbankan masih menjadi tantangan yang harus terus ditingkatkan agar dapat melindungi nasabah secara maksimal. Pihak perbankan sendiri telah melakukan berbagai upaya untuk meningkatkan sistem keamanan, mulai dari penggunaan kecerdasan buatan (*Artificial Intelligence*), sistem pemantauan transaksi secara real-time, hingga sosialisasi kepada nasabah tentang cara melindungi akun mereka dari serangan siber. Upaya ini tidak akan efektif jika masyarakat sebagai pengguna tidak memiliki kesadaran yang cukup terhadap pentingnya menjaga keamanan data pribadi dalam bertransaksi digital.

Tantangan utama dalam meningkatkan keamanan perbankan digital adalah bagaimana membangun keseimbangan antara kenyamanan pengguna dan perlindungan data. Meskipun fitur keamanan seperti verifikasi biometrik dan otentikasi ganda telah diterapkan, sebagian pengguna masih merasa bahwa proses ini terlalu rumit dan memperlambat transaksi. Akibatnya, banyak dari mereka yang cenderung mengabaikan langkah-langkah keamanan, seperti menggunakan kata sandi yang lemah atau mengklik tautan mencurigakan yang dapat mengarahkan mereka ke situs *phishing* (Abil, Rizky Dwi & Rahma, 2022). Lemahnya regulasi dan penegakan hukum terhadap kejahatan siber di beberapa negara juga menjadi faktor yang memperparah situasi. Banyak kasus pencurian data dan dana dari rekening nasabah yang sulit dilacak karena pelaku sering menggunakan jaringan anonim dan metode pencucian uang yang kompleks.

Oleh karena itu, diperlukan kerja sama antara pemerintah, perbankan, dan masyarakat untuk menciptakan ekosistem perbankan digital yang lebih aman. Dalam konteks Indonesia, tingkat literasi digital masyarakat masih menjadi kendala dalam penerapan sistem keamanan perbankan digital yang efektif. Masih banyak pengguna yang belum sepenuhnya memahami risiko yang dapat terjadi saat mereka menggunakan layanan perbankan digital secara tidak hati-hati. Edukasi tentang keamanan *cyber* harus lebih digencarkan agar masyarakat dapat memahami bagaimana cara melindungi diri dari ancaman kejahatan siber.

Seiring dengan meningkatnya penggunaan perbankan digital, penting untuk memahami bagaimana persepsi masyarakat terhadap keamanan sistem ini. Persepsi tersebut dapat memengaruhi keputusan mereka dalam menggunakan layanan perbankan digital, baik dalam hal frekuensi penggunaan maupun kepercayaan terhadap layanan perbankan tertentu. Jika masyarakat merasa bahwa layanan perbankan digital tidak cukup aman, mereka mungkin akan lebih memilih metode transaksi konvensional yang dianggap lebih dapat diandalkan.

Dengan memahami faktor-faktor yang mempengaruhi persepsi ini, diharapkan dapat memberikan gambaran yang lebih jelas mengenai tantangan yang dihadapi dalam upaya meningkatkan keamanan perbankan digital. Penelitian ini juga akan mengeksplorasi bagaimana berbagai faktor seperti usia,

tingkat pendidikan, pengalaman penggunaan teknologi, dan tingkat literasi digital memengaruhi persepsi masyarakat terhadap risiko kejahatan siber di sektor perbankan. Hal ini penting untuk mengetahui kelompok mana yang paling rentan terhadap ancaman siber dan bagaimana langkah-langkah pencegahan dapat lebih difokuskan.

2. METODE

Penelitian ini menggunakan pendekatan studi pustaka (*literature review*), yaitu metode penelitian yang dilakukan dengan mengumpulkan, menganalisis, dan mengevaluasi berbagai sumber literatur yang relevan (Dian Pertiwi dkk, 2023). Studi pustaka dipilih karena penelitian ini bertujuan untuk memahami persepsi masyarakat terhadap keamanan dan risiko *cyber crime* dalam perbankan digital (Sugiyono, 2019). Penelitian ini bersifat deskriptif kualitatif, di mana data yang dikumpulkan akan dianalisis secara mendalam untuk memahami bagaimana persepsi masyarakat terhadap keamanan dan risiko kejahatan siber dalam perbankan digital.

