aml/cft journal
journal of anti-money laundering / countering the financing of terrorism

Original paper

# Tren Keamanan Siber dan Evolusi Fraud Pada Sektor Perbankan di Era Digital

**Jum'an[1]* , Muhammad Asyura[2]**
[1] Fakultas Ekonomi dan Bisnis Islam, Institut Agama Islam Sultan Muhammad Syafiuddin Sambas, Indonesia
[2] Politeknik Negeri Sambas, Indonesia

Korespondensi penulis: juman.sambas123@gmail.com

*Kata Kunci:*
Fraud, Keamanan Siber, Media Sosial, Perbankan

**Abstrak**

Transformasi digital dalam sektor perbankan telah meningkatkan efisiensi layanan keuangan, namun sekaligus memperbesar risiko kejahatan siber dan fraud. Kejahatan keuangan perbankan tidak hanya bersumber dari pelaku internal, tetapi juga dari serangan eksternal yang memanfaatkan celah teknologi dan kelemahan perilaku pengguna. Penelitian ini bertujuan untuk mengkaji tren keamanan siber serta evolusi modus fraud pada sektor perbankan di era digital. Metode yang digunakan adalah pendekatan kualitatif melalui *Systematic Literature Review* (SLR) dengan menganalisis berbagai publikasi ilmiah yang relevan, menggunakan kerangka CIA Triad dan teori fraud sebagai dasar analisis. Hasil kajian menunjukkan bahwa ancaman utama yang dihadapi perbankan meliputi ransomware, kerentanan akibat penerapan kerja jarak jauh, serangan berbasis cloud, rekayasa sosial seperti phishing dan whaling, serta serangan rantai pasokan. Selain itu, modus fraud yang dominan pada layanan perbankan digital adalah social engineering dan phishing yang memanfaatkan faktor manusia sebagai titik lemah utama sistem keamanan. Temuan ini menegaskan bahwa keamanan siber dan fraud merupakan dua aspek yang saling terkait, sehingga diperlukan strategi mitigasi yang terintegrasi antara teknologi, proses bisnis, dan sumber daya manusia untuk memperkuat ketahanan sektor perbankan digital.

Dikirimkan: 14 Agustus 2024
Diterima: 6 Desember 2025
Diterbitkan: 6 Desember 2025



***Untuk mensitasi artikel ini*:** Jum'an. 2025. *Tren Keamanan Siber dan Evolusi Fraud Pada Sektor Perbankan di Era Digital. AML/CFT Journal: The Journal of Anti Money Laundering and Countering the Financing of Terrorism* 4(1):1-12, https://doi.org/10.59593/amlcft.2025.v4i1.225

## Pendahuluan

Dalam regulasi yang berkembang pesat saat ini, lembaga keuangan selalu berada di garis depan dalam memerangi kejahatan keuangan yang semakin kompleks serta canggih, tantangan yang dihadapi oleh lembaga keuangan memasuki tahun 2024 mengharuskan penerapan pendekatan yang proaktif serta adaptif terhadap manajemen risiko. Kejahatan keuangan telah berkembang mulai dari cara tradisional hingga meliputi metode digital, ancaman dunia maya dan penipuan. Risiko yang terjadi menuntut lembaga keuangan untuk mengevaluasi sistem keuangan serta memprioritaskan manajemen risiko perbankan dan integritas sistem keuangan.

Perbankan sebagai sektor vital dalam masyarakat menjadikan perbankan rentan terhadap penyalahgunaan wewenang dan tindakan kriminal, baik oleh pihak internal maupun eksternal yang mencoba memanfaatkannya untuk keuntungan pribadi atau kegiatan ilegal. Tindakan

kriminal dalam aktivitas perbankan seringkali melibatkan pelanggaran terhadap ketentuan resmi, yang dikenal sebagai tindak pidana perbankan. Karena itu, keamanan sistem perbankan menjadi sangat penting untuk melindungi informasi dan aset keuangan dari ancaman tersebut.[1]

Di era sekarang, di mana perkembangan teknologi terjadi dengan pesat, menyebabkan perubahan yang signifikan terhadap aspek sosial, ekonomi, dan budaya tidak terelakkan. Namun, di balik kemajuan ini, ada risiko seperti penyebaran virus, pembajakan, dan serangan terhadap layanan perangkat lunak. Serangan siber yang melibatkan pelaku dan korban dari berbagai negara, menjadi bentuk kejahatan lintas batas yang serius. Hal ini juga membuka peluang bagi individu atau keompok untuk melakukan serangan tehadap sistem teknologi. Serangan siber merupakan kejahatan baru yang muncul sebagai akibat dari berkembangnya teknologi informasi.[2]

Kejahatan keuangan merupakan istilah umum yang mencakup setiap jenis tindakan criminal yang terkait dengan entitas dan pasar keuangan, termasuk bank, perusahaan fintech, pemberi pinjaman, dan sebagainya. Salah satu jenis kejahatan keuangan yang marak atau banyak terjadi pada saat ini dan menjadi kekhawatiran bagi orang di sektor ini dan juga tentunya pemerintah serta masyarakat.[3]

Sektor perbankan menghadapi berbagai tantangan dalam mengatasi ancaman siber yang terus berkembang. Salah satu tantangan utama adalah peran teknologi yang semakin canggih, yang memungkinkan penjahat siber untuk menciptakan metode baru dalam menyerang sistem perbankan. Selain itu, minimnya kesadaran mengenai pentingnya keamanan data baik di pihak bank maupun nasabah juga menjadi faktor yang memperburuk kondisi ini. Di sisi lain, perbankan harus tetap menjaga kelancaran operasional dan layanan kepada nasabah tanpa mengorbankan keamanan data yang mereka miliki. Seiring dengan tantangan-tantangan tersebut, sektor perbankan harus menemukan solusi inovatif untuk memperkuat keamanan siber.[4]

Melawan serangan siber, pastinya ada konsekuensi yang harus ditanggung oleh sektor perbankan. Sebab, pada dasarnya serangan siber pada sektor keuangan khususnya perbankan hampir 3 kali lebih banyak dibandingkan sektor lainnya. Adapun tujuan berasal dari pelaku kejahatan siber sangat majemuk. Ada yang hanya sekadar iseng dan terdapat juga yang termasuk kategori kejahatan berfokus demi keuntungan finansial. Keuntungan yang diperoleh dipergunakan untuk berbagai keperluan, keperluan pribadi hingga biaya politik.

Risiko ancaman siber tidak mampu diabaikan di era digital yang membuat industri keuangan saling terhubung saat ini, karena itu sangat penting untuk mengenali modus kejahatan siber serta cara mengantisipasinya guna melindungi kepentingan pribadi serta bisnis berasal ancaman siber tersebut. Sebagai pelaku industri keuangan, perbankan harus mempunyai perhatian yang sama penuhnya terkait ancaman siber, apalagi *fraud* yang menggunakan modus *social engineering* marak terjadi seiringnya penggunaan media sosial.

