Resiliensi
Jurnal Ekonomi dan Keuangan Syariah
Yayasan Paramarta Akademika Indonesia

Analisis Kesiapan Perbankan Syariah Menghadapi Risiko Deepfake dan Penipuan Digital pada Era Artificial Intelligence

ABSTRACT *- The development of artificial intelligence (AI) has accelerated the digital transformation of Islamic banking while increasing the risks of deepfakes and digital fraud, which can result in identity theft, account hacking, and loss of public trust. The objective of this research is to assess the readiness of Islamic banking in facing these threats by using a literature review and descriptive qualitative analysis of various scientific journals, books, articles, and government reports. The findings of this study indicate that security technology impacts the readiness of Islamic banking, as well as regulatory support, risk management, the quality of human resources, and digital literacy. AI-based security systems, layered biometric authentication, deepfake detection technology, real-time transaction monitoring, and customer education are key strategies to reduce the risk of digital fraud while adhering to Sharia principles such as trust, justice, and transparency. As a result, combining technological innovation, cybersecurity governance, and human resource capacity development is crucial for the resilience, sustainability, and competitiveness of Islamic banking in the era of artificial intelligence.*

ABSTRAK -. Perkembangan kecerdasan buatan Artificial intelligence (AI) telah mempercepat transformasi digital perbankan syariah sambil meningkatkan risiko deepfake dan penipuan digital, yang dapat mengakibatkan pencurian identitas, peretasan akun, dan hilangnya kepercayaan publik. Tujuan dari penelitian ini adalah untuk menilai kesiapan perbankan syariah dalam menghadapi ancaman-ancaman ini dengan menggunakan tinjauan pustaka dan analisis kualitatif deskriptif dari berbagai jurnal ilmiah, buku, artikel, dan laporan pemerintah. Temuan studi ini menunjukkan bahwa teknologi keamanan berdampak pada kesiapan perbankan syariah, begitu juga dengan dukungan regulasi, manajemen risiko, kualitas sumber daya manusia, dan literasi digital Sistem keamanan berbasis Artificial intelligence (AI), otentikasi biometrik berlapis, teknologi deteksi deepfake, pemantauan transaksi waktu nyata, dan edukasi pelanggan adalah strategi utama untuk mengurangi risiko penipuan digital sambil mematuhi prinsip-prinsip Syariah seperti kepercayaan, keadilan, dan transparansi. Akibatnya, menggabungkan inovasi teknologi, tata kelola keamanan siber, dan pengembangan kapasitas sumber daya manusia sangat penting untuk ketahanan, keberlanjutan, dan daya saing perbankan syariah di era kecerdasan buatan.

Author
[1] **Mawarni Gultom**
[2] **Nazwa Zahra**,
[3] **Yunanda Eka Putra**,
[1,2,3] Program Studi Manajemen, Fakultas Ekonomi, Universitas Al-Azhar Medan, Indonesia

*[1]***Corresponding email:**
mawarnigultom515@gmail.com

Article History
Submitted: 13 Juli 2026
Revised: 14 Juli 2026
Accepted: 23 Juli 2026
Published: 23 Juli 2026

Keywords
Perbankan Syariah, Kecerdasan Buatan, Deepfake, Keamanan Siber.

PENDAHULUAN

Perkembangan kecerdasan buatan Artificial intelligence (AI) telah menghasilkan perubahan signifikan di sektor layanan keuangan, termasuk perbankan syariah. Artificial intelligence (AI) dapat meningkatkan efisiensi operasional, mempercepat layanan digital, dan meningkatkan analisis data serta manajemen risiko. Namun, seiring kemajuan teknologi, ancaman baru muncul, seperti deepfake dan bentuk penipuan digital lainnya

yang semakin sulit diidentifikasi. Teknologi deepfake memungkinkan penjahat untuk membuat wajah, suara, atau video yang sangat mirip dengan identitas asli seseorang, yang berpotensi mengarah pada peretasan akun, pencurian identitas, dan penipuan transaksi keuangan (Anugrah et al., 2026).