Data dalam penelitian ini diperoleh dari berbagai sumber kredibel, seperti jurnal ilmiah, buku referensi, laporan resmi dari Bank Indonesia dan Otoritas Jasa Keuangan (OJK), serta artikel berita yang membahas kasus kejahatan siber dalam perbankan digital. Pengumpulan data dilakukan dengan mengidentifikasi sumber yang relevan, mengevaluasi kredibilitasnya, menganalisis isi literatur, serta menyintesis data untuk mendapatkan pemahaman yang lebih luas mengenai topik penelitian. Analisis data dilakukan dengan metode analisis isi (*content analysis*), yang mencakup pengelompokan data berdasarkan tema utama, interpretasi hubungan antar konsep, serta penyusunan kesimpulan. Dari berbagai literatur yang dikaji, penelitian ini berupaya mengidentifikasi pola persepsi masyarakat terhadap keamanan perbankan digital dan langkah-langkah yang telah diambil untuk mengurangi risiko kejahatan siber.

3. HASIL DAN PEMBAHASAN

Analisis Persepsi Masyarakat terhadap Keamanan dan Risiko *Cyber Crime* dalam Perbankan Digital

Perbankan digital telah menjadi bagian tak terpisahkan dari kehidupan modern, memberikan kemudahan dalam melakukan transaksi keuangan secara cepat dan efisien. Dibalik kemajuan teknologi, muncul berbagai tantangan terkait keamanan, terutama yang berkaitan dengan risiko *cyber crime*. Kejahatan siber dalam perbankan digital mencakup berbagai ancaman, seperti pencurian data pribadi, peretasan akun, serta serangan phishing yang menargetkan nasabah. Maka dari itu terkait persepsi masyarakat terhadap keamanan perbankan digital menjadi faktor penting dalam menentukan tingkat kepercayaan dan adopsi layanan ini.

Masyarakat memiliki persepsi yang beragam terhadap keamanan perbankan digital, tergantung pada pemahaman mereka terhadap teknologi dan pengalaman mereka dalam menggunakan layanan perbankan online. Sebagian masyarakat merasa aman karena adanya fitur keamanan seperti autentikasi dua faktor (*two-factor authentication*), enkripsi data, serta kebijakan perlindungan konsumen yang diterapkan oleh bank. Sebagian lainnya masih merasa ragu dan khawatir terhadap potensi kebocoran data dan penyalahgunaan informasi pribadi. Kekhawatiran ini umumnya muncul akibat maraknya kasus peretasan dan penipuan digital yang semakin sering diberitakan di media.

Kepercayaan masyarakat terhadap keamanan perbankan digital juga sangat dipengaruhi oleh pengalaman pribadi. Mereka yang pernah mengalami atau mengetahui kasus *cyber crime* cenderung lebih waspada dan kurang percaya terhadap keamanan sistem perbankan online. Sebaliknya, nasabah yang belum pernah mengalami insiden keamanan dan merasa mendapat edukasi yang cukup dari pihak bank cenderung lebih percaya diri dalam menggunakan layanan perbankan digital. Edukasi dan literasi digital memainkan peran penting dalam membangun persepsi positif masyarakat terhadap keamanan perbankan digital. Faktor usia dan tingkat pendidikan juga berpengaruh terhadap persepsi masyarakat. Kelompok usia muda yang lebih akrab dengan teknologi umumnya lebih percaya diri dalam

menggunakan perbankan digital dibandingkan dengan kelompok usia yang lebih tua, yang sering kali masih memiliki ketergantungan pada transaksi konvensional. Di sisi lain, masyarakat dengan tingkat pendidikan lebih tinggi cenderung memiliki pemahaman yang lebih baik mengenai risiko *cyber crime* dan cara menghindarinya, sehingga lebih berhati-hati dalam menggunakan layanan digital.

