

Peran Artificial Intelligence dalam Mitigasi Risiko Transaksi Mobile Banking: Tinjauan Governansi dan Etika Data

Erni Wiriani, Jauharil Maknuni*, Esti Alemlia Puspita, Masitah Masitah

Program Studi Keuangan Dan Perbankan, Akademi Keuangan Perbankan Nusantara

Jln.Medan-Banda Aceh, Kampung Beusa, Peureulak Barat, Aceh Timur, Indonesia

Email: ¹erniwiriani71@gmail.com, ^{2,*}jauharilmaknuni537@gmail.com ³estialemliapuspitas@gmail.com, ⁴masitahdea@gmail.com

Email Penulis Korespondensi: jauharilmaknuni537@gmail.com

Abstrak—Kemajuan teknologi kecerdasan buatan (Artificial Intelligence/AI) telah membawa transformasi signifikan dalam sektor perbankan digital, khususnya pada layanan mobile banking. Salah satu tantangan utama dalam perkembangan ini adalah meningkatnya risiko transaksi mencurigakan, termasuk penipuan dan penyalahgunaan data. Penelitian ini bertujuan untuk menganalisis peran AI dalam memitigasi risiko transaksi mencurigakan serta meninjau aspek governansi dan etika data yang menyertainya. Dengan menggunakan pendekatan kualitatif melalui studi literatur dan studi kasus pada Bank Syariah Indonesia cabang Aceh Timur yang telah mengimplementasikan sistem deteksi fraud berbasis AI, data penelitian diperoleh dari analisis dokumen internal bank, wawancara mendalam dengan staf IT dan manajer kepatuhan, serta observasi terhadap proses operasional mobile banking. Hasil penelitian menunjukkan bahwa AI mampu meningkatkan kecepatan dan akurasi dalam mendeteksi pola transaksi tidak wajar secara real time. Namun, efektivitas implementasi AI sangat bergantung pada tata kelola teknologi yang baik, kebijakan perlindungan data yang ketat, serta kesesuaian sistem dengan prinsip etika dan transparansi. Selain itu, keberhasilan mitigasi risiko juga ditentukan oleh kemampuan lembaga keuangan dalam menjaga akuntabilitas algoritma dan memastikan tidak adanya bias dalam pengambilan keputusan otomatis. Studi ini menegaskan pentingnya sinergi antara inovasi teknologi dan prinsip governansi yang kuat untuk menciptakan sistem keuangan digital yang aman, terpercaya, dan berkeadilan. Rekomendasi disampaikan untuk penguatan kebijakan internal perbankan terkait audit algoritma, perlindungan data nasabah, dan pelatihan etika digital bagi pengembang sistem AI.

Kata Kunci: Kecerdasan Buatan; Mobile Banking; Mitigasi Risiko; Deteksi Penipuan; Governansi Teknologi

Abstract—The advancement of Artificial Intelligence (AI) technology has brought significant transformation in the digital banking sector, particularly in mobile banking services. One of the main challenges in this development is the increasing risk of suspicious transactions, including fraud and data misuse. This study aims to analyze the role of AI in mitigating the risks of suspicious transactions while reviewing the accompanying aspects of data governance and ethics. Using a qualitative approach through literature review and a case study at Bank Syariah Indonesia, Aceh Timur branch, which has implemented an AI-based fraud detection system, research data were obtained from the analysis of internal bank documents, in-depth interviews with IT staff and compliance managers, as well as observations of mobile banking operational processes. The findings indicate that AI is capable of enhancing both speed and accuracy in detecting unusual transaction patterns in real time. However, the effectiveness of AI implementation highly depends on sound technology governance, strict data protection policies, and the system's alignment with ethical principles and transparency. In addition, the success of risk mitigation is also determined by the ability of financial institutions to maintain algorithm accountability and ensure the absence of bias in automated decision-making. This study emphasizes the importance of synergy between technological innovation and strong governance principles to create a safe, trustworthy, and equitable digital financial system. Recommendations are provided to strengthen internal banking policies related to algorithm auditing, customer data protection, and digital ethics training for AI system developers.

Keywords: Artificial Intelligence; Mobile Banking; Risk Mitigation; Fraud Detection; Technology Governance

1. PENDAHULUAN

Perkembangan teknologi digital yang sangat pesat telah membawa dampak signifikan terhadap transformasi industri jasa keuangan, khususnya sektor perbankan. Salah satu manifestasi utama dari transformasi ini adalah meningkatnya penggunaan layanan mobile banking oleh masyarakat dalam menjalankan aktivitas finansial sehari-hari, seperti transfer dana, pembayaran tagihan, dan pembelian produk keuangan secara daring. Meskipun layanan ini menawarkan kemudahan dan efisiensi, kompleksitas transaksi digital turut meningkatkan kerentanan terhadap ancaman keamanan, seperti serangan siber, penipuan (*fraud*), dan pencurian identitas (Johora et al., 2024). Hal ini menunjukkan bahwa kasus *fraud* harus menjadi perhatian yang harus dimitigasi oleh setiap organisasi (Baqir & Sulhani, 2023). Untuk menjawab tantangan ini, adopsi teknologi kecerdasan buatan (Artificial Intelligence/AI) menjadi langkah strategis dalam memperkuat sistem pengawasan dan keamanan transaksi finansial.

Penerapan AI dalam sistem perbankan memungkinkan analisis terhadap volume data transaksi dalam jumlah besar dengan kecepatan tinggi. Dengan memanfaatkan pendekatan *machine learning*, sistem dapat mempelajari pola-pola transaksi normal dan mendeteksi penyimpangan yang berpotensi sebagai tindakan mencurigakan. Teknologi ini mampu memberikan notifikasi secara real time terhadap aktivitas yang tidak lazim, seperti transaksi dalam jumlah besar yang tidak sesuai dengan profil nasabah atau transaksi dari lokasi geografis yang tidak biasa (Awosika et al., 2023; Ridzuan et al, 2024). Efisiensi dan keakuratan dalam deteksi penipuan ini menjadikan AI sebagai elemen penting dalam strategi perlindungan aset digital bank. Meskipun demikian, keberhasilan teknologi ini tidak hanya ditentukan oleh kemampuannya dalam mengenali risiko, tetapi juga oleh adanya kerangka *governance* yang memadai dan penerapan prinsip-prinsip etika data yang konsisten.