Kemananan siber ialah semua prosedur perlindungan yang digunakan buat meminimalisir gangguan pada ketersediaan, integritas, dan kerahasiaan dari sebuah informasi. Kerahasiaan

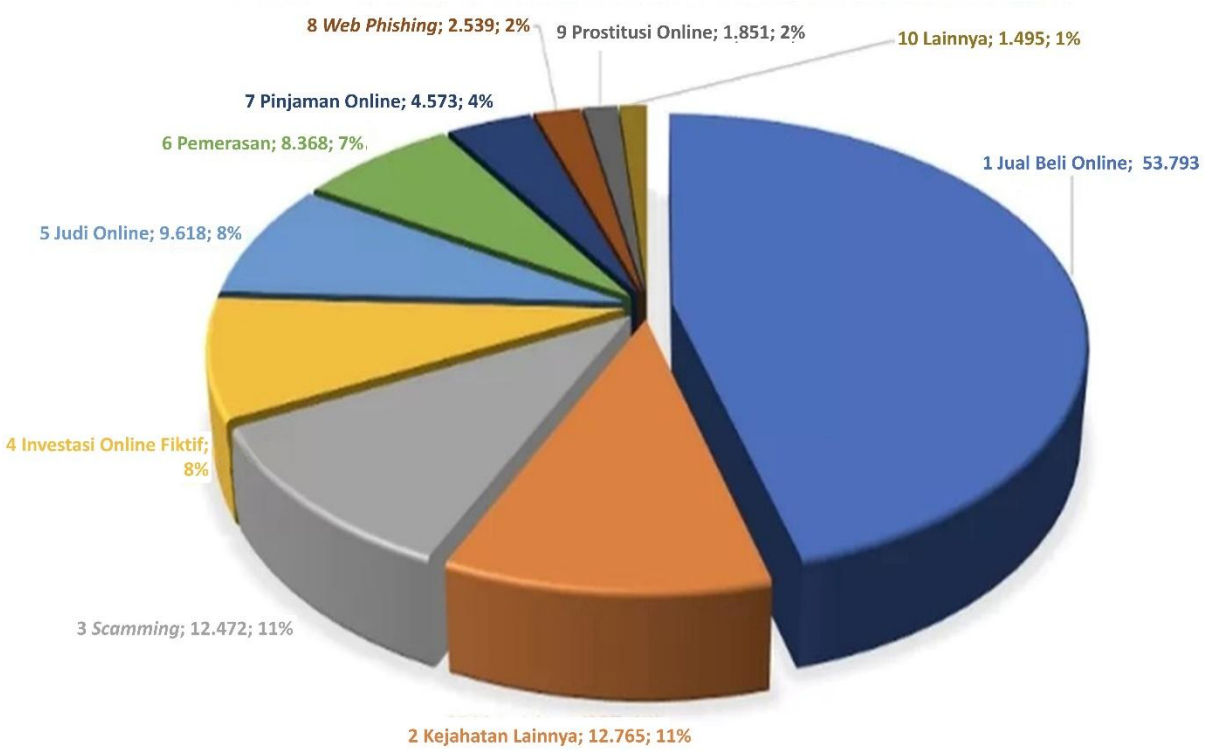
[1] Nida Rafa Arofah and Yeni Priatnasari, "Internet Banking dan Cyber Crime: Sebuah Studi Kasus di Perbankan Nasional," *Jurnal Pendidikan Akuntansi Indonesia* 18, no. 2 (2020): 107–19, https://doi.org/10.21831/jpai.v18i2.35872.

[2] Ervina Chintia et al., "Kasus Kejahatan Siber yang Paling Banyak Terjadi di Indonesia dan Penanganannya," *JIEET (Journal of Information Engineering and Educational Technology)* 2, no. 2 (2018): 65–69, https://doi.org/10.26740/jieet.v2n2.p65-69.

[3] Anisyah Nur Radiyah and Abshoril Fithry, "Kejahatan Keuangan pada Tindak Pidana Money Laundering dalam Menghilangkan Jejak Kejahatan," *Prosiding SNAPP: Sosial Humaniora, Pertanian, Kesehatan dan Teknologi* 2, no. 1 (2023): 39–45, https://doi.org/10.24929/snapp.v2i1.3179.

[4] Eka Febriantika Nur Afifah, Diny Widya Evriyanti Simatangkir, and Nafiza Salsabila Faliha, "Keamanan Siber dalam Perbankan serta Tantangan dan Solusi di Era Digital," *Jurnal Multidisiplin Ilmu Akademik* 2, no. 1 (2025): 33–42, https://doi.org/10.61722/jmia.v2i1.3119.

data merujuk pada akses yg disetujui terhadap sebuah data, yang berarti hanya pihak yang mempunyai akses saja yang dapat membukanya. Upaya untuk mendapatkan akses menggunakan cara mencuri informasi diartikan sebagai tindakan membahayakan kerahasiaan data.[5]




**Gambar 1. Statistik Kejahatan Siber Indonesia Tahun 2023**
Sumber: BSNN (2023)

Gambar 1 menunjukkan bahwa kegiatan yang paling banyak dilaporkan dan menjadi wahana utama kejahatan siber ialah jual beli online yg menempati peringkat 1 dengan 53.793 peristiwa dan menguasai 45,87% laporan dari keseluruhan, lalu diikuti oleh *Scamming* pada peringkat 2 dengan 12.472 insiden atau 10,63%. Investasi online fiktif ialah kerja *freelance online* yang sangat banyak memakan korban pencari kerja dan kemudian menipu korbannya untuk menyetorkan uang kepada penipu dengan iming-iming keuntungan besar, menempati peringkat 3 dengan laporan sebesar 9.618 peristiwa atau 8,36%. kemudian diikuti oleh aktivitas Judi Online sebesar 9.618 atau 7,13% dari total laporan. Pelaporan atas pemerasan yang dilakukan *debt collector* sebanyak 4.573 insiden atau 3.90%.[6]

Seiring dengan berkembangnya ancaman masalah *fraud* serta kejahatan keuangan yang menargetkan sektor perbankan dengan sangat cepat akibat didorong oleh kemajuan digital, para pelaku sektor perbankan harus bisa menyampaikan respon secara komprehensif. Respons tersebut perlu menegaskan langkah-langkah keamanan yang kuat, yang mencakup orang, proses bisnis serta teknologi. Berita umum yang dilakukan oleh GBG (*GB Group plc*) bekerjasama menggunakan *Chartis Risk* menyampaikan bahwa Indonesia menduduki peringkat teratas pada masalah aktivitas *money mule* (perkara *fraud* transfer) serta pencurian identitas yaitu 67%. Berita umum GBG serta *Chartis Risk* menggarisbawahi bahwa kasus *Fraud* terus