Bank dan lembaga keuangan terus berupaya meningkatkan sistem keamanan guna mengurangi risiko kejahatan siber. Langkah-langkah seperti implementasi teknologi biometrik, sistem deteksi anomali, serta peningkatan keamanan aplikasi mobile banking telah diterapkan untuk melindungi nasabah. Namun, meskipun berbagai upaya telah dilakukan, celah keamanan tetap menjadi perhatian utama, terutama ketika penjahat siber semakin canggih dalam menciptakan metode kejahatan baru.

Masyarakat diharapkan semakin sadar akan pentingnya menjaga keamanan data pribadi mereka sendiri. Penggunaan kata sandi yang kuat, tidak membagikan informasi sensitif kepada pihak yang tidak dikenal, serta selalu memperbarui aplikasi perbankan adalah beberapa langkah yang dapat dilakukan untuk mengurangi risiko menjadi korban *cyber crime*. Pihak bank juga perlu terus melakukan sosialisasi dan edukasi kepada nasabah mengenai modus-modus kejahatan digital yang sedang berkembang.

Dengan meningkatnya kepercayaan masyarakat terhadap keamanan sistem perbankan digital, diharapkan adopsi layanan ini semakin luas. Namun, jika risiko *cyber crime* tidak ditangani dengan serius, maka akan berdampak pada menurunnya tingkat kepercayaan masyarakat, yang pada akhirnya dapat menghambat perkembangan digitalisasi perbankan. Oleh karena itu, diperlukan kerja sama antara bank, pemerintah, dan masyarakat dalam menciptakan ekosistem perbankan digital yang aman dan terpercaya.

Persepsi Masyarakat terhadap Tingkat Keamanan Perbankan Digital dalam Menghadapi Risiko Cyber Crime

Persepsi masyarakat terhadap keamanan perbankan digital sangat beragam, tergantung pada pemahaman individu tentang teknologi dan pengalaman mereka dalam menggunakan layanan digital banking. Sebagian masyarakat merasa percaya diri dalam menggunakan layanan perbankan digital karena adanya fitur keamanan seperti autentikasi dua faktor (*two-factor authentication*), enkripsi data, dan proteksi transaksi berbasis biometrik (Roganda Andreas Pakpahan dkk. 2024). Mereka menganggap bahwa bank telah menerapkan sistem keamanan yang cukup kuat untuk melindungi data dan transaksi mereka. Di sisi lain, masih banyak masyarakat yang merasa ragu dan khawatir terhadap keamanan perbankan digital. Ketakutan ini umumnya disebabkan oleh banyaknya kasus *cyber crime* yang sering diberitakan di media, seperti pencurian data, pembobolan akun, serta *phishing* yang menargetkan nasabah bank. Masyarakat yang kurang paham mengenai cara kerja sistem keamanan perbankan digital sering kali merasa bahwa layanan ini rentan terhadap serangan hacker dan penyalahgunaan data pribadi (Hayatin Nupus, Ayu Kartini, dan Lidia Desiana, 2025).

Oleh karena itu, penting bagi masyarakat untuk meningkatkan literasi digital dan memahami langkah-langkah pencegahan yang dapat dilakukan untuk mengurangi risiko menjadi korban kejahatan siber. Bank juga memiliki tanggung jawab untuk terus mengembangkan sistem keamanan yang lebih kuat serta memberikan edukasi secara berkelanjutan kepada nasabah. Sinergi antara pengguna dan penyedia layanan perbankan dalam menjaga keamanan digital akan membantu menciptakan ekosistem perbankan yang lebih aman dan terpercaya. Dengan demikian, persepsi masyarakat terhadap keamanan perbankan digital dapat semakin meningkat, sehingga mereka dapat memanfaatkan layanan ini dengan lebih nyaman dan percaya diri.