Governance teknologi AI merupakan aspek krusial dalam penggunaan sistem otomatis untuk layanan publik dan keuangan. *Governance* ini meliputi seperangkat kebijakan, regulasi, dan praktik yang menjamin pengembangan dan pemanfaatan teknologi secara etis, transparan, dan bertanggung jawab (Bas et al., 2025). Dalam konteks perbankan, tata kelola yang baik harus mampu menjamin bahwa sistem AI tidak memproduksi keputusan yang bias, diskriminatif, atau melanggar privasi nasabah. Ketidakseimbangan dalam regulasi dan lemahnya pengawasan teknologi dapat menimbulkan kerugian sistemik dan mengikis kepercayaan publik (Iqbal et al., 2025). Oleh karena itu, tata kelola AI harus dilengkapi dengan mekanisme evaluasi dan audit berkala, serta partisipasi pemangku kepentingan lintas sektor untuk menjamin keadilan dan transparansi.

Selain tata kelola, aspek etika data juga menjadi perhatian utama dalam pengembangan sistem AI yang bertanggung jawab. Etika data mengacu pada prinsip moral dalam perlakuan terhadap data pribadi, termasuk proses pengumpulan, penyimpanan, penggunaan, dan distribusinya. Dalam sistem berbasis AI, data adalah komponen inti yang menentukan keakuratan dan objektivitas hasil analisis. Oleh karena itu, penting bagi lembaga keuangan untuk menjamin *informed consent*, perlindungan terhadap identitas individu melalui proses anonimisasi, serta hak akses dan kontrol data oleh pemiliknya (Sain & Adinugraha, 2025). Kegagalan dalam menerapkan prinsip-prinsip ini dapat menimbulkan risiko hukum, reputasi, dan ketidakpercayaan masyarakat. Dengan demikian, integrasi antara kemajuan teknologi dan kerangka etika yang kuat menjadi syarat utama dalam membangun ekosistem keuangan digital yang adil, aman, dan berkelanjutan.

Meskipun terdapat sejumlah penelitian sebelumnya yang membahas pemanfaatan AI dalam deteksi penipuan di sektor perbankan, sebagian besar penelitian tersebut masih menitikberatkan pada aspek teknis seperti akurasi algoritma, efisiensi sistem, dan model pembelajaran mesin yang digunakan (Johora et al., 2024; Ridzuan et al., 2024). Relatif sedikit kajian yang secara eksplisit mengeksplorasi dimensi *governance* dan etika data, khususnya dalam konteks perbankan syariah yang memiliki prinsip kehati-hatian dan nilai-nilai kepatuhan syariah sebagai landasan operasional (Iqbal et al., 2022; Sain & Adinugraha, 2025). Kekosongan penelitian ini menunjukkan adanya kebutuhan mendesak untuk mengkaji bagaimana integrasi antara inovasi teknologi dan tata kelola yang beretika dapat menciptakan sistem keuangan digital yang tidak hanya aman dan efektif, tetapi juga sejalan dengan nilai keadilan dan kepercayaan publik.

Berdasarkan uraian di atas, penelitian ini bertujuan untuk menganalisis secara mendalam bagaimana kecerdasan buatan dapat berperan dalam mendeteksi dan memitigasi risiko transaksi mencurigakan dalam layanan *mobile banking*. Fokus utama diarahkan pada bagaimana lembaga keuangan yang menerapkan sistem AI berlandaskan tata kelola yang akuntabel serta etika data yang dapat dipertanggungjawabkan. Kajian ini diharapkan tidak hanya memberikan kontribusi teoritis terhadap pengembangan literatur di bidang teknologi keuangan, tetapi juga menawarkan wawasan praktis bagi perbankan dalam merancang kebijakan teknologi yang inklusif dan berorientasi pada perlindungan nasabah.

2. METODE PENELITIAN

2.1 Kerangka Dasar Penelitian

Penelitian ini menggunakan pendekatan kualitatif dengan metode studi kasus untuk menggali secara mendalam implementasi sistem deteksi transaksi mencurigakan berbasis Artificial Intelligence (AI) pada layanan *mobile banking*. Studi difokuskan pada Bank Syariah Indonesia (BSI) cabang Aceh Timur, sebagai salah satu institusi keuangan yang telah mengadopsi teknologi AI dalam proses mitigasi risiko transaksi. Pendekatan kualitatif dipilih karena sesuai untuk memahami fenomena kompleks, seperti integrasi teknologi dan dampaknya terhadap tata kelola serta etika data dalam praktik perbankan digital (Schoonenboom, 2021; Rahi, 2020; Nowell & Albrecht, 2019).

2.2 Lokasi dan Objek Penelitian

Lokasi penelitian berada di Bank Syariah Indonesia (BSI) cabang Aceh Timur. Objek penelitian mencakup sistem AI yang digunakan dalam mendeteksi fraud atau aktivitas transaksi mencurigakan, kebijakan governansi yang mengatur penggunaannya, serta prinsip-prinsip etika data yang diterapkan. Penelitian menekankan pada praktik nyata dan kebijakan internal bank yang berkaitan dengan deteksi transaksi mencurigakan.

2.3 Teknik Pengumpulan Data

Data dikumpulkan melalui beberapa teknik, yaitu:

- Wawancara mendalam dengan pejabat teknologi informasi, analis risiko, dan petugas kepatuhan di BSI Aceh Timur untuk memperoleh informasi langsung mengenai penerapan AI.
- Studi dokumentasi, termasuk analisis terhadap kebijakan internal bank, pedoman etika data, dan prosedur sistem deteksi fraud.
- Studi literatur yang mencakup jurnal ilmiah, laporan riset industri, serta regulasi nasional dan internasional terkait AI dan perbankan digital.

Teknik triangulasi data diterapkan untuk memastikan validitas dan reliabilitas temuan.