[5] Nikola Schmidt, "Critical Comments on Current Research Agenda in Cyber Security," *Obrana a Strategie* 14, no. 1 (2014): 29–38.
[6] Wahyu Subyanto, "Statistik Kejahatan Siber Indonesia 2023, Jual Beli Online Terbanyak Penipuan," nextren.grid.id, last modified November 27, 2023, https://nextren.grid.id/read/013955948/statistik-kejahatan-siber-indonesia-2023-jual-beli-online-terbanyak-penipuan?page=all.

bertransformasi dan berkembang. Indonesia menjadi sasaran utama sebab pasar produk digitalnya yang berkembang dan tingkat inklusi keuangan tinggi yang diperkirakan akan mencapai 90% pada tahun 2024. *Fraud* menjadi kata kecurangan yg mempunyai makna penyimpangan serta unsur pelanggaran aturan (*Illegal act*) yang sengaja dilakukan untuk tujuan tertentu seperti menyampaikan kesalahan atau menipu pihak lain yang dilakukan oleh satu orang atau lebih, baik dalam atau luar organisasi.[7]

*Fraud* merupakan ekspresi, kelalaian atau penyembunyian atau pengambaran yang menyesatkan sehingga orang lain terpedaya dan berujung pada kerugian.[8] *Association of Certified Fraud Examiners* mendefinisikan *Fraud* menjadi tindakan penipuan atau kekeliruan yang didesain oleh seorang atau badan yang mengetahui bahwa kekeliruan tersebut dapat menyebabkan beberapa manfaat yang tidak baik kepada individu atau pihak lain.[9]

Dalam dunia bisnis dan teknologi informasi, fraud atau kecurangan merupakan masalah yang serius. Salah satu teori yang banyak digunakan untuk memahami terjadinya fraud adalah Fraud Triangle, yang dikemukakan oleh Donald Cressey (1973). Teori ini menjelaskan bahwa fraud muncul apabila terdapat tiga faktor utama, yaitu *pressure* atau tekanan yang memotivasi seseorang untuk melakukan kecurangan, *opportunity* atau kesempatan yang memungkinkan tindakan tersebut dilakukan tanpa mudah terdeteksi, serta *rationalization* atau rasionalisasi yang memungkinkan individu membenarkan tindakannya.[10]

Seiring dengan berkembangnya teknologi informasi, perlindungan terhadap data dan sistem menjadi sangat penting. Konsep keamanan informasi biasanya dirujuk melalui CIA Triad, yang terdiri dari *confidentiality* (kerahasiaan), *integrity* (integritas), dan *availability* (ketersediaan).[11] Kerahasiaan menjamin informasi hanya diakses oleh pihak yang berhak, integritas memastikan data tetap akurat dan konsisten, sedangkan ketersediaan menjamin informasi dapat diakses ketika dibutuhkan. Ketiga prinsip ini menjadi landasan bagi pengembangan kebijakan, prosedur, dan teknologi keamanan informasi di berbagai organisasi.

Dalam konteks kejahatan digital, organisasi menghadapi risiko yang dapat menimbulkan kerugian signifikan. Model risiko kejahatan digital menekankan pentingnya memahami tiga komponen utama, yaitu *threat* (ancaman), *vulnerability* (kerentanan), dan *impact* (dampak). Ancaman adalah faktor yang dapat membahayakan sistem informasi, kerentanan adalah kelemahan yang memungkinkan ancaman terealisasi, sedangkan dampak menggambarkan kerugian yang muncul akibat terjadinya ancaman.[12] Risiko sendiri merupakan kombinasi dari kemungkinan ancaman terjadi dan besarnya dampak yang ditimbulkan. Pemahaman terhadap model ini memungkinkan organisasi melakukan *risk assessment* dan merancang kontrol yang efektif untuk mencegah atau memitigasi kejahatan digital.

Penelitian mengenai keamanan siber dan fraud perbankan era digital telah banyak dilakukan, baik di tingkat global maupun lokal, yang memperkuat temuan terkait modus kejahatan digital dan strategi mitigasinya.

---

[7] Imam Suhartadi, "Survei GBG: RI Duduki Peringkat Teratas Kasus Money Mule dan Pencurian Identitas," Investor.Id, last modified August 5, 2024, https://investor.id/business/369245/survei-gbg-ri-duduki-peringkat-teratas-kasus-money-mule-dan-pencurian-identitas.

[8] Daniel T. H. Manurung and Andhika Ligar Hardika, "Analysis of Factors that Influence Financial Statement Fraud in the Perspective Fraud Diamond: Empirical Study on Banking Companies Listed on the Indonesia Stock Exchange Year 2012 to 2014," *International Conference on Accounting Studies (ICAS) 2015* (2015): 280–86, https://doi.org/10.13140/RG.2.1.2058.8563.

[9] Ernst and Young, *Detecting Financial Statement Fraud: What Every Manager Needs to Know* (London: E & Y LLP, 2009).

[10] Donald R. Cressey, *Other People's Money: A Study in the Social Psychology of Embezzlement* (Montclair, NJ: Patterson Smith, 1973).

[11] M. E. Whitman and H. J. Mattord, *The CIA Triad: Confidentiality, Integrity, and Availability*, 4th ed. (Waltham, MA: Elsevier/Morgan Kaufmann, 2017).

[12] Gary Stoneburner, Alice Goguen, and Alexis Feringa, "Risk Management Guide for Information Technology Systems," *NIST Special Publication* 800, no. 30 (2002): 800–830.

Naam (2013) melakukan penelitian khususnya mengenai bagaimana pertahanan diri dari serangan malware dengan mengindentifikasi jalur kerja serta jenis dari malware itu sendiri. Tujuan dari penelitianya adalah bagaimana memberikan solusi dari serangan malware dengan menganalisis cara kerja dan jenis malware untuk mengetahui langkah-langkah yang dapat dilakukan menanggulangi dampak dari infeksi malware pada system komputer.[13] Faridi (2018) melakukan penelitian terkait kejahatan siber dalam bidang perbankan. Tujuan dari penelitiannya adalah bagaimana mengidentifikasi jenis-jenis kejahatan perbankan serta bagaimana cara pencegahan dan penanggulangan tindak kejahatan pada perbankan.[14] Meliana and Hartono (2019) melakukan penelitian tentang fraud perbankan Indonesia pada studi eksplorasi. Tujuan penelitiannya untuk melihat secara mendalam apa yang memotivasi pelaku kejahatan perbankan di Indonesia.[15] Setiawan and Wahyudi (2023) melakukan penelitian tentang pencegahan *fraud* pada kejahatan siber Perbankan. Penelitian ini bertujuan untuk menjelaskan realitas kasus kejahatan dunia maya pada internet banking di Indonesia dan memberikan alternatif pencegahan untuk meminimalisir terjadinya kejahatan dunia maya pada internet banking di Indonesia.[16] Penelitian Alodhiani (2023) yang berjudul sistematis tinjauan literatur Financial Technology (*Fintech*) dan keamanan siber bertujuan untuk mengenali ancaman dunia maya dan keamanan siber pada sektor keuangan serta tindakan yang dapat diambil oleh sektor keuangan.[17] Penelitian oleh Nur Afifah, Simatangkir, dan Faliha (2023) menegaskan bahwa malware, phishing, dan serangan DDoS (Distributed Denial of Service) menjadi ancaman nyata bagi perbankan digital di Indonesia.[18]