Transformasi digital yang sedang berlangsung di sektor perbankan Indonesia telah menyebabkan peningkatan penggunaan layanan perbankan seluler, perbankan internet, dan proses verifikasi identitas elektronik. Situasi ini menempatkan perbankan, termasuk perbankan syariah, di antara industri yang paling rentan terhadap serangan siber yang didukung Artificial intelligence (AI). Otoritas Jasa Keuangan (OJK) telah memperingatkan bahwa penipuan berbasis deepfake merupakan ancaman serius bagi industri keuangan, yang memerlukan sistem verifikasi identitas yang lebih kuat, teknologi deteksi kehadiran, dan pemantauan transaksi secara real-time.

Deepfake dan penipuan digital mengancam perbankan syariah, yang mengakibatkan kerugian finansial dan hilangnya kepercayaan publik terhadap sistem tersebut. Kepercayaan adalah pilar fundamental perbankan Islam, yang didasarkan pada prinsip kepercayaan, keadilan, dan transparansi. Akibatnya, kemampuan perbankan Islam untuk mengelola risiko digital sangat penting bagi stabilitas industri dan keberlanjutan jangka panjang di era kecerdasan buatan (Gunawan & Janisriwati, 2023).

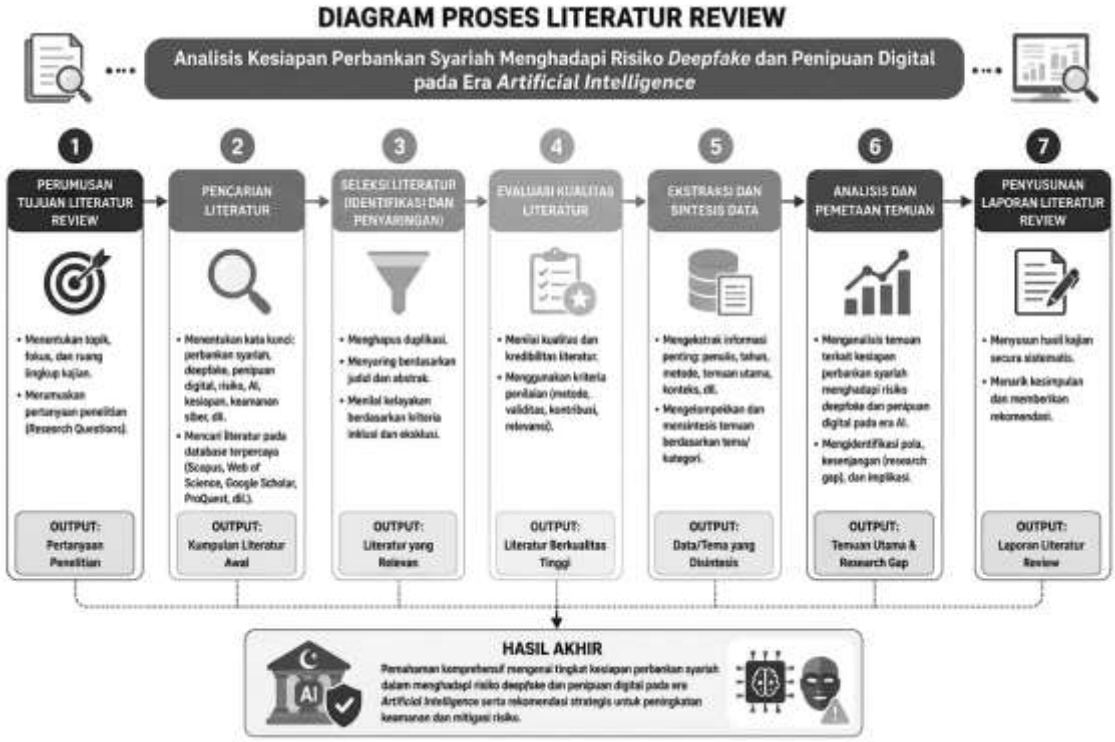
Selain teknologi yang lebih baik, kesiapan ini memerlukan dukungan regulasi, manajemen risiko, peningkatan literasi digital, dan pengembangan sumber daya manusia yang mampu mengantisipasi evolusi teknik kejahatan siber. Perbankan Islam harus mengambil langkah-langkah strategis seperti menerapkan sistem keamanan berbasis Artificial intelligence (AI), autentikasi biometrik canggih, dan mendidik pelanggan tentang bahaya penipuan digital. Menurut penelitian, kecerdasan buatan dapat mendeteksi serangan deepfake dan penipuan identitas digital, meningkatkan efektivitas sistem keamanan perbankan (Fraud, 2026).