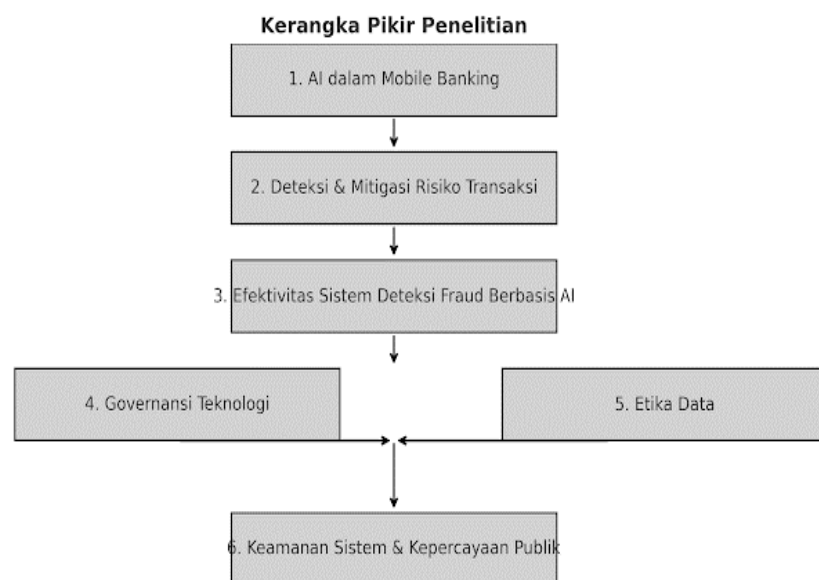
2.4 Teknik Analisis Data

Data dianalisis menggunakan analisis tematik, yaitu dengan mengidentifikasi tema-tema utama seperti efektivitas sistem deteksi, tata kelola teknologi, serta prinsip-prinsip etika yang diimplementasikan. Setiap tema dikodekan, dikategorikan, dan dikaitkan dengan teori serta literatur yang relevan. Pendekatan ini memungkinkan peneliti untuk menafsirkan makna mendalam dari hasil temuan dan menghasilkan pemahaman komprehensif (Braun & Clarke, 2019).

2.5 Validitas Penelitian

Validitas diperkuat melalui member checking kepada narasumber kunci untuk mengonfirmasi hasil interpretasi data, serta menggunakan sumber data dan metode yang beragam untuk membandingkan hasil (Denzin & Lincoln, 2018). Dengan pendekatan ini, penelitian diharapkan mampu menghasilkan gambaran objektif mengenai bagaimana AI berperan dalam mitigasi risiko transaksi mencurigakan dan bagaimana governansi serta etika data dijalankan dalam praktiknya.

2.6 Kerangka Pemikiran



Gambar 1. Kerangka pikir

Gambar 1 kerangka Pikir menjelaskna (1) AI dalam Mobile Banking Penerapan teknologi kecerdasan buatan dalam aplikasi mobile banking digunakan untuk meningkatkan efisiensi, keamanan, dan akurasi layanan digital perbankan.(2) Deteksi & Mitigasi Risiko Transaksi AI digunakan untuk mendeteksi pola anomali pada transaksi keuangan dan membantu mencegah fraud atau penyalahgunaan akun. (3) Efektivitas Sistem Deteksi Fraud Berbasis AI Menilai sejauh mana AI mampu mengurangi insiden fraud dan false alarm, serta bagaimana sistem belajar dari data untuk meningkatkan akurasi deteksi. (4) Governansi Teknologi dan Etika Data Dua pilar penting dalam implementasi AI governansi mengatur tata kelola dan tanggung jawab teknologi, sedangkan (5) etika data memastikan perlindungan privasi dan keadilan dalam proses otomatisasi keputusan. (6) Keamanan Sistem & Kepercayaan Publik Efektivitas, transparansi, dan etika dalam sistem AI akan membentuk persepsi masyarakat terhadap keandalan layanan mobile banking, yang pada akhirnya berpengaruh terhadap kepercayaan pengguna.

3. HASIL DAN PEMBAHASAN

3.1 Peningkatan Kecepatan dan Akurasi Deteksi

Temuan ini merupakan inti dari manfaat AI dalam deteksi fraud. AI secara signifikan meningkatkan kecepatan dan akurasi dalam mendeteksi pola transaksi tidak wajar secara *real-time*. Sistem AI mampu menganalisis volume data transaksi yang sangat besar dalam waktu singkat, mengidentifikasi anomali yang mungkin terlewatkan oleh metode deteksi manual atau berbasis aturan konvensional. Ini memungkinkan bank untuk merespons potensi penipuan lebih cepat dan meminimalkan kerugian finansial.

3.1.1. Pemrosesan Data Skala Besar dan Kecepatan *Real-time*

Di era *mobile banking*, jutaan transaksi terjadi setiap hari. Metode tradisional, yang bergantung pada pemeriksaan manual atau aturan statis, akan kewalahan menghadapi volume data sebesar ini. AI, dengan arsitektur komputasi

paralel dan algoritma *machine learning* yang efisien, dapat memproses dan menganalisis setiap transaksi dalam hitungan milidetik. Ini berarti anomali dapat terdeteksi saat transaksi sedang berlangsung, bukan setelah kerugian terjadi. Kemampuan ini memungkinkan bank untuk mengambil tindakan pencegahan seperti memblokir transaksi, mengirim notifikasi peringatan, atau bahkan menangguhkan akun yang mencurigakan secara instan.

3.1.2 Identifikasi Pola Anomali yang Kompleks dan Tersembunyi

Kekuatan utama AI terletak pada kemampuannya untuk mempelajari dan mengidentifikasi pola yang tidak dapat dikenali oleh manusia atau sistem berbasis aturan sederhana. Penipu terus mengembangkan modus operandi yang lebih canggih, seringkali meniru perilaku transaksi normal untuk menghindari deteksi. Algoritma AI, seperti *deep learning* atau *unsupervised learning*, dapat:

- Mendeteksi *Outlier*: Mengidentifikasi transaksi yang secara signifikan menyimpang dari pola kebiasaan nasabah (misalnya, transaksi dalam jumlah besar di lokasi yang tidak biasa atau pada waktu yang tidak lazim).
- Mengenali Jaringan Penipuan: Menganalisis hubungan antar transaksi, akun, atau perangkat untuk menemukan jaringan penipuan yang terorganisir.
- Beradaptasi dengan Modus Baru: Melalui pembelajaran berkelanjutan (*continuous learning*), model AI dapat secara otomatis memperbarui pengetahuannya tentang pola penipuan baru yang muncul, mengurangi waktu yang dibutuhkan untuk mengembangkan aturan deteksi baru.

3.1.3 Reduksi *False Positives* dan Peningkatan Efisiensi

Sistem berbasis aturan seringkali menghasilkan banyak *false positives* (transaksi sah yang salah dikategorikan sebagai fraud), yang dapat mengganggu pengalaman nasabah dan membebani tim fraud. AI, dengan kemampuannya untuk membedakan antara variasi perilaku normal dan anomali asli dengan akurasi lebih tinggi, dapat secara signifikan mengurangi *false positives*. Ini tidak hanya meningkatkan kepuasan nasabah tetapi juga membebaskan analisis fraud untuk fokus pada kasus-kasus yang benar-benar berisiko tinggi, meningkatkan efisiensi operasional bank.