Syahraeni et al. (2024) meneliti tentang kasus penipuan di perbankan Syariah pada analisis Fraud internal dan implikasinya terhadap kepercayaan nasabah. Penelitian ini bertujuan untuk menganalisis faktor-faktor penyebab *fraud* serta mengevaluasi efektivitas sistem pengendalian internal dan kebijakan anti penipuan yang direrapkan oleh lembaga.[19] Balaka et al. (2024) meneliti tentang pencurian informasi nasabah di sektor perbankan yang merupakan ancaman serius di era digital. Penelitiannya bertujuan untuk melihat bagaimana modus operandi *cyber crime* dalam pencurian data nasabah di sektor perbankan serta bagaimana upaya pencegahan tindak pidana pencurian data nasabah disektor perbankan yang dilakukan secara siber.[20] Azzahra et al. (2024) melakukan penelitian tentang literatur mengenai ancaman cybercrime dan implementasi keamanan siber di sektor perbankan, bertujuan mengidentifikasi ancaman utama *cyber crime*, mengevaluasi langkah-langkah keamanan bank, dan merekomendasikan strategi peningkatan keamanan siber.[21] Penelitian Munajat and Yusuf (2024) mengenai peran teknologi

[13] Jufriadif Naam, "Metoda Pertahan Diri Program Virus," *Jurnal PROCESSOR* 8, no. 2 (2013): 36.

[14] Muhammad Khairul Faridi, "Kejahatan Siber dalam Bidang Perbankan," *Cyber Security dan Forensik Digital* 1, no. 2 (2018): 57–61, https://doi.org/10.14421/csecurity.2018.1.2.1373.

[15] Meliana Meliana and Trie Rundi Hartono, "Fraud Perbankan Indonesia: Studi Eksplorasi," *Prosiding Seminar Nasional Pakar* 1, no. 1 (2019): 2521–27, https://doi.org/10.25105/pakar.v0i0.4335.

[16] Nanang Setiawan and Imam Wahyudi, "Pencegahan Fraud pada Kejahatan Siber Perbankan," *Kabillah: Journal of Social Community* 8, no. 1 (2023): 508–18, https://doi.org/10.35127/kabillah.v8i1.280.

[17] Ahmed Abdulrhman B. Alodhiani, "Financial Technology (Fintech) and Cybersecurity: A Systematic Literature Review.," *Arab Journal for Humanities and Social Sciences*, no. 20 (2023), https://doi.org/10.59735/arabjhs.vi20.55.

[18] Afifah, Simatangkir, and Faliha, "Keamanan Siber dalam Perbankan serta Tantangan dan Solusi Di Era Digital."

[19] Syahraeni Syahraeni, Nur Hikmah, and Sitti Nikmah Marzuki, "Kasus Penipuan di Perbankan Syariah: Analisis Fraud Internal dan Implikasinya terhadap Kepercayaan Nasabah," *Lan Tabur: Jurnal Ekonomi Syariah* 6, no. 1 (2024): 122–40, https://doi.org/10.53515/lantabur.2024.6.1.122-140.

[20] Kemal Idris Balaka, Aulia Rahman Hakim, and Frygyta Dwi Sulistyany, "Pencurian Informasi Nasabah Di Sektor Perbankan: Ancaman Serius di Era Digital," *Yustitiabelen* 10, no. 2 (2024): 105–30, https://doi.org/10.36563/yustitiabelen.v10i2.1167.

[21] Nasywa Shafa Azzahra et al., "Tinjauan Literatur tentang Ancaman Cybercrime dan Implementasi Keamanan Siber di Industri Perbankan," *HUMANITIS: Jurnal Homaniora, Sosial dan Bisnis* 2, no. 7 (2024): 692–700.

informasi dalam pencegahan dan pengungkapan tindak pidana ekonomi khusus studi tentang kejahatan keuangan berbasis digital. Penelitian ini mengulas peran teknologi seperti kecerdasan buatan (AI), analisis big data, dan blockchain dalam mendeteksi aktivitas mencurigakan di sektor keuangan.[22]

Studi sistematis oleh Waliullah et al. (2025) menunjukkan bahwa ancaman siber seperti phishing, malware, dan *ransomware* menjadi faktor utama yang memengaruhi adopsi dan pertumbuhan layanan digital banking, dan menekankan pentingnya penerapan teknologi keamanan seperti multi-factor authentication (MFA) dan biometrik.[23] Selaras dengan itu, George et al. (2023) melalui review terhadap 118 studi terkait mendapati bahwa penggunaan machine learning, termasuk metode supervised dan deep learning, semakin efektif dalam mendeteksi pola fraud baru, meskipun implementasi real-time masih menjadi tantangan.[24]

Beberapa penelitian terdahulu menunjukkan kesenjangan penelitian (*research gap*) yang melatarbelakangi penelitian ini yaitu keterpisahan fokus antara studi keamanan siber dan studi *fraud* finansial. Penelitian terdahulu umumnya menyoroti salah satu aspek *cyber security* atau *financial fraud* namun belum mengintegrasikan keduanya secara sistematis dalam konteks sektor perbankan, Kurangnya kajian mengenai tren dan evolusi modus fraud digital di era perbankan modern. Sebagian besar penelitian terdahulu masih membahas kasus klasik fraud atau keamanan sistem konvensional, belum menyesuaikan dengan perubahan pola serangan yang semakin kompleks dan terotomatisasi, Minimnya pendekatan empiris dan multidimensional. Beberapa penelitian masih bersifat konseptual atau studi literatur, belum membahas keterkaitan antara teknologi keamanan, perilaku pelaku, serta efektivitas sistem pertahanan siber perbankan. Belum ada model konseptual atau kerangka analisis yang mengaitkan keamanan siber, perilaku *fraud*, dan kepercayaan nasabah. Dengan demikian, penelitian ini berbeda secara signifikan dari penelitian-penelitian sebelumnya karena Tidak hanya membahas aspek keamanan atau fraud secara terpisah, tetapi menggabungkan kedua dimensi tersebut dalam satu kerangka analisis yang saling berhubungan, Memberikan analisis tren dan pola kejahatan yang lebih mutakhir sesuai dengan transformasi digital sektor perbankan serta Menawarkan kontribusi teoritis dan praktis, baik dalam pemahaman perilaku *fraud* digital maupun strategi penguatan keamanan siber perbankan