Faktor-Faktor yang Memengaruhi Tingkat Kepercayaan Masyarakat terhadap Keamanan Layanan Perbankan Digital

Beberapa faktor utama yang memengaruhi kepercayaan masyarakat terhadap keamanan layanan perbankan digital meliputi tingkat literasi digital, pengalaman pribadi dalam menggunakan layanan perbankan digital, usia, tingkat pendidikan, serta regulasi dan kebijakan yang diterapkan oleh perbankan dan pemerintah.

Masyarakat yang memiliki tingkat literasi digital tinggi umumnya lebih memahami cara melindungi data pribadi dan mengenali modus kejahatan siber (B. Junedi Hutagaol, Riama Santy Sitorus, dan Nindya Hutagaol, 2024). Mereka lebih percaya diri dalam menggunakan layanan perbankan digital karena memahami mekanisme keamanan yang diterapkan oleh bank. Masyarakat yang masih kurang memahami teknologi digital cenderung lebih waspada atau bahkan menghindari penggunaan layanan digital banking karena khawatir menjadi korban kejahatan siber. Pengalaman pribadi juga berperan besar dalam membentuk kepercayaan masyarakat. Mereka yang pernah mengalami insiden seperti kebocoran data atau penipuan online biasanya menjadi lebih waspada dan skeptis terhadap sistem keamanan perbankan digital. Sebaliknya, nasabah yang merasa bahwa layanan digital banking yang mereka gunakan selalu aman dan nyaman akan cenderung lebih percaya terhadap sistem perbankan digital.

Usia dan tingkat pendidikan juga memengaruhi persepsi masyarakat. Kelompok usia muda yang lebih akrab dengan teknologi cenderung lebih percaya pada sistem keamanan digital dibandingkan dengan kelompok usia yang lebih tua, individu dengan pendidikan lebih tinggi umumnya lebih memahami risiko *cyber crime* dan bagaimana cara menghindarinya, sehingga lebih berhati-hati dalam menggunakan layanan perbankan digital.

Regulasi dan kebijakan yang diterapkan oleh bank serta otoritas keuangan, seperti Bank Indonesia dan Otoritas Jasa Keuangan (OJK), juga memiliki pengaruh besar terhadap kepercayaan masyarakat. Jika bank secara aktif memberikan perlindungan terhadap nasabah serta menyediakan informasi yang transparan terkait keamanan, maka kepercayaan masyarakat terhadap layanan perbankan digital akan semakin meningkat.

Upaya Perbankan dalam Meningkatkan Kepercayaan Masyarakat terhadap Keamanan Transaksi Digital dan Efektivitasnya

Bank memiliki peran penting dalam meningkatkan kepercayaan masyarakat terhadap keamanan transaksi digital dengan menerapkan berbagai strategi keamanan yang canggih dan inovatif. Salah satu upaya utama adalah penguatan sistem keamanan melalui teknologi seperti enkripsi data, autentikasi dua faktor (2FA), serta pemantauan transaksi secara real-time untuk mendeteksi aktivitas mencurigakan. Bank juga menerapkan kebijakan perlindungan nasabah, seperti pemberian notifikasi transaksi, batasan jumlah transaksi, serta prosedur verifikasi yang ketat untuk mencegah akses tidak sah (Kemal Idris, Aulia Rahman dan Frygyta Dwi, 2024). Keamanan ini diperkuat dengan kerja sama antara bank dan lembaga keamanan siber guna memastikan bahwa sistem perbankan digital selalu diperbarui terhadap ancaman kejahatan siber terbaru. Selain aspek teknis, bank juga berupaya membangun kepercayaan masyarakat dengan meningkatkan literasi digital dan edukasi terkait keamanan siber. Penyediaan layanan pelanggan yang responsif dan transparan juga menjadi faktor penting dalam membangun kepercayaan. Ketika nasabah merasa didukung dan mendapatkan solusi yang cepat saat menghadapi masalah keamanan, mereka akan lebih yakin untuk tetap menggunakan layanan perbankan digital.