3.2 Ketergantungan pada Tata Kelola Teknologi yang Baik

Efektivitas implementasi AI dalam mitigasi risiko sangat bergantung pada adanya tata kelola teknologi yang baik. Ini mencakup kerangka kerja yang jelas untuk pengembangan, implementasi, dan pemeliharaan sistem AI. Tanpa governansi yang kuat, potensi AI untuk mitigasi risiko tidak dapat dimanfaatkan secara optimal, dan bahkan dapat menimbulkan risiko baru.

- Kerangka Kerja Komprehensif: Tata kelola teknologi yang baik berarti bank harus memiliki kebijakan, prosedur, dan standar yang jelas untuk setiap fase siklus hidup sistem AI, mulai dari perencanaan, desain, pelatihan model, implementasi, pemantauan, hingga pembaruan dan penghentian. Ini mencakup pemilihan algoritma, sumber data pelatihan, validasi model, dan kriteria kinerja. Tanpa kerangka kerja yang jelas, implementasi AI bisa menjadi tidak terstruktur, tidak konsisten, dan rentan terhadap kegagalan.
- Manajemen Risiko yang Terintegrasi: Sistem AI dapat memperkenalkan risiko baru, seperti risiko model (ketidakakuratan atau bias dalam algoritma), risiko operasional (gangguan sistem), dan risiko keamanan siber (kerentanan terhadap serangan). Tata kelola yang efektif memastikan bahwa risiko-risiko ini diidentifikasi, dinilai, dimitigasi, dan dipantau secara berkelanjutan. Integrasi AI ke dalam kerangka manajemen risiko perusahaan adalah esensial untuk memastikan bahwa manfaat AI tidak diimbangi oleh potensi kerugian.
- Struktur Organisasi dan Akuntabilitas: Diperlukan pembentukan tim atau komite khusus yang bertanggung jawab atas pengawasan AI, termasuk ahli data, insinyur AI, pakar etika, dan perwakilan hukum. Kejelasan peran dan tanggung jawab, serta jalur akuntabilitas yang transparan, memastikan bahwa ada pihak yang bertanggung jawab atas kinerja dan dampak sistem AI. Di BSI cabang Aceh Timur, ini mungkin berarti adanya tim internal yang berkolaborasi dengan kantor pusat untuk implementasi dan pemantauan sistem.

3.3 Pentingnya Kebijakan Perlindungan Data yang Ketat

Kesuksesan sistem deteksi fraud berbasis AI sangat terkait dengan kebijakan perlindungan data yang ketat. AI mengandalkan akses terhadap data nasabah dalam jumlah besar untuk melatih model dan mendeteksi anomali. Oleh karena itu, perlindungan data pribadi nasabah dari penyalahgunaan, kebocoran, atau akses tidak sah adalah mutlak.

- Volume dan Sensitivitas Data: Sistem AI untuk deteksi fraud memerlukan akses ke berbagai jenis data nasabah, termasuk informasi transaksi, demografi, lokasi, dan bahkan perilaku penggunaan aplikasi. Banyak dari data ini sangat sensitif dan bersifat pribadi. Kebocoran atau penyalahgunaan data tersebut dapat menyebabkan kerugian finansial, pencurian identitas, dan hilangnya kepercayaan nasabah, serta pelanggaran regulasi yang berpotensi menimbulkan sanksi berat.
- Kepatuhan Regulasi: Perbankan di Indonesia tunduk pada berbagai regulasi perlindungan data, seperti Peraturan Otoritas Jasa Keuangan (POJK) terkait perlindungan konsumen dan Undang-Undang Perlindungan Data Pribadi (UU PDP). Kebijakan perlindungan data yang ketat memastikan bank mematuhi regulasi ini, menghindari denda dan sanksi hukum. BSI, sebagai institusi keuangan syariah, juga memiliki tanggung jawab tambahan untuk menjaga amanah data nasabah sesuai prinsip syariah.
- Strategi Keamanan Data: Implementasi AI harus disertai dengan strategi keamanan data berlapis, meliputi:

1. Enkripsi Data adalah Data nasabah harus dienkripsi baik saat transit maupun saat disimpan.
2. Anonimisasi/Pseudonimisasi adalah Jika memungkinkan, data yang digunakan untuk pelatihan model AI harus dianonimkan atau dipseudonimkan untuk mengurangi risiko identifikasi pribadi.
3. Kontrol Akses yang ketat adalah Hanya personel yang berwenang dan memiliki kebutuhan jelas yang boleh mengakses data nasabah.
4. Audit Keamanan Rutin adalah melakukan audit keamanan secara berkala untuk mengidentifikasi dan memperbaiki kerentanan dalam sistem penyimpanan dan pemrosesan data.

3.4 Kesesuaian Sistem dengan Prinsip Etika dan Transparansi

Implementasi AI dalam perbankan digital harus selaras dengan prinsip etika dan transparansi. Ini berarti bahwa keputusan yang diambil oleh sistem AI, terutama yang berdampak pada nasabah (misalnya, pemblokiran transaksi), harus dapat dijelaskan dan dipertanggungjawabkan. Kurangnya transparansi dalam algoritma dapat menimbulkan kekhawatiran tentang bias dan keadilan.

- a. Prinsip **Explainable AI** (XAI): Dalam konteks keuangan, di mana keputusan AI dapat memiliki dampak signifikan pada kehidupan finansial nasabah, prinsip *Explainable AI* (XAI) menjadi sangat penting. Bank perlu memahami "mengapa" AI membuat keputusan tertentu (misalnya, mengapa suatu transaksi ditandai sebagai fraud). Kemampuan untuk menjelaskan penalaran di balik keputusan AI ini sangat penting untuk:
 1. Kepercayaan Nasabah: Nasabah berhak tahu mengapa transaksi mereka diblokir atau mengapa akun mereka ditangguhkan. Penjelasan yang transparan membangun kepercayaan.
 2. Kepatuhan Regulasi: Beberapa regulasi, seperti GDPR di Eropa, mulai meminta penjelasan tentang keputusan otomatis yang berdampak pada individu.
 3. Debugging dan Peningkatan Model: Kemampuan untuk memahami bagaimana model AI bekerja juga membantu tim pengembang dalam mengidentifikasi kesalahan dan meningkatkan kinerja model.
- b. Transparansi Proses dan Kebijakan: Transparansi tidak hanya pada algoritma, tetapi juga pada proses di mana AI diimplementasikan dan kebijakan yang mengaturnya. Bank perlu secara jelas mengkomunikasikan kepada nasabah tentang penggunaan AI dalam deteksi fraud dan bagaimana hak-hak mereka dilindungi. Ini termasuk menyediakan saluran bagi nasabah untuk mengajukan banding atas keputusan otomatis yang mereka rasa tidak adil.
- c. Memastikan Keadilan dan Perlakuan Sama: Penggunaan AI yang tidak transparan dapat menimbulkan kekhawatiran tentang diskriminasi atau perlakuan tidak adil. Jika AI memblokir transaksi nasabah tanpa penjelasan yang masuk akal, hal itu dapat merusak reputasi bank. Prinsip etika menuntut bahwa sistem AI diperlakukan secara adil terhadap semua nasabah, tanpa memandang latar belakang sosial, ekonomi, atau demografi.