Penelitian ini hadir untuk mengisi celah tersebut yang bertujuan untuk mengetahui bagaimana tren keamanan siber dan evolusi modus fraud pada sektor perbankan di era digital. Kondisi ini perlu mendapat perhatian khusus terkait tindak kejahatan yang terjadi pada sektor perbankan menginggat akhir-akhir ini masih banyak laporan-laporan yang dilakukan oleh masyarakat atas kejahatan keuangan yang dialaminya. Metode penelitian dalam penelitian ini menggunakan pendekatan *Systematic Literature Review* (SLR) untuk secara sistematis mengidentifikasi, menyeleksi, dan menganalisis literatur terkait keamanan siber dan modus fraud di sektor perbankan. Pendekatan SLR dipilih karena memungkinkan kajian literatur yang transparan, terstruktur, dan dapat direplikasi, sehingga memberikan gambaran komprehensif tentang tren penelitian serta evolusi modus kejahatan digital. Proses penelitian dimulai dengan perumusan tujuan dan pertanyaan penelitian, yaitu untuk mengidentifikasi jenis fraud yang sering terjadi di sektor perbankan digital, membahas aspek keamanan informasi seperti *confidentiality, integrity, dan availabilit*y. Hasil dari penelitian ini diharapkan dapat

[22] Andi Ahmad Munajat and Hudi Yusuf, "Peran Teknologi Informasi dalam Pencegahan dan Pengungkapan Tindak Pidana Ekonomi Khusus: Studi Tentang Kejahatan Keuangan Berbasis Digital," *Jurnal Intelek Insan Cendikia* 1, no. 9 (2024): 4853–65.

[23] Md Waliullah et al., "Assessing the Influence of Cybersecurity Threats and Risks on the Adoption and Growth of Digital Banking: A Systematic Literature Review," *American Journal of Advanced Technology and Engineering Solutions* 1, no. 1 (2025): 226–57, https://doi.org/10.63125/fh49gz18.

[24] Md Zahin Hossain George, Md Khorshed Alam, and Md Tarek Hasan, "Machine Learning for Fraud Detection in Digital Banking: A Systematic Literature Review REVIEW," *ASRC Procedia: Global Perspectives in Science and Scholarship* 3, no. 1 (2023): 37–61, https://doi.org/10.63125/913ksy63.

memberikan dasar ilmiah yang kuat bagi pengembangan kebijakan keamanan informasi, strategi mitigasi risiko fraud, dan perencanaan sistem perlindungan data di sektor perbankan, sekaligus menjadi referensi bagi penelitian lanjutan di bidang keamanan siber dan kejahatan digital.

## Pembahasan

### Tren Keamanan Siber pada Sektor Perbankan

Digitalisasi sebagai fenomena yang menyasar ke berbagai sektor kehidupan, salah satunya ialah sektor perbankan. Digitalisasi perbankan memberikan kemudahan namun juga risiko yang wajib dihindari, salah satunya ialah tentang keamanan siber. Keamanan siber dalam dunia perbankan menjadi perhatian khusus terlebih dengan maraknya kejahatan siber yang tejadi pada bank-bank nasional.

Menurut ISO (*International Organization for Standardization*) (2018) keamanan siber adalah sebagai tindakan untuk melindungi sistem komputer dari serangan digital atau akses ilegal.[25] Terdapat beberapa elemen dari *cybersecurity* antara lain, *application security, information security, cloud security, network security, disaster recovery/business continuity planning, operational security,* dan *end-user education*. Elemen-elemen ini sangat penting guna memastikan keamanan *cybersecurity* secara keseluruhan, karena risiko terkena ancaman digital terus meningkat dan ancamannya pun semakin beragam. Maka dari itu, penting untuk melindungi sistem bahkan dari risiko terkecil sekalipun.[26]

Keamanan siber berperan krusial untuk mencegah serangan yang bertujuan menonaktifkan atau menghambat operasional sistem atau perangkat.Meningkatnya ancaman siber yang semakin canggih serta maraknya insiden siber menuntut kewaspadaan serta kemampuan bank untuk menghadapi serta menangani ancaman yang timbul. Peristiwa siber yang tidak ditangani dengan baik dapat merusak proses bisnis perbankan yang akan berdampak secara luas. Selain itu, keamanan siber yg kurang memadai pula akan berdampak di hilangnya kepercayaan terhadap bank serta bisa menimbulkan risiko reputasi yang relatif substansial.

Menurut National Cyber Security Center (CNS), Beberapa tren keamanan siber yang harus diwaspadai oleh sektor perbankan sebagai berikut:[27]

1. *Ransomware*

   Beberapa tahun terakhir Virus *ransomware* menjadi sebuah masalah besar bagi organisasi di seluruh dunia. Jenis virus ini merupakan metode kejahatan dunia maya di mana berkas dienkripsi serta pengguna dikunci, sementara itu penjahat meminta uang untuk mengakses kembali sistem tersebut. Organisasi yang terdampak serangan *ransomware* sistemnya akan lumpuh pada waktu yang lama, terutama bagi organisasi yang tak memiliki cadangan.
2. Risiko Berkelanjutan Berasal Kerja Jeda Jauh

   Saat pandemi memasuki tahun keempat, ketergantungan pada kerja menjadi jauh dan sistem perangkat lunak berbasis *cloud* telah menjadi hal yang wajar. Hal ini berarti bahwa sektor perbankan lebih banyak memiliki potensi kerentanan siber daripada sektor lainnya. Karyawan tidak akan selalu mengakses data di sistem serta jaringan yang akan dikendalikan oleh suatu organisasi, sebagai akibatnya kewaspadaan yang komprehensif sangat diperlukan.

[25] ISO, *ISO/IEC 27005:2018 Information Technology - Security Techniques - Information Security Risk Management* (Geneva, Switzerland: International Organization for Standardization (ISO), 2018).

[26] ISO, *ISO/IEC 27005:2018 Information Technology - Security Techniques - Information Security Risk Management*.

[27] Ervina Anggraini, "Antisipasi 5 Tren Keamanan Siber Ini di 2024!," CTI - Biggest IT Distributor Company in Indonesia, last modified December 15, 2023, https://computradetech.com/id/blog-id/antisipasi-5-tren-keamanan-siber-ini-di-2024/.