METODOLOGI

Penelitian Penelitian ini menggunakan metode tinjauan pustaka dan pendekatan kualitatif deskriptif. Data sekunder dikumpulkan dari jurnal ilmiah, buku, artikel, dan laporan pemerintah tentang perbankan syariah, deepfake, penipuan digital, dan Kecerdasan Artificial intelligence (AI). Analisis data dilakukan melalui tahap pengumpulan, pemilihan, dan tinjauan literatur yang relevan, dan kemudian disusun untuk memberikan gambaran tentang kesiapan perbankan syariah dalam menghadapi risiko deepfake dan penipuan digital di era Artificial intelligence (AI).

Studi ini menggunakan metode tinjauan pustaka dengan pendekatan kualitatif deskriptif-analitis untuk menilai risiko deepfake dan penipuan digital di era kecerdasan buatan. Data sekunder berasal dari makalah ilmiah, jurnal, dan laporan penelitian dari OJK, Bank Indonesia, dan FSB. Laporan-laporan ini dipilih berdasarkan relevansi, kredibilitas (terindeks/peer-reviewed), dan evaluasi data non-ilmiah. Proses pengumpulan, pemilihan, kategorisasi tema, sintesis, dan interpretasi naratif-deskriptif diikuti oleh analisis konten dan analisis tematik dari materi yang dikumpulkan melalui dokumentasi dan pencarian kata kunci di basis data akademik. Meskipun hasil penelitian bersifat konseptual karena hanya menggunakan literatur yang dipublikasikan tanpa data

primer, validitas kesimpulan tetap terjaga melalui triangulasi sumber dan verifikasi keakuratan data.



Gambar 1: Diagram alur

HASIL DAN PEMBAHASAN

Menurut temuan tinjauan pustaka, perbankan Islam telah beralih ke digital, dengan diperkenalkannya layanan perbankan seluler, perbankan internet, dan sistem verifikasi elektronik untuk meningkatkan kualitas layanan (Nazim Ali & Hakim Jumat, 2024). Namun, seiring dengan kemajuan teknologi Kecerdasan Buatan/Artificial intelligence (AI), ancaman baru telah muncul, termasuk deepfake dan berbagai jenis penipuan digital, yang berpotensi menyebabkan pencurian identitas, peretasan akun, manipulasi data pelanggan, dan penyalahgunaan autentikasi biometric (Irsyad, 2025). Temuan menunjukkan bahwa kesiapan perbankan syariah untuk menghadapi risiko ini dipengaruhi tidak hanya oleh kecanggihan teknologi keamanan, tetapi juga oleh kesiapan regulasi, manajemen risiko, kualitas sumber daya manusia, dan literasi digital masyarakat (Wahab & Ihsan, 2025).

Menurut literatur, penerapan sistem keamanan berbasis Artificial intelligence (AI), teknologi deteksi keaktifan, otentikasi biometrik berlapis, pemantauan transaksi waktu nyata, dan edukasi pelanggan adalah semua langkah strategis untuk mengurangi dampak penipuan digital (Ke et al., 2025). Selain itu, penerapan prinsip-prinsip tata kelola risiko yang sesuai dengan syariah seperti kepercayaan, keadilan, dan transparansi sangat penting untuk menjaga kepercayaan publik terhadap industri perbankan syariah (Arifin et al., 2025). Dengan demikian, temuan studi ini menunjukkan bahwa perbankan Islam harus meningkatkan integrasi teknologi, kebijakan keamanan siber, dan kapasitas sumber

daya manusia untuk secara efektif menangani ancaman deepfake dan penipuan digital sambil juga memastikan keberlanjutan jangka panjang layanan keuangan di era Artificial intelligence (AI) (Popa et al., 2025).