3.5 Pembahasan

Pembahasan ini mendalami temuan-temuan penelitian mengenai peran AI dalam memitigasi risiko transaksi mencurigakan pada layanan *mobile banking*, dengan penekanan pada studi kasus Bank Syariah Indonesia (BSI) cabang Aceh Timur. Analisis ini juga mencakup aspek governansi dan etika data yang krusial dalam implementasi teknologi AI.

3.5.1 Peningkatan Kecepatan dan Akurasi Deteksi sebagai Pilar Utama Efektivitas AI

Salah satu manfaat utama penerapan AI dalam deteksi fraud adalah kemampuannya meningkatkan kecepatan sekaligus akurasi identifikasi transaksi mencurigakan. AI mampu memproses *big data* secara real-time, menganalisis jutaan transaksi dalam hitungan milidetik, serta mengenali pola anomali yang kompleks dan dinamis. Hal ini menjadikan AI jauh lebih unggul dibandingkan metode manual maupun sistem berbasis aturan statis yang cenderung lambat dan mudah melewatkan indikasi penipuan. Dengan demikian, respons bank terhadap potensi fraud menjadi lebih cepat, risiko kerugian finansial berkurang, dan efektivitas pengendalian internal semakin optimal.



Gambar 2. Salah contoh notifikasi Fraud AI

Gambar 2 memperlihatkan pengalaman implementasi sistem deteksi fraud berbasis *Artificial Intelligence* (AI) di Bank Syariah Indonesia (BSI) cabang Aceh Timur. Penerapan teknologi ini menandai pergeseran paradigma dari pendekatan reaktif menuju proaktif dalam mengelola risiko keuangan. Pada sistem konvensional, aktivitas fraud umumnya baru terdeteksi setelah timbulnya kerugian nyata atau ketika nasabah melaporkan adanya aktivitas mencurigakan pada rekening mereka. Pola tersebut jelas tidak efisien karena kerugian sudah terjadi dan seringkali menimbulkan dampak reputasi bagi bank. Dengan adanya integrasi sistem AI, deteksi fraud dapat dilakukan secara real-time. Transaksi yang menunjukkan indikasi mencurigakan segera dikenali oleh sistem dan dapat diblokir seketika sebagaimana ditunjukkan pada Gambar 2. Hal ini memungkinkan bank untuk mencegah kerugian finansial sebelum benar-benar terjadi, sekaligus meningkatkan keamanan layanan perbankan digital. Keunggulan ini didorong oleh kemampuan algoritma *machine learning* yang bekerja dengan cara belajar dari data historis transaksi nasabah, lalu membangun model perilaku normal. Setiap penyimpangan (*outlier*) atau aktivitas yang tidak sesuai dengan pola tersebut secara otomatis ditandai sebagai indikasi potensi *fraud*. Selain aspek efektivitas, adopsi AI juga berdampak pada peningkatan akurasi deteksi. Sistem cerdas ini mampu menekan jumlah *false positives* (transaksi sah yang salah dikategorikan sebagai *fraud*). Pengurangan kesalahan deteksi semacam ini memberikan dua keuntungan strategis: pertama, mengurangi ketidaknyamanan nasabah yang sah sehingga kepercayaan terhadap layanan bank tetap terjaga; kedua, mengurangi beban kerja tim investigasi *fraud* yang sebelumnya harus menangani banyak kasus palsu. Dengan demikian, sumber daya manusia dapat difokuskan pada investigasi kasus *fraud* yang benar-benar nyata dan kritis (Awosika et al., 2024; Preciado Martínez et al., 2025; Miao, 2024)

3.5.2 Tata Kelola Teknologi yang Baik sebagai Fondasi Implementasi AI

Efektivitas implementasi AI tidak hanya bergantung pada kecanggihan algoritmanya, tetapi juga pada pondasi tata kelola teknologi yang baik (Good Technology Governance). Temuan ini menekankan bahwa tanpa kerangka kerja yang jelas untuk pengembangan, implementasi, dan pemeliharaan sistem AI, potensi AI dapat tidak dimanfaatkan secara optimal dan bahkan menimbulkan risiko baru. Regulasi dan pedoman dari otoritas keuangan global maupun nasional (misalnya, OJK di Indonesia) semakin menegaskan pentingnya tata kelola AI yang komprehensif di sektor keuangan (Bank for International Settlements., 2021).

BSI cabang Aceh Timur adanya kebijakan internal yang mengatur siklus hidup AI, mulai dari proses pengumpulan data, pelatihan model, validasi, hingga *deployment* dan pemantauan berkelanjutan. Governansi yang kuat mencakup penetapan peran dan tanggung jawab yang jelas bagi tim pengembangan, operasional, dan kepatuhan. Ini juga melibatkan pengelolaan risiko terkait AI, seperti risiko model (ketidakakuratan prediksi), risiko operasional (gangguan sistem), dan risiko keamanan siber (ancaman terhadap integritas data dan algoritma). Sebuah studi oleh (Accenture., 2023) menyoroti bahwa perusahaan yang berhasil mengintegrasikan AI memiliki kerangka tata kelola yang matang, memastikan bahwa inovasi teknologi sejalan dengan tujuan strategis dan kepatuhan regulasi. Berikut tabel cara modul penipuan dan tindakan aman untuk nasabah