Efektivitas dari upaya ini dapat terlihat dari meningkatnya jumlah pengguna perbankan digital serta rendahnya tingkat keluhan atau kasus kejahatan siber yang berhasil menembus sistem perbankan (Taufik Kukuh Efendi, 2024). Tantangan tetap ada, terutama dalam menghadapi metode kejahatan yang semakin canggih dan sulit dideteksi. Untuk meningkatkan efektivitas upaya yang dilakukan, bank perlu bekerja sama dengan pemerintah dan lembaga keamanan siber untuk menciptakan regulasi yang lebih ketat serta mekanisme perlindungan yang lebih baik bagi nasabah. Edukasi mengenai keamanan digital harus lebih luas dan menjangkau semua lapisan masyarakat, terutama kelompok yang masih rentan terhadap ancaman *cyber crime*. Bank harus terus berinovasi dalam teknologi keamanan serta memastikan bahwa edukasi dan perlindungan bagi nasabah berjalan secara konsisten. Dengan pendekatan yang komprehensif ini, kepercayaan masyarakat terhadap keamanan transaksi digital dapat

terus meningkat, sehingga mendukung pertumbuhan ekosistem perbankan digital yang lebih aman dan andal.

4. KESIMPULAN

Perbankan digital memberikan kemudahan dalam transaksi keuangan, tetapi juga menghadirkan tantangan keamanan, terutama terkait risiko *cyber crime* seperti pencurian data dan peretasan akun. Persepsi masyarakat terhadap keamanan layanan ini bervariasi, tergantung pada pemahaman teknologi, pengalaman pribadi, serta faktor usia dan pendidikan. Masyarakat yang memiliki literasi digital tinggi cenderung lebih percaya diri menggunakan layanan ini, sementara mereka yang kurang memahami teknologi lebih rentan terhadap kekhawatiran akan kebocoran data dan penipuan. Untuk meningkatkan kepercayaan masyarakat, perbankan telah menerapkan berbagai teknologi keamanan seperti autentikasi dua faktor dan sistem deteksi anomali.

Namun, ancaman *cyber crime* terus berkembang, sehingga diperlukan kerja sama antara bank, pemerintah, dan masyarakat dalam meningkatkan sistem keamanan dan edukasi digital. Jika risiko ini tidak ditangani dengan serius, tingkat kepercayaan masyarakat bisa menurun, yang dapat menghambat pertumbuhan perbankan digital. Oleh karena itu, inovasi keamanan dan kesadaran akan pentingnya perlindungan data pribadi harus terus diperkuat.