Tabel 1.

Matriks penilaian Risiko Deepfake dan Penipuan Digital di Perbankan Syariah Tahun 2025

No.	Jenis Resiko	Proporsi (%)	Likelihood (1-5)	Impact (1-5)	Skor Risiko (L x I)	Kategori Risiko	Prioritas Mitigasi
1	Pencurian Identitas	32,0	5	5	25	Sangat Tinggi	I
2	Peretas Akun	25,0	4	5	20	Tinggi	II
3	Manipulasi Data Nasabah	20,0	4	4	16	Tinggi	III
4	Penyalahgunaan Autentikasi Biometrik	12,5	3	4	12	Sedang	IV
5	Penipuan Transaksi Digital	10,5	2	4	8	Rendah	V

Matriks penilaian Risiko Deepfake dan Penipuan Digital di Perbankan Syariah Tahun 2025

Keterangan:

Kemungkinan (L): 1 sangat rendah, 2 rendah, 3 sedang, 4 tinggi, dan 5 sangat tinggi.

Dampak (I): Skor 1 menunjukkan dampak yang sangat rendah, sementara skor 5 menunjukkan dampak yang sangat signifikan.

Skor Risiko = Dampak x Kemungkinan. Sangat Tinggi (20–25), Tinggi (15–19), Sedang (10–14), dan Rendah (1–9) adalah kategori risiko.



Gambar 2. Proporsi Potensi Risiko Deepfake dan Penipuan Digital di Perbankan Syariah (2025)

Grafik tersebut menunjukkan bahwa pencurian identitas dan peretasan akun adalah ancaman yang paling umum, diikuti oleh manipulasi data pelanggan, penyalahgunaan autentikasi biometrik, dan penipuan transaksi digital. Visualisasi ini didasarkan pada sintesis literatur untuk mendukung temuan penelitian.

Ketika diperiksa lebih dekat, terdapat disparitas antara tingkat inovasi teknologi Artificial intelligence (AI) yang digunakan oleh penjahat digital dan tingkat adopsi regulasi serta infrastruktur keamanan perbankan syariah. Teknologi deepfake, misalnya, berkembang dengan tingkat realisme yang sulit dideteksi oleh sistem verifikasi tradisional, sementara pembaruan standar regulasi dan keamanan biasanya bersifat reaktif, dikembangkan hanya setelah insiden terjadi. Kondisi ini menunjukkan bahwa kesiapan perbankan Islam ditentukan tidak hanya oleh ketersediaan teknologi keamanan, tetapi juga oleh kemampuan institusi untuk menciptakan sistem yang dapat mengantisipasi dan beradaptasi dengan pola ancaman yang berubah (Teknologi & Dahlan, 2025). Selain itu, literasi digital di masyarakat sering diabaikan demi investasi teknologi, meskipun fakta bahwa celah keamanan sering dieksploitasi melalui rekayasa sosial, yang menargetkan kerentanan pengguna daripada kerentanan sistem. Akibatnya, strategi keamanan yang efektif harus bersifat multifaset, menggabungkan penguatan teknis, peningkatan tata kelola berbasis Syariah, dan perbaikan kapasitas literasi digital secara bersamaan, sehingga perbankan Islam tidak hanya mampu menghadapi ancaman saat ini seperti deepfake dan penipuan digital, tetapi juga memiliki fondasi institusional yang kuat untuk mengantisipasi bentuk ancaman baru yang mungkin muncul seiring perkembangan Artificial intelligence (AI) di masa depan. Dari sudut pandang regulasi, kerangka hukum Otoritas Jasa Keuangan meningkatkan kemampuan perbankan syariah untuk memerangi deepfake dan penipuan digital. POJK Nomor 11/POJK.03/2022 mengatur penggunaan teknologi informasi oleh bank komersial, yang mencakup tata kelola TI, manajemen risiko, ketahanan siber, dan keamanan (Umum, 2014).