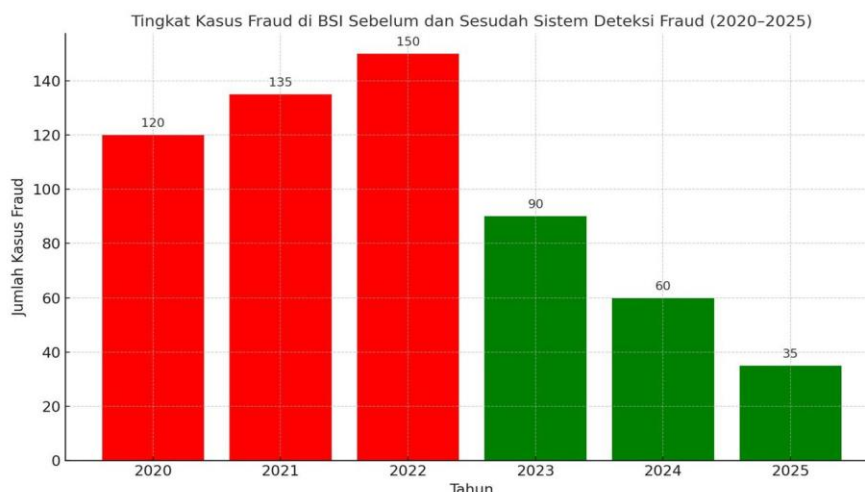
Tabel 1. Cara Modul Penipuan Dan Tindakan Aman Untuk Nasabah

Modus Penipuan	Ciri-ciri	Tindakan Aman
Smishing/SMS phishing	Urgensi, link atau kode, nomor aneh	Jangan klik, hapus pesan, hubungi bank langsung (bsigroup.com, bsi.bund.de) atau call 14040
Phishing via email/whatsapp	Alamat email tak resmi, tata bahasa asal-asalan	Cek header & URL, verifikasi via saluran resmi
BEC / CEO fraud	Instruksi transfer mendesak dari rekan/atasan	Konfirmasi langsung via telepon, jangan balas otomatis

Tabel 1 menjelaskan berbagai modus penipuan digital yang kerap menargetkan nasabah perbankan beserta ciri-ciri dan langkah aman yang perlu dilakukan. Smishing atau SMS phishing biasanya ditandai dengan adanya pesan berisi urgensi tertentu, tautan atau kode, serta dikirim dari nomor tidak dikenal. Dalam kasus ini, nasabah disarankan untuk tidak mengklik tautan, segera menghapus pesan, dan menghubungi bank melalui kanal resmi seperti situs *bsigroup.com* atau layanan 14040. Selanjutnya, phishing melalui email atau WhatsApp umumnya memiliki alamat pengirim yang tidak resmi serta tata bahasa yang asal-asalan. Untuk mencegah kerugian, nasabah perlu memeriksa *header* dan URL email, serta melakukan verifikasi melalui saluran resmi bank. Adapun Business Email Compromise (BEC) atau CEO fraud biasanya berbentuk instruksi transfer mendesak yang seolah datang dari rekan kerja atau atasan. Dalam kondisi seperti ini, tindakan aman adalah dengan melakukan konfirmasi langsung melalui telepon dan tidak merespons instruksi secara otomatis.

3.5.3 Kebijakan Perlindungan Data yang Ketat: Imperatif dalam Era AI

Keberhasilan sistem deteksi fraud berbasis AI sangat terkait erat dengan kebijakan perlindungan data yang ketat. AI membutuhkan akses ke volume besar data nasabah yang sensitif untuk melatih modelnya. Oleh karena itu, perlindungan data pribadi nasabah dari penyalahgunaan, kebocoran, atau akses tidak sah adalah mutlak. Ini bukan hanya masalah kepatuhan regulasi (misalnya, UU Perlindungan Data Pribadi di Indonesia) tetapi juga fondasi kepercayaan nasabah (Ikhsan et al, 2025; Wang et al, 2024).



Gambar 3. Tingkat Kasus Fraud BSI dari tahun 2020-2025

Gambar 3 Penerapan sistem deteksi fraud berbasis kecerdasan buatan (AI) di Bank Syariah Indonesia (BSI) memberikan dampak signifikan terhadap penurunan jumlah kasus fraud. Sebelum implementasi AI, jumlah kasus fraud di BSI cabang Aceh Timur mengalami peningkatan tajam, yakni mencapai 150 kasus pada tahun 2022. Namun, setelah penerapan sistem deteksi fraud berbasis AI, jumlah kasus tersebut menurun secara signifikan menjadi hanya 35 kasus pada pertengahan tahun 2025. Hal ini dapat dilihat secara lebih jelas pada Gambar 3, di mana warna oranye merepresentasikan kondisi sebelum penerapan AI, sedangkan warna hijau menggambarkan kondisi setelah penerapan AI. Penurunan ini menunjukkan bahwa pemanfaatan AI mampu meningkatkan efektivitas pengawasan serta memperkuat keamanan sistem perbankan syariah. Namun demikian, efektivitas teknologi tersebut hanya dapat terjaga apabila didukung oleh praktik keamanan siber yang kuat. Di antaranya adalah penerapan enkripsi data end-to-end, penggunaan teknik anonimisasi atau pseudonimisasi data, serta penerapan kontrol akses berbasis peran yang ketat.

Pentingnya keamanan siber ini tidak hanya berkaitan dengan kepatuhan terhadap regulasi, tetapi juga menyangkut keberlanjutan kepercayaan nasabah. Pelanggaran data dapat menimbulkan kerugian finansial yang signifikan, sanksi regulasi, serta kerusakan reputasi institusi yang sulit diperbaiki. Penelitian terbaru menegaskan bahwa perlindungan data harus ditempatkan sebagai prioritas utama dalam setiap desain sistem berbasis AI, khususnya di sektor perbankan yang sangat diatur secara ketat (Alhassan & Asante, 2022; Bag et al., 2023; Hossain et al., 2024).

3.5.4 Kesesuaian Sistem dengan Prinsip Etika dan Transparansi

Implementasi AI dalam perbankan digital harus selaras dengan prinsip etika dan transparansi. Keputusan yang diambil oleh sistem AI, terutama yang berdampak langsung pada nasabah (misalnya, pemblokiran transaksi atau penolakan layanan), harus dapat dijelaskan dan dipertanggungjawabkan (OECD, 2023). Kurangnya transparansi dalam algoritma dapat menimbulkan kekhawatiran tentang bias, keadilan, dan bahkan diskriminasi.

Dalam konteks BSI sebagai bank syariah, prinsip etika memiliki bobot tambahan. Transparansi dalam operasional adalah fundamental. Nasabah harus memiliki pemahaman dasar tentang bagaimana AI digunakan untuk melindungi mereka dan bagaimana keputusan diambil. Konsep *Explainable AI* (XAI) menjadi sangat relevan di sini. Bank harus berinvestasi dalam teknologi dan proses yang memungkinkan penjelasan mengapa suatu transaksi ditandai sebagai mencurigakan (Darpa, 2020). Ini tidak hanya membangun kepercayaan nasabah tetapi juga membantu bank dalam mengidentifikasi dan memperbaiki potensi kesalahan atau bias dalam model AI.