5. DAFTAR PUSTAKA

- Ahmadi Abu, "*Psikologi Umum*", Jakarta: Rieka Cipta, 2009.
- Dian Pertiwi dkk., "Bank Digital Sebagai Peradaban Lembaga Keuangan Syariah Di Indonesia," *Indonesian Scientific Journal of Islamic Finance*, 1, (2) 2023. 172-182.
- Hayatin Nupus, Ayu Kartini, dan Lidia Desiana. "Pengaruh Cyber Crime dan Persepsi Keamanan Terhadap Tingkat Kepercayaan Pengguna Produk E-banking (Survei Pada Pengguna E-banking Bank Syariah di Indonesia)." *Jurnal Semesta Ilmu Manajemen dan Ekonomi* 1, no. 3 (4 Februari 2025): 102-16.
- Hidayatullah Cahyo, "Jenis Dan Dampak Cyber Crime," *Prosiding SAINTEK: Sains Dan Teknologi* 2, no. 1 (2023): 216-21
- Hutagaol, B. Junedi, Riama Santy Sitorus, dan Nindya Hutagaol. "Identifikasi Tingkat Kesadaran Pengguna Mobile Banking terhadap Ancaman Cybercrime." *Jurnal Teknologi Sistem Informasi dan Aplikasi* 7, no. 3 (31 Juli 2024): 1043-54.
- Idris Balaka, Kemal, Aulia Rahman Hakim, dan Frygyta Dwi Sulistyany. "Pencurian Informasi Nasabah Di Sektor Perbankan: Ancaman Serius Di Era Digital." *Yustitiabelen* 10, no. 2 (1 Agustus 2024): 105-30.
- Mauliza, Abil Yositya Indah, Rizky Dwi Salsabilla Machmudi, dan Rachma Indrarini. "Pengaruh Perlindungan Data Dan Cyber Security Terhadap Tingkat Kepercayaan Menggunakan Fintech Masyarakat Di Surabaya." *SIBATIK JOURNAL: Jurnal Ilmiah Bidang Sosial, Ekonomi, Budaya, Teknologi, dan Pendidikan* 1, no. 11 (30 Oktober 2022): 2497-2516.
- Muhammad Esza Maulana Firmanda, Taufik Kukuh Efendi. "Analisis Kebijakan Perlindungan Nasabah Pada Bank Digital Syariah di Indonesia," 2 November 2024.
- Pakpahan, Roganda Andreas, Achmad Fauzi, Fadhli Nursal, Ade Ilham Prasetyo, Crist Doohan Ananda Mayki, Pharosandika Sihombing, dan Michael Laurence. "Cyber Crime dan Tingkat Kepercayaan Terhadap Penggunaan Produk E-Banking" 3, no. 3 (2024).
- Pertiwi, Dian, Amin Suyitno, Endang Rochmiatun, dan Widiya Nur Anisa. "Bank Digital Sebagai Peradaban Lembaga Keuangan Syariah Di Indonesia," *Indonesian Scientific Journal of Islamic Finance*, 2 (1) 2023, 172-182.

- Riskiyadi, Moh, Alexander Anggono, dan Tarjo. "Cybercrime dan Cybersecurity pada Fintech: Sebuah Tinjauan Pustaka Sistematis." *Jurnal Manajemen dan Organisasi* 12, no. 3 (29 Desember 2021): 239-51.
- Rohid Akbar, Muhammad Irwan Padli Nasution. "Analisis Keamanan Data Pada Aplikasi Mobile Banking," 25 Juni 2024.
- Simatupang, Jones P, Helena Thatcher Pakpahan, Lince R. Panataria, Donny Simatupang, dan Kenal Hutapea. "Strategi pengembangan agrowisata jeruk petik sendiri di Kecamatan Merek Kabupaten Karo." *Jurnal Agrotek Ummat* 9, no. 1 (31 Januari 2022): 65.
- Sugiyono, Metode Penelitian Kuantitatif, Kualitatif, dan R&D. Bandung : Alfabeta, 2019.
- Tanuwijaya, Alvin, dan Agus Zainul Arifin. "Persepsi Risiko Pada Penggunaan M-Banking Dalam Layanan Perbankan D Indonesia," *Jurnal Distribusi*, 11 (2), 2023, 165-180.
- Toha Mifta, "*Perilaku Organisasi Konsep Dasar Dan Aplikasinya*", Jakarta: Rajawali Press, 2007.
- Utomo, Bimo Cokro, dan Atep Aulia Rahman. "Analisis Kesadaran Keamanan Data Pribadi pada Pengguna E-Wallet DANA." *JRST (Jurnal Riset Sains dan Teknologi)* 8, no. 2 (4 Oktober 2024): 155.
- Zamzami Akromi Lubis dan Fauzi Arif Lubis. "Pengaruh Persepsi Keamanan dan Kepercayaan Terhadap Loyalitas Nasabah: Studi Kasus Serangan Siber di Bank Syariah Indonesia." *El-Mal: Jurnal Kajian Ekonomi & Bisnis Islam* 5, no. 10 (7 Oktober 2024).
- Zed, Mestika, Metode Penelitian Kepustakaan. Jakarta : Yayasan Obor Indonesia, 2003.