Selain itu, ketika dilihat melalui lensa manajemen risiko, kesiapan perbankan Syariah dapat dibagi menjadi tiga lapisan yang saling terkait: teknologi, tata kelola, dan sumber daya manusia, dengan kekurangan pada satu lapisan mengurangi efektivitas lapisan lainnya, meskipun lapisan-lapisan tersebut telah sepenuhnya diinvestasikan. Misalnya, bahkan sistem deteksi kehadiran yang paling canggih sekalipun akan menjadi tidak efektif jika tidak didukung oleh kebijakan tata kelola yang mengatur protokol eskalasi ketika anomali terdeteksi, serta personel layanan yang dapat mengenali pola rekayasa sosial yang terkait dengan upaya penipuan berbasis deepfake. Ini menunjukkan bahwa mengambil pendekatan parsial, seperti hanya fokus pada pembaruan teknologi tanpa juga memperkuat regulasi internal dan melatih sumber daya manusia, dapat menghasilkan rasa siap yang palsu, dengan organisasi tampak siap secara teknis tetapi masih rentan pada titik interaksi antara lapisan yang belum sepenuhnya terintegrasi. POJK Nomor 22 Tahun 2023, yang berkaitan dengan Perlindungan Konsumen dan Masyarakat di Sektor Jasa Keuangan, memperkuat aspek perlindungan konsumen dengan menekankan kewajiban penyedia jasa keuangan, termasuk bank syariah, untuk memastikan keamanan sistem informasi dan privasi data konsumen(POJK no 22 tahun 2023, 2023).

Akibatnya, perbankan syariah tidak hanya harus meningkatkan jumlah instrumen keamanan, tetapi juga membangun integrasi jangka panjang antara lapisan-lapisan ini, sehingga respons terhadap ancaman deepfake dan penipuan digital tercermin dalam kebijakan tata kelola adaptif dan kapasitas manusia yang merespons dinamika ancaman berbasis Artificial intelligence (AI) yang terus berubah (Fadhil et al., 2025).

Perkembangan teknologi Artificial Intelligence (AI) telah membawa perubahan signifikan dalam industri jasa keuangan, termasuk perbankan syariah. Selain menghadirkan berbagai peluang untuk meningkatkan efisiensi operasional, AI juga memunculkan risiko baru berupa penyalahgunaan teknologi, salah satunya adalah deepfake. Deepfake merupakan teknologi berbasis kecerdasan buatan yang mampu menghasilkan manipulasi wajah, suara, maupun video sehingga tampak sangat menyerupai individu asli. Dalam sektor perbankan, teknologi ini berpotensi dimanfaatkan untuk melakukan pencurian identitas, penipuan transaksi, pembobolan rekening, manipulasi proses verifikasi nasabah (electronic Know Your Customer/e-KYC), hingga penyebaran informasi palsu yang dapat merusak reputasi lembaga keuangan.

Bagi perbankan syariah, ancaman tersebut tidak hanya berkaitan dengan aspek keamanan informasi, tetapi juga menyangkut prinsip amanah (trustworthiness), keadilan ('adl), transparansi (shiddiq), dan perlindungan terhadap harta (hifz al-mal) sebagai bagian dari maqashid syariah. Oleh karena itu, kesiapan perbankan syariah dalam menghadapi risiko deepfake harus dipandang sebagai bagian dari implementasi tata kelola risiko yang sesuai dengan prinsip syariah dan good corporate governance.

Kesiapan tersebut dapat dianalisis melalui beberapa dimensi. Pertama, kesiapan teknologi, yaitu kemampuan bank dalam mengadopsi sistem keamanan berbasis AI yang mampu mendeteksi manipulasi gambar, suara, maupun dokumen digital. Penggunaan teknologi biometrik multimodal, liveness detection, behavioral analytics, serta AI-based fraud detection menjadi komponen penting untuk mengurangi risiko penyalahgunaan identitas digital.

Kedua, kesiapan tata kelola risiko (risk governance). Perbankan syariah perlu memperkuat kerangka Enterprise Risk Management (ERM) dengan memasukkan risiko deepfake sebagai bagian dari risiko operasional dan risiko siber. Pengelolaan risiko tidak hanya dilakukan melalui penguatan infrastruktur teknologi, tetapi juga melalui penyusunan Standard Operating Procedure (SOP), audit keamanan informasi secara berkala, serta pembentukan tim respons insiden siber yang mampu melakukan mitigasi secara cepat ketika terjadi serangan digital.