3.5.5 Akuntabilitas Algoritma dan Pencegahan Bias

Terakhir, keberhasilan mitigasi risiko juga ditentukan oleh kemampuan lembaga keuangan dalam menjaga akuntabilitas algoritma dan memastikan tidak adanya bias dalam pengambilan keputusan otomatis. Algoritma AI, jika tidak dirancang dan dilatih dengan hati-hati, dapat mewarisi atau bahkan memperkuat bias yang ada dalam data pelatihan historis, yang berpotensi menyebabkan diskriminasi atau keputusan yang tidak adil terhadap kelompok nasabah tertentu (Smith & Lee, 2023).

BSI cabang Aceh Timur, seperti lembaga keuangan lainnya, harus proaktif dalam mengidentifikasi dan memitigasi bias algoritmik. Ini bisa berarti melakukan audit bias secara rutin, menggunakan dataset pelatihan yang representatif dan seimbang, serta menerapkan teknik *fairness-aware AI* dalam pengembangan model. Adanya bias dapat merusak reputasi bank, memicu keluhan nasabah, dan bahkan tuntutan hukum. Oleh karena itu, *human-in-the-loop* (pengawasan manusia) tetap menjadi elemen krusial, memastikan bahwa keputusan otomatis yang kritis selalu dapat ditinjau dan divalidasi oleh pakar manusia, terutama ketika melibatkan konsekuensi signifikan bagi nasabah. Akuntabilitas ini juga mencakup mekanisme umpan balik dan penyelesaian sengketa bagi nasabah yang merasa dirugikan oleh keputusan otomatis.

Hasil studi kasus di BSI cabang Aceh Timur menunjukkan bahwa implementasi sistem deteksi fraud berbasis AI memberikan dampak transformatif bagi efektivitas mitigasi risiko transaksi mencurigakan. AI terbukti meningkatkan kecepatan dan akurasi deteksi dengan kemampuan menganalisis big data secara real-time, mengidentifikasi pola anomali kompleks, serta mengurangi false positives yang sebelumnya membebani tim fraud. Selain itu, penerapan AI tidak hanya meningkatkan efisiensi operasional, tetapi juga memungkinkan pergeseran paradigma dari strategi reaktif menjadi proaktif dalam pencegahan fraud. Kontribusi unik penelitian ini terletak pada pembuktian empiris di konteks perbankan syariah Indonesia, khususnya di BSI, di mana prinsip tata kelola, etika, dan perlindungan data memiliki bobot tambahan yang mendukung kepercayaan publik.

Penelitian ini menegaskan bahwa efektivitas AI tidak semata-mata ditentukan oleh kecanggihan algoritma, melainkan juga oleh tata kelola teknologi yang kuat, kebijakan perlindungan data yang ketat, serta penerapan prinsip etika dan transparansi. Studi ini menyoroti bagaimana BSI berhasil menurunkan kasus fraud secara signifikan setelah penerapan AI pada tahun 2023, dengan integrasi strategi keamanan berlapis, komitmen terhadap Explainable AI, serta pengawasan manusia (*human-in-the-loop*) untuk menjaga akuntabilitas dan mencegah bias algoritmik. Dengan demikian, penelitian ini memberi kontribusi ilmiah dan praktis. Secara akademik memperkuat diskursus global mengenai peran AI dalam sistem keuangan, dan secara praktis memberikan model implementasi yang dapat direplikasi oleh lembaga keuangan lain di Indonesia, khususnya bank syariah, dalam membangun sistem deteksi fraud yang efektif, etis, dan berkelanjutan.

4. KESIMPULAN

Penelitian ini secara komprehensif mengkaji peran transformatif kecerdasan buatan (AI) dalam mitigasi risiko transaksi mencurigakan, khususnya pada layanan *mobile banking* di sektor perbankan digital. Dengan menggunakan pendekatan kualitatif, studi kasus di Bank Syariah Indonesia (BSI) cabang Aceh Timur, kami menemukan bahwa AI secara fundamental meningkatkan kecepatan dan akurasi deteksi *fraud* secara *real-time*, jauh melampaui kemampuan metode manual atau berbasis aturan konvensional. Kemampuan AI untuk menganalisis volume data transaksi yang masif dan mengidentifikasi pola anomali yang kompleks dan dinamis memungkinkan bank untuk merespons ancaman penipuan dengan lebih cepat dan efektif, sehingga meminimalkan potensi kerugian finansial. Namun keberhasilan implementasi AI ini tidaklah berdiri sendiri. Temuan kunci penelitian ini menegaskan bahwa efektivitas AI sangat bergantung pada adanya tata kelola teknologi yang baik, yang mencakup kerangka kerja yang jelas untuk pengembangan, implementasi, dan pemeliharaan sistem AI. Selain itu, kebijakan perlindungan data yang ketat adalah imperatif mutlak, mengingat AI mengandalkan akses terhadap data nasabah dalam jumlah besar; tanpa perlindungan yang memadai, risiko kebocoran dan penyalahgunaan data akan meningkat. Lebih lanjut, studi ini menyoroti pentingnya kesesuaian sistem dengan prinsip etika dan transparansi, memastikan bahwa keputusan otomatis AI dapat dijelaskan dan dipertanggungjawabkan, serta akuntabilitas algoritma dan pencegahan bias untuk menghindari diskriminasi atau perlakuan tidak adil terhadap nasabah. Secara keseluruhan, penelitian ini menyimpulkan bahwa AI merupakan aset yang tak ternilai dalam memperkuat keamanan siber perbankan digital. Namun, potensi penuhnya hanya dapat direalisasikan melalui sinergi yang kuat antara inovasi teknologi dan prinsip governansi yang kokoh. Implementasi AI harus diiringi dengan kebijakan internal yang kuat terkait audit algoritma, perlindungan data nasabah yang komprehensif, dan pelatihan etika digital bagi seluruh pemangku kepentingan. Dengan demikian, industri perbankan dapat menciptakan ekosistem keuangan digital yang tidak hanya aman dan efisien, tetapi juga terpercaya dan berkeadilan bagi semua. Penelitian ini memiliki beberapa keterbatasan yang Pertama, fokus studi hanya pada satu lokasi, yaitu BSI cabang Aceh Timur, sehingga hasilnya belum dapat digeneralisasikan untuk seluruh sektor perbankan di Indonesia. Kedua, penelitian ini menggunakan pendekatan kualitatif sehingga tidak mengukur secara kuantitatif efektivitas sistem AI terhadap penurunan kasus fraud. Oleh karena itu, penelitian selanjutnya disarankan untuk menggunakan metode kuantitatif dengan cakupan bank yang lebih luas.