3. Serangan Siber Berbasis *Cloud*

   Dengan banyaknya sistem perangkat lunak dan data yang disimpan di *cloud*, penjahat di dunia maya akan memanfaatkannya, dan akibatnya peningkatan serangan berbasis *cloud* telah menjadi salah satu ancaman dunia maya yang paling umum bagi sektor perbankan. Bank perlu memastikan bahwa infrastruktur *cloud* dikonfigurasi dengan aman untuk melindungi dari pelanggaran yang berbahaya.
4. Rekayasa Sosial

   Salah satu ancaman terbesar baru-baru ini pada sektor perbankan adalah rekayasa sosial. Orang-orang sering kali menjadi mata rantai yang paling rentan dalam rantai keamanan. Orang-orang dapat ditipu agar memberikan informasi dan kredensial yang sensitif. Hal tersebut juga dapat memengaruhi karyawan bank bahkan nasabahnya. Rekayasa sosial dapat terjadi dalam berbagai bentuk yaitu melalui serangan *phishing* atau *whaling* dan dengan mengirimkan faktur palsu yang mengaku berasal dari sumber yang terpercaya. Penting untuk terus memberikan informasi kepada karyawan terkait dengan taktik rekayasa sosial dan bagaimana ancaman ini berkembang.
5. Serangan Rantai Pasokan

   Metode penyebaran *malware* yang semakin popular oleh penjahat di dunia maya adalah dengan menargetkan vendor perangkat lunak kemudian mengirimkan kode berbahaya kepada pelanggan dan pihak lain dalam rantai pasokan pada suatu produk. Serangan jenis ini dapat membahayakan sistem distribusi dan memungkinkan penjahat dunia maya memasuki jaringan pelanggan.

   Beberapa langkah preventif yang harus dilakukan oleh pemangku kebijakan (dalam hal ini adalah pemerintah) untuk penanggulangan kejahatan Siber.[28] Pertama, melakukan modernisasi hukum pidana nasional beserta hukum acaranya, yang diselaraskan dengan konvensi internasional yang terkait dengan kejahatan tersebut. Kedua, meningkatkan sistem pengamanan jaringan computer nasional sesuai standar internasional. Ketiga, meningkatkan pemahaman serta keahlian aparatur penegak hukum mengenai upaya pencegahan, investigasi dan penuntutan perkara-perkara yang berhubungan dengan *cyber-crime*

## Modus *Fraud* pada Sektor Perbankan

Perkembangan teknologi yang sangat pesat mempengaruhi cara masyarakat dalam melakukan kegiatan perbankan. ketika ini, masyarakat bisa melakukan transaksi *online banking* secara digital melalui *smartphone*. Hal ini tentunya menuntut sektor perbankan untuk menyediakan layanan transaksi *online banking* yang aman. Perbankan telah menyediakan fitur keamaan yang canggih, namun pelaku kejahatan berupaya mencari celah untuk melakukan penipuan serta mengambil keuntungan dari korbannya. Modus penipuan yang banyak terjadi dalan transaksi *online banking* ialah *Social Engineering* serta *phishing.* Pelaku melakukan teknik manipulasi yang memanfaatkan kelengahan kepada korban menggunakan tujuan untuk menerima akses atas info pribadi dan data perbankan milik korban mirip User ID, *password*, PIN dan sebagainya.

Otoritas Jasa Keuangan melaporkan modus baru terkait penipuan pada sektor perbankan yang terus berkembang dan memunculkan penemuan baru. terdapat beberapa modus yang termasuk baru ialah modus salah transfer yang dilakukan oleh Pinjaman Online (Pinjol) illegal. Modus tersebut ditandai dengan adanya uang masuk dari entitas pinjol illegal, padahal pemilik rekening tidak mengajukan pinjaman. Modus ini umumnya akan diikuti dengan adanya kegiatan penagihan yang terjadi melalui telepon yang terhitung utang dengan bunga pinjaman yang memberatkan.

[28] Dista Amalia Arifah, "Kasus Cybercrime di Indonesia," *Jurnal Bisnis dan Ekonomi* 18, no. 2 (2011): 185–95.

Modus fraud yang paling sering terjadi adalah *phishing* dan *social engineering*. Pelaku menggunakan teknik manipulasi psikologis untuk menipu nasabah agar memberikan informasi pribadi seperti User ID, password, dan PIN. Informasi ini kemudian digunakan untuk mengakses rekening korban dan menguras saldo. Modus ini memanfaatkan celah dalam kerahasiaan (*confidentiality*) sistem perbankan digital, menunjukkan bahwa meskipun teknologi perbankan sudah canggih, faktor manusia tetap menjadi titik lemah utama.

Selain itu, muncul modus salah transfer oleh Pinjaman Online (Pinjol) ilegal, yang tergolong baru. Dalam kasus ini, uang masuk ke rekening nasabah tanpa permintaan pinjaman, dan kemudian diikuti oleh penagihan palsu melalui telepon dengan bunga yang membebani korban. Modus ini menunjukkan kombinasi celah teknis dan manipulasi sosial, serta menekankan pentingnya pengawasan integritas data **(***integrity***)** dan validasi transaksi dalam sistem perbankan.

Modus lain yang ditemukan adalah penipuan melalui website palsu atau aplikasi ilegal yang meniru situs resmi bank. Nasabah diarahkan untuk melakukan konfirmasi transaksi, kemudian memasukkan data sensitif mereka. Kejadian ini memanfaatkan celah ketersediaan dan keamanan sistem**,** karena pelaku mampu memanfaatkan fitur yang seharusnya mempermudah layanan nasabah untuk melakukan tindakan fraud.

*Fraud* pada sistem perbankan diharapkan setidaknya mereda, karena *fraud* tidak bisa dihilangkan sampai nihil. Harapan berkurangnya *fraud* tersebut sangat bergantung pada kesiapan masing-masing bank untuk mencegahnya. Hal ini perlu dilakukan upaya yang jelas, nyata, perlu aksi serta tidak hanya sekadar bicara. Perlu ada campur tangan pemerintah untuk membongkar masalah demi masalah yang tidak mengenakan. Sektor perbankan dihadapkan di dua pilihan yaitu membentuk lingkungan dengan potensi *fraud* yang rendah atau menyusul bobolnya bank-bank terdahulu.

Berdasarkan Peraturan OJK (Otoritas Jasa Keuangan) Nomor 39/POJK.03/2019, berikut ini adalah hal yang digunakan untuk menghindari modus *Fraud* pada sektor perbankan untuk dapat dilakukan, adalah sebagai berikut:[29]

1. Ciptakan Kontrol internal yang baik. Kontrol internal yang baik setidaknya wajib meliputi kontrol lingkungan yang baik, sistem akuntansi yang canggih dan kontrol mekanisme yang bagus. Kuncinya kontrol lingkungan wajib memiliki integritas, nilai etika dan kompetensi sumber daya manusia, gaya serta filosofi manajemen serta perhatian dan arahan dewan direksi. Sementara kontrol akuntansi yang baik harus menyampaikan berita yang benar, lengkap serta tepat waktu. Kontrol prosedur yang baik wajib mencakup beberapa hal yaitu mencakup kontrol fisik atas asset-asset, otoritas yang tepat, pengecekan independen, serta dokumentasi yang lengkap.
2. Menyebarkan informasi kepada nasabah tentang kebijakan bank, contohnya perilaku suap untuk memperoleh kucuran dana. Bank mampu membentuk surat secara periodik kepada nasabah yang mengungkapkan tentang kebijakan perusahaan yang tidak menerima segala jenis suap
3. Supervisi personel. Para pelaku *fraud* umumnya menggunakan hasil jarahannya untuk mendukung gaya hidup yang mewah. Mengawasi gaya hidup setiap personel dan fasilitas eksklusif pada sekelilingnya, bank bisa melakukan langkah pencegahan, karena para personel yang berpotensi melakukan *fraud* seolah-olah merasa diawasi.
4. Membentuk jalur spesifik pelaporan *fraud* (tips online). Secanggih apapun fraud dilakukan, tak jarang *fraud* bisa ditemukan melalui tips. Saat seorang personel merasakan bahwa rekan kerjanya mempunyai cara yang sangat praktis untuk melaporkan terjadinya *fraud*.