Ketiga, kesiapan sumber daya manusia. Keberhasilan mitigasi risiko digital sangat dipengaruhi oleh kompetensi pegawai. Seluruh karyawan, khususnya pada bagian layanan nasabah, teknologi informasi, audit internal, dan manajemen risiko, perlu memperoleh pelatihan mengenai karakteristik deepfake, teknik social engineering, phishing berbasis AI, serta prosedur verifikasi identitas digital. Peningkatan literasi keamanan siber juga harus diberikan kepada nasabah agar mereka mampu mengenali berbagai modus penipuan yang memanfaatkan teknologi AI.

Keempat, kesiapan regulasi dan kepatuhan (compliance readiness). Perbankan syariah harus memastikan seluruh kebijakan keamanan digital sejalan dengan regulasi yang ditetapkan oleh Otoritas Jasa Keuangan (OJK), Bank Indonesia, serta ketentuan perlindungan data pribadi. Selain itu, Dewan Pengawas Syariah (DPS) memiliki peran strategis dalam memastikan bahwa pemanfaatan AI tetap berada dalam koridor etika Islam, tidak mengandung unsur gharar (ketidakjelasan), tadlis (penipuan), maupun tindakan yang merugikan pihak lain.

Dari perspektif ekonomi Islam, ancaman deepfake dapat dikategorikan sebagai bentuk tadlis (penipuan) dan gharar (ketidakpastian) karena menciptakan informasi palsu yang dapat memengaruhi pengambilan keputusan ekonomi. Praktik tersebut jelas bertentangan dengan nilai-nilai syariah sebagaimana firman Allah SWT dalam QS. An-Nisa ayat 29 yang melarang pengambilan harta orang lain dengan cara yang batil. Rasulullah SAW juga menegaskan dalam hadis bahwa "Barang siapa menipu, maka ia bukan termasuk golongan kami" (HR. Muslim). Dengan demikian, penguatan sistem keamanan digital merupakan implementasi nyata dari prinsip perlindungan harta (hifz al-mal) dan penjagaan kemaslahatan (maslahah) dalam sistem keuangan syariah.

Dalam konteks transformasi digital, kesiapan perbankan syariah tidak hanya diukur dari kemampuan mengadopsi teknologi AI, tetapi juga dari kemampuannya membangun ekosistem keamanan digital yang adaptif terhadap perkembangan ancaman siber. Kolaborasi antara regulator, industri perbankan, perusahaan teknologi, akademisi, dan lembaga sertifikasi keamanan informasi menjadi faktor penting dalam menciptakan sistem keuangan syariah yang tangguh, terpercaya, dan berkelanjutan.

Secara keseluruhan, kesiapan perbankan syariah menghadapi risiko deepfake harus mengintegrasikan tiga aspek utama, yaitu ketahanan teknologi (technological resilience), ketahanan organisasi (organizational resilience), dan kepatuhan terhadap prinsip-prinsip syariah (sharia compliance). Integrasi ketiga aspek tersebut akan meningkatkan kepercayaan masyarakat terhadap layanan digital perbankan syariah sekaligus memperkuat stabilitas sistem keuangan syariah di era Artificial Intelligence.

KESIMPULAN

Kemajuan kecerdasan buatan Artificial intelligence (AI) telah mempercepat transformasi digital perbankan syariah, tetapi juga meningkatkan risiko deepfake dan bentuk penipuan digital lainnya, yang dapat membahayakan keamanan transaksi dan kepercayaan publik. Menurut temuan tinjauan pustaka, kemampuan perbankan syariah untuk menghadapi ancaman ini ditentukan tidak hanya oleh penggunaan teknologi keamanan canggih, tetapi juga oleh dukungan regulasi, manajemen risiko, kualitas sumber daya manusia, dan literasi digital. Sistem keamanan berbasis Artificial intelligence (AI), otentikasi biometrik berlapis, teknologi deteksi deepfake, pemantauan transaksi waktu nyata, dan edukasi pelanggan adalah semua langkah strategis yang diperlukan untuk memperkuat prinsip-prinsip Syariah seperti kepercayaan, keadilan, dan transparansi. Akibatnya, perbankan Syariah harus mengintegrasikan inovasi teknologi, tata kelola keamanan siber, dan kapasitas sumber daya manusia untuk secara efektif melawan ancaman deepfake dan penipuan digital sambil juga memastikan keberlanjutan dan daya saing jangka panjangnya di era kecerdasan buatan.