REFERENCES

- Accenture. (2025). *Reinventing risk management*. Accenture Research Report. Diakses dari Accenture website.
- Alhassan, I., & Asante, J. (2022). Artificial intelligence applications in financial services: Opportunities, risks, and regulatory implications. *Journal of Banking Regulation*, 23(4), 345–361. <https://doi.org/10.1057/s41261-021-00178-1>
- Awosika, T., Shukla, R. M., & Pranggono, B. (2024). Transparency and Privacy: The Role of Explainable AI and Federated Learning in Financial Fraud Detection. *IEEE Access*, 12, 64551–64560. <https://doi.org/10.1109/access.2024.3394528>
- Bag, S., Pretorius, J. H. C., Gupta, S., & Dwivedi, Y. K. (2023). Role of artificial intelligence in fraud detection in banking sector: A systematic literature review and research agenda. *Technological Forecasting and Social Change*, 188, 122262. <https://doi.org/10.1016/j.techfore.2022.122262>
- Bas, B.M, Rhamadhan. R. F, Anggraeni. R.N, I P, E,Darmawan, & P. A, Djuri. (2025). Artificial Intelligence and Financial Regulation in Indonesia's Islamic Banking. *Paradoks: Jurnal Ilmu Ekonomi*, 8(3), 1174–1187. <https://doi.org/10.57178/paradoks.v8i3.1519>
- Bank for International Settlements. (2021). The use of supervisory and regulatory technology by authorities and regulated institutions: In *Market developments and financial stability implications*. (Vol. 7, p. 2987632). Retrieved from https://www.bis.org/publ/fsb_reports.htm
- Baqir, N. Al, & Sulhani, S. (2023). Corporate Governance, Effectiveness of Internal Audit Function and Fraud in Islamic Banking

- in Indonesia. *Asia Pacific Fraud Journal*, 8(1), 77. <https://doi.org/10.21532/apfjournal.v8i1.272>
- Braun, V., & Clarke, V. (2019). Reflecting on reflexive thematic analysis. *Qualitative Research in Sport, Exercise and Health*, 11(4), 589–597. <https://doi.org/10.1080/2159676X.2019.1628806>
- Darpa. (2020). *Explainable Artificial Intelligence (XAI)*. Defense Advanced Research Projects Agency. (2022), 11948.
- Denzin, N. K., & Lincoln, Y. S. (2018). *The SAGE handbook of qualitative research (5th ed.)*. SAGE Publications.
- Hossain, M. S., Rahman, M. M., & Islam, M. R. (2024). Cybersecurity and data privacy challenges in the financial industry under AI adoption. *Computers & Security*, 147, 104051. <https://doi.org/10.1016/j.cose.2024.104051>
- Ikhsan, R. B., Fernando, Y., Prabowo, H., Yuniarty, Gui, A., & Kuncoro, E. A. (2025). An empirical study on the use of artificial intelligence in the banking sector of Indonesia by extending the TAM model and the moderating effect of perceived trust. *Digital Business*, 5(1), 100103. <https://doi.org/10.1016/j.digbus.2024.100103>
- Iqbal, M. S., Sukanto, F. A. M. S. B., Norizan, S. N. B., Mahmood, S., Fatima, A., & Hashmi, F. (2025). AI in Islamic finance: Global trends, ethical implications, and bibliometric insights. *Review of Islamic Social Finance and Entrepreneurship*, 4(1), 70–85. <https://doi.org/10.20885/risfe.vol4.iss1.art6>
- Johora, F. T., Mahmud, M. A. Al. (2024). AI-Powered Fraud Detection in Banking: Safeguarding Financial Transactions. *The American Journal of Management and Economics Innovations*, 6(6), 8–22. <https://doi.org/10.37547/tajmei/volume06issue06-02>
- Miao, Z. (2024). Financial Fraud Detection and Prevention. *Journal of Organizational and End User Computing*, 36(1), 1–27. <https://doi.org/10.4018/joeuc.354411>
- Nowell, L. S., & Albrecht, L. (2019). A critical review of qualitative case study research in education. *Journal of Curriculum Studies*, 51(6), 873–890. <https://doi.org/10.1080/00220272.2019.1572742>
- OECD. (2023). *OECD recommendation on artificial intelligence: Towards responsible AI innovation*. Organisation for Economic Co-operation and Development. <https://doi.org/10.1787/5e5f42d5-en>
- Preciado Martínez, P. M., Reier Forradellas, R. F., Garay Gallastegui, L. M., & Nández Alonso, S. L. (2025). Comparative analysis of machine learning models for the detection of fraudulent banking transactions. *Cogent Business & Management*, 12(1). <https://doi.org/10.1080/23311975.2025.2474209>
- Rahi, S. (2020). Research design and methods: A systematic review of research paradigms, sampling issues and instruments development. *International Journal of Economics & Management Sciences*, 9(2), 1–11. <https://doi.org/10.35248/2162-6359.20.9.578>
- Ridzuan, N. N., Masri, M., Anshari, M., Fitriyani, N. L., & Syafrudin, M. (2024). AI in the Financial Sector: The Line between Innovation, Regulation and Ethical Responsibility. *Information (Switzerland)*, 15(8), 1–30. <https://doi.org/10.3390/info15080432>
- Sain, Z., & Adinugraha, H. H. (2025). Artificial Intelligence and Islamic Finance: Enhancing Sharia Compliance and Social Impact in Banking 4.0. *Journal of Business Management and Islamic Banking*, 4(1), 025–046. <https://doi.org/10.14421/jbmib.2025.0401-03>
- Schoonenboom, J. (2021). The use of theory in qualitative case study research and how this differs from quantitative case study research. *International Journal of Qualitative Methods*, 20, 1–13. <https://doi.org/10.1177/1609406921995306>
- Smith, J., & Lee, R. (2023). AI bias: Exploring discriminatory algorithmic decision-making models and the application of possible machine-centric solutions adapted from the pharmaceutical industry. MIT. *MIT Technology Review*. PubMed Central.
- Wang, S., Asif, M., Shahzad, M. F., & Ashfaq, M. (2024). Data privacy and cybersecurity challenges in the digital transformation of the banking sector. *Computers & Security*, 147, 104051. <https://doi.org/10.1016/j.cose.2024.104051>