*Proactive fraud auditing*. Seringkali pemeriksaan terhadap fraud dilakukan sesudah terdapat korban, yang ialah bersifat reaktif. Audit yang bersifat pro-aktif diharapkan akan

[29] Otoritas Jasa Keuangan (OJK), *Peraturan OJK Nomor 39/POJK.03/2019 Tentang Penerapan Strategi Anti-Fraud Bagi Bank Umum* (Jakarta: OJK, 2019).

menciptakan kesadaran para personel bahwa apa yang dilakukannya bisa saja direview. Hal ini akan memberikan para personel rasa takut akan tertangkap jika melakukan *fraud* Hasil kajian literatur melalui pendekatan *Systematic Literature Review* (SLR) dan proses seleksi PRISMA menunjukkan adanya pola umum dalam modus *fraud* di sektor perbankan era digital, termasuk *phishing, skimming, insider threat,* dan *malware* banking. Meta-analisis terhadap data kuantitatif dari studi terpilih memperlihatkan bahwa *fraud* yang melibatkan kombinasi kelemahan teknis dan faktor manusia memiliki probabilitas kerugian lebih tinggi dibandingkan kasus yang hanya disebabkan oleh satu faktor. Sementara itu, penerapan prinsip *confidentiality*, *integrity*, dan *availability* (CIA Triad) secara konsisten dikaitkan dengan penurunan kejadian *fraud*, meskipun efektivitasnya berbeda-beda tergantung pada kesiapan infrastruktur TI (Teknologi Informasi), budaya organisasi, dan regulasi yang berlaku. Analisis kritis dari literatur menunjukkan bahwa sebagian besar penelitian lebih menekankan aspek teknis keamanan siber, seperti enkripsi, firewall, dan monitoring, sementara integrasi antara faktor manusia, perilaku internal karyawan, dan budaya organisasi masih kurang mendapat perhatian. Perbandingan antar studi juga mengungkapkan variasi geografis dan kontekstual; studi dari negara maju cenderung memiliki kerangka keamanan lebih matang, data lebih terdokumentasi, dan fokus pada mitigasi berbasis teknologi, sedangkan studi di negara berkembang lebih menekankan tantangan implementasi, keterbatasan sumber daya, dan kebutuhan penguatan regulasi. Temuan ini menegaskan bahwa keamanan siber dan fraud tidak dapat dipisahkan secara konseptual, karena kelemahan teknis yang tidak diimbangi pengelolaan risiko manusia dapat membuka peluang bagi terjadinya *fraud*. Dengan demikian, hasil penelitian ini memberikan wawasan kritis mengenai hubungan antara teknologi, proses, dan perilaku manusia, serta menjadi dasar bagi pengembangan strategi keamanan yang lebih holistik, perancangan kebijakan mitigasi risiko, dan panduan penelitian lanjutan untuk memahami interaksi kompleks antara keamanan siber dan modus *fraud* di era digital

## Kesimpulan

Beberapa tren keamanan siber yang harus diwaspadai oleh sektor perbankan, antara lain yaitu pertama, *ransomware* telah menjadi sebuah masalah besar bagi organisasi di seluruh dunia. Jenis virus ini adalah metode kejahatan dunia maya di mana berkas dienkripsi dan pengguna dikunci, sementara penjahat meminta uang untuk mengakses kembali sistem. Kedua, Risiko Berkelanjutan dari Kerja Jarak Jauh yang artinya bahwa sektor perbankan memiliki lebih banyak potensi kerentanan keamanan siber daripada sebelumnya. Karyawan tidak akan selalu mengakses data pada sistem dan jaringan yang akan dikendalikan oleh suatu organisasi, sehingga kewaspadaan yang ekstra sangat diperlukan. Ketiga, serangan siber berbasis *cloud* dengan banyaknya sistem perangkat lunak dan data yang disimpan, penjahat di dunia maya akan memanfaatkannya, dan akibatnya peningkatan serangan berbasis *cloud* telah menjadi salah satu ancaman dunia maya yang paling banyak bagi sektor perbankan. Keempat, Rekayasa Sosial dapat terjadi dalam berbagai bentuk yaitu melalui serangan *Phishing* atau *Whaling* dan dengan mengirimkan faktur palsu yang mengaku berasal dari sumber yang terpercaya. Kelima, serangan rantai pasokan metode penyebaran *malware* yang semakin popular oleh penjahat di dunia maya adalah dengan menargetkan vendor perangkat lunak kemudian mengirimkan kode berbahaya kepada pelanggan dan pihak lain dalam rantai pasokan dalam bentuk produk.

Perkembangan teknologi yang sangat pesat mempengaruhi cara masyarakat dalam melakukan aktivitas perbankan. Masyarakat bisa melakukan transaksi *online banking* secara digital melalui *smartphone.* Hal ini tentunya menuntut sektor perbankan untuk menyediakan layanan transaksi *online banking* yang aman. Meskipun perbankan telah menyediakan fitur keamaan yang canggih, tetapi pelaku kejahatan berupaya mencari celah untuk melakukan penipuan dan mengambil keuntungan dari korbannya. Modus penipuan yang seringkali terjadi dalan transaksi *online banking* ialah *social engineering* dan *phishing.*

**Daftar Pustaka**


Afifah, Eka Febriantika Nur, Diny Widya Evriyanti Simatangkir, and Nafiza Salsabila Faliha. "Keamanan Siber dalam Perbankan Serta Tantangan dan Solusi Di Era Digital." *Jurnal Multidisiplin Ilmu Akademik* 2, no. 1 (2025): 33–42. https://doi.org/10.61722/jmia.v2i1.3119.

Alodhiani, Ahmed Abdulrhman B. "Financial Technology (Fintech) and Cybersecurity: A Systematic Literature Review." *Arab Journal for Humanities and Social Sciences*, no. 20 (2023). https://doi.org/10.59735/arabjhs.vi20.55.

Anggraini, Ervina. "Antisipasi 5 Tren Keamanan Siber Ini di 2024!" CTI - Biggest IT Distributor Company in Indonesia. Last modified December 15, 2023. https://computradetech.com/id/blog-id/antisipasi-5-tren-keamanan-siber-ini-di-2024/.

Arifah, Dista Amalia. "Kasus Cybercrime di Indonesia." *Jurnal Bisnis dan Ekonomi* 18, no. 2 (2011): 185–95.