REFERENSI

Anugrah, Z., Qamar, N., & Sutiawati, S. (2026). Behind the Advancement of Artificial Intelligence Lies Deepfake as a Threat of Modern Digital Fraud. 1(2), 1–13.

Arifin, S., Mustofa, Rachmawati, S., & Zahroh, F. (2025). Harmoni Digital dalam Keuangan Islam: Tinjauan Pustaka Tentang Kepatuhan Syariah dan Integrasi Teknologi. Al-Kharaj: Jurnal Ekonomi, Keuangan & Bisnis Syariah, 7(9), 3641–3659. https://doi.org/10.47467/alkharaj.v7i9.8163

Dedes, K., Prasetya, A., Laksana, E. P., Ramadhani, L., & Setia, V. (2022). Peran Etika dalam Teknologi Informasi. Jurnal Inovasi Teknologi Dan Edukasi Teknik, 2(1), 11–19. https://doi.org/10.17977/um068v2i12022p11-19

Fraud, S. (2026). Journal of Data Science and Analytics AI-Enhanced SOC Operations for Deepfake and Synthetic Fraud Detection in Banking : A Comparative Study with Traditional. January, 87–129. https://doi.org/10.63125/ykaw3t36

Gunawan, I. J., & Janisriwati, S. (2023). Legal Analysis on the Use of Deepfake Technology: Threats to Indonesian Banking Institutions. Law and Justice, 8(2), 192–210. https://doi.org/10.23917/laj.v8i2.2513

Handono, T., Aziz, H., Azhari, M. R., & Alqodri, A. (2026). Perlindungan Hukum Nasabah Terhadap Deepfake Fraud Pada Perbankan Digital Di Indonesia. 6838–6847.

Irsyad, M. (2025). Iqtishaduna, Vol. 16 No. 2 December 2025. 16(2).

Ke, Z., Zhou, S., Zhou, Y., Chang, C. H., & Zhang, R. (2025). Detection of AI Deepfake and Fraud in Online Payments Using GAN-Based Models. 2025 8th International Conference on Advanced Algorithms and Control Engineering, ICAACE 2025, 1786–1790. https://doi.org/10.1109/ICAACE65325.2025.11020513

Nazim Ali, S., & Hakim Jumat, Z. (2024). Islamic finance in the age of digital transformation: an introduction. Islamic Finance in the Digital Age, 1–7. https://doi.org/10.4337/9781035322954.00009

Popa, C., Pallath, R., Cunningham, L., Tahiri, H., Kesavarajah, A., & Wu, T. (2025). Deepfake Technology Unveiled: The Commoditization of AI and Its Impact on Digital Trust. http://arxiv.org/abs/2506.07363

Wahab, R., & Ihsan, M. (2025). Revolusi digital perbankan syariah. Jurnal Revolusi Digital, 7(1), 87–99.

Fadhil, M., Hermansyah, T., Muda, I., & Soemitra, A. (2025). Analisis Deskriptif Literasi Digital Terhadap Minat Adopsi Layanan Digital Berbasis AI. Jurnal Masharif Al-Syariah: Jurnal Ekonomi Dan Perbankan Syariah, 10(5), 3445–3460. https://journal.um-surabaya.ac.id/Mas/article/view/28852/10039

Teknologi, I., & Dahlan, A. (2025). Pengembangan Model Manajemen Risiko Terintegrasi untuk Inovasi Digital Perbankan Syariah. 11(06), 97–104.

Umum, K. (2014). Lembaran Negara. 184, 1–27.