Arofah, Nida Rafa, and Yeni Priatnasari. "Internet Banking dan Cyber Crime: Sebuah Studi Kasus di Perbankan Nasional." *Jurnal Pendidikan Akuntansi Indonesia* 18, no. 2 (2020): 107–19. https://doi.org/10.21831/jpai.v18i2.35872.

Azzahra, Nasywa Shafa, Aron Micael Tambunan, Najwa Nayra Aulia, Arista Binarsih, and Tubagus Hedi Saepudin. "Tinjauan Literatur Tentang Ancaman Cybercrime dan Implementasi Keamanan Siber di Industri Perbankan." *HUMANITIS: Jurnal Homaniora, Sosial dan Bisnis* 2, no. 7 (2024): 692–700.

Balaka, Kemal Idris, Aulia Rahman Hakim, and Frygyta Dwi Sulistyany. "Pencurian Informasi Nasabah di Sektor Perbankan: Ancaman Serius di Era Digital." *Yustitiabelen* 10, no. 2 (2024): 105–30. https://doi.org/10.36563/yustitiabelen.v10i2.1167.

Chintia, Ervina, Rofiqoh Nadiah, Humayyun Nabila Ramadhani, Zulfikar Fahmi Haedar, Adam Febriansyah, and Nur Aini Rakhmawati. "Kasus Kejahatan Siber yang Paling Banyak Terjadi di Indonesia dan Penanganannya." *JIEET (Journal of Information Engineering and Educational Technology)* 2, no. 2 (2018): 65–69. https://doi.org/10.26740/jieet.v2n2.p65-69.

Cressey, Donald R. *Other People's Money: A Study in the Social Psychology of Embezzlement*. Montclair, NJ: Patterson Smith, 1973.

Ernst and Young. *Detecting Financial Statement Fraud: What Every Manager Needs to Know*. London: E & Y LLP, 2009.

Faridi, Muhammad Khairul. "Kejahatan Siber dalam Bidang Perbankan." *Cyber Security dan Forensik Digital* 1, no. 2 (2018): 57–61. https://doi.org/10.14421/csecurity.2018.1.2.1373.

George, Md Zahin Hossain, Md Khorshed Alam, and Md Tarek Hasan. "Machine Learning for Fraud Detection in Digital Banking: A Systematic Literature Review REVIEW." *ASRC Procedia: Global Perspectives in Science and Scholarship* 3, no. 1 (2023): 37–61. https://doi.org/10.63125/913ksy63.

ISO. *ISO/IEC 27005:2018 Information Technology - Security Techniques - Information Security Risk Management*. Geneva, Switzerland: International Organization for Standardization (ISO), 2018.

Manurung, Daniel T. H., and Andhika Ligar Hardika. "Analysis of Factors that Influence Financial Statement Fraud in the Perspective Fraud Diamond: Empirical Study on Banking Companies Listed on the Indonesia Stock Exchange Year 2012 to 2014." *International Conference on Accounting Studies (ICAS) 2015* (2015): 280–86. https://doi.org/10.13140/RG.2.1.2058.8563.

Meliana, Meliana, and Trie Rundi Hartono. "Fraud Perbankan Indonesia: Studi Eksplorasi." *Prosiding Seminar Nasional Pakar* 1, no. 1 (2019): 2521–27. https://doi.org/10.25105/pakar.v0i0.4335.

Munajat, Andi Ahmad, and Hudi Yusuf. "Peran Teknologi Informasi dalam Pencegahan dan Pengungkapan Tindak Pidana Ekonomi Khusus: Studi Tentang Kejahatan Keuangan Berbasis Digital." *Jurnal Intelek Insan Cendikia* 1, no. 9 (2024): 4853–65.

Naam, Jufriadif. "Metoda Pertahan Diri Program Virus." *Jurnal PROCESSOR* 8, no. 2 (2013): 36.

Otoritas Jasa Keuangan (OJK). *Peraturan OJK Nomor 39/POJK.03/2019 Tentang Penerapan Strategi Anti-Fraud Bagi Bank Umum*. Jakarta: OJK, 2019.

Radiyah, Anisyah Nur, and Abshoril Fithry. "Kejahatan Keuangan pada Tindak Pidana Money Laundering dalam Menghilangkan Jejak Kejahatan." *Prosiding SNAPP: Sosial Humaniora, Pertanian, Kesehatan dan Teknologi* 2, no. 1 (2023): 39–45. https://doi.org/10.24929/snapp.v2i1.3179.

Schmidt, Nikola. "Critical Comments on Current Research Agenda in Cyber Security." *Obrana a Strategie* 14, no. 1 (2014): 29–38.

Setiawan, Nanang, and Imam Wahyudi. "Pencegahan Fraud pada Kejahatan Siber Perbankan." *Kabillah : Journal of Social Community* 8, no. 1 (2023): 508–18. https://doi.org/10.35127/kabillah.v8i1.280.

Stoneburner, Gary, Alice Goguen, and Alexis Feringa. "Risk Management Guide for Information Technology Systems." *NIST Special Publication* 800, no. 30 (2002): 800–830.

Subyanto, Wahyu. "Statistik Kejahatan Siber Indonesia 2023, Jual Beli Online Terbanyak Penipuan." nextren.grid.id. Last modified November 27, 2023. https://nextren.grid.id/read/013955948/statistik-kejahatan-siber-indonesia-2023-jual-beli-online-terbanyak-penipuan?page=all.

Suhartadi, Imam. "Survei GBG: RI Duduki Peringkat Teratas Kasus Money Mule dan Pencurian Identitas." Investor.Id. Last modified August 5, 2024. https://investor.id/business/369245/survei-gbg-ri-duduki-peringkat-teratas-kasus-money-mule-dan-pencurian-identitas.

Syahraeni, Syahraeni, Nur Hikmah, and Sitti Nikmah Marzuki. "Kasus Penipuan di Perbankan Syariah: Analisis Fraud Internal dan Implikasinya terhadap Kepercayaan Nasabah." *Lan Tabur: Jurnal Ekonomi Syariah* 6, no. 1 (2024): 122–40. https://doi.org/10.53515/lantabur.2024.6.1.122-140.

Waliullah, Md, Md Zahin Hossain George, Md Tarek Hasan, Md Khorshed Alam, Mosa Sumaiya Khatun Munira, and Noor Alam Siddiqui. "Assessing the Influence of Cybersecurity Threats and Risks on the Adoption and Growth of Digital Banking: A Systematic Literature Review." *American Journal of Advanced Technology and Engineering Solutions* 1, no. 1 (2025): 226–57. https://doi.org/10.63125/fh49gz18.

Whitman, M. E., and H. J. Mattord. *The CIA Triad: Confidentiality, Integrity, and Availability*. 4th ed. Waltham, MA: Elsevier/Morgan Kaufmann, 2017.