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

Original paper

Deteksi Tipologi Pencucian Uang Berbasis *Graph Analytics* dan *Neural Network*

Lalu Garin Alham[1]*, Nadia Tsabitah[2], Yusuf Muhammad Nur Zaman[2]

[1] Fraud Management & Authorization, PT Espay Debit Indonesia Koe (DANA), Indonesia
[2] Audit, PT Bank Rakyat Indonesia Tbk (BRI), Indonesia

Korespondensi penulis: alhamgarin@gmail.com

Kata Kunci:
Kejahatan keuangan, Pembelajaran mesin, Pencucian uang, Teori graf

Abstrak

Pencucian uang diestimasi mencakup 2–5% dari Produk Domestik Bruto (PDB) global setiap tahunnya, dengan skala yang terus meningkat seiring ekspansi ekosistem digital. Sistem Anti-Pencucian Uang (AML) konvensional yang mengandalkan aturan (rule-based) dan pola transaksi memiliki keterbatasan dalam mendeteksi perilaku relasional pada kejahatan keuangan. Penelitian ini mengusulkan kerangka analitik graf terintegrasi untuk mendeteksi pola struktural pencucian uang dengan memanfaatkan metrik graf yang diintegrasikan ke dalam alur kerja (pipeline) jaringan saraf tiruan. Studi ini mengevaluasi metrik eksentrisitas, derajat (degree), kedekatan (closeness), serta arah aliran dana untuk membedakan aktivitas pencucian uang. Hasil uji Welch's t-test mengonfirmasi adanya perbedaan signifikan secara statistik pada lima dari enam metrik yang diuji ($p<0,001$). Selanjutnya, model Multi-Layer Perceptron (MLP) diterapkan untuk mengklasifikasikan 17 tipologi pencucian uang dengan tingkat akurasi mencapai 80%. Kontribusi utama penelitian ini membuktikan bahwa tipologi kejahatan keuangan dapat diekstraksi langsung dari topologi jaringan tanpa bergantung sepenuhnya pada fitur transaksi. Dengan menghubungkan metrik graf terhadap perilaku pencucian uang, termasuk pola *placement, layering*, dan *integration*. Penelitian ini menawarkan pendekatan deteksi AML berbasis jaringan yang skalabel. Penelitian mendatang disarankan untuk berfokus pada validasi data riil serta pengembangan alur klasifikasi waktu nyata (real-time) menggunakan inferensi jaringan saraf berbasis graf.

Dikirimkan: 15 Juli 2025
Diterima: 15 Desember 2025
Diterbitkan: 31 Desember 2025

***Untuk mensitasi artikel ini*:** Alham, L. G., Tsabitah, N., & Zaman, Y. M. N. 2025. *Deteksi Tipologi Pencucian Uang Berbasis Graph Analytics dan Neural Network. AML/CFT Journal: The Journal of Anti Money Laundering and Countering the Financing of Terrorism* 4(1):49-67, https://doi.org/10.59593/amlcft.2025.v4i1.269

Pendahuluan

Kejahatan keuangan dan pencucian uang terus menjadi ancaman serius terhadap integritas sistem keuangan global. Selain itu, pandemi COVID-19 semakin meningkatkan peluang

terjadinya angka kriminalitas melalui digitalisasi di saluran komunikasi dan pembayaran.[1] Hal ini signifikan terjadi di kawasan Asia-Pasifik (Asia-Pacific/APAC), di mana digitalisasi perekonomian terwujud melalui pertumbuhan *e-commerce* dan inovasi teknologi finansial (*financial technology/fintech*).[2] Kawasan ini dipandang sebagai *hotspot* aktivitas pencucian uang akibat pertumbuhan ekonomi yang pesat, sistem keuangan yang beragam, serta tingkat penegakan regulasi yang bervariasi. Oleh karena itu, upaya Anti-Pencucian Uang (*Anti-Money Laundering/AML*) di kawasan APAC perlu mempertimbangkan perilaku sosial kolektif dan strategi keuangan yang kompleks serta melampaui batas-batas yurisdiksi nasional.[3]

Menurut United Nations Office on Drugs and Crime,[4] sekitar 2–5% dari Produk Domestik Bruto (PDB) global mengalami pencucian dana setiap tahunnya, dengan nilai yang diperkirakan mencapai 1,7 triliun hingga 4,2 triliun dolar AS pada tahun 2020. Kawasan Asia Timur dan Asia Tenggara berkontribusi signifikan terhadap angka tersebut, terutama melalui penipuan (*scam*) dan kecurangan dalam ekosistem keuangan, dengan estimasi kerugian sebesar 18–37 miliar dolar AS.[5] Meskipun demikian, berkembangnya ekonomi digital justru memperparah risiko tersebut. Laporan lain[6] juga menyebutkan bahwa penipuan uang beserta aliran transaksi ilegal yang menyertainya, telah menyebar ke domain-domain terkait karena pengawasan yang tidak merata. Terlepas dari berbagai temuan tersebut, skala sebenarnya dari pencucian uang sangat mungkin masih *underreported*, khususnya di wilayah dengan tata kelola AML yang lebih longgar dan kapasitas penegakan hukum yang terbatas. Risiko pencucian uang yang relevan dengan isu yang dibahas dalam artikel ini meliputi: (1) penggunaan mata uang kripto dan platform aset terdesentralisasi yang memungkinkan transaksi anonim di tengah ketidakjelasan pengaturan;[7] (2) perjudian daring (*online gambling*) dan pemanfaatannya untuk pencucian uang melalui aset virtual;[8] (3) praktik pendirian badan usaha yang permisif, yang memfasilitasi pembentukan perusahaan cangkang (*shell companies*);[9] (4) penggunaan identitas

[1] APG, "About Anti-Money Laundering and Counter Terrorism Financing | Asia / Pacific Group On Money Laundering," last modified 2021, https://www.apgml.org/about-us/about-anti-money-laundering-and-counter-terrorism-financing.

[2] World Economic Forum, *Digital Transformation: Powering the Great Reset* (Switzerland: World Economic Forum, 2020).

[3] Jacopo Costa, "Research Case Study 3: Exposing the Networks behind Transnational Corruption and Money Laundering Schemes," Basel Institute on Governance, last modified May 31, 2023, https://baselgovernance.org/publications/research-case-3.

[4] APG, "About Anti-Money Laundering and Counter Terrorism Financing | Asia / Pacific Group On Money Laundering"; Ali Alkaabi et al., "A Comparative Analysis of the Extent of Money Laundering in Australia, UAE, UK and the USA," SSRN Scholarly Paper no. 1539843 (Rochester, NY: Social Science Research Network, 2010), https://doi.org/10.2139/ssrn.1539843.

[5] Sam Rogers, "Cyber-Fraud, Underground Banking, and Technological Innovation Fuels Crime in SE Asia," GASA, last modified December 17, 2024, https://www.gasa.org/post/unodc-cyber-fraud-underground-banking-and-technological-innovation-fuels-crime-in-se-asia; Dennis Miralis et al., *Anti-Money Laundering Laws and Regulations Anti-Money Laundering in the Asia-Pacific Region: An Overview 2025* (London: International Comparative Legal Guides (ICLG), 2025), United Kingdom.

[6] Katherine Cloud and Ilya Brovin, "How Identity Fraud Is Changing in the Age of AI," World Economic Forum, last modified December 11, 2025, https://www.weforum.org/stories/2025/12/how-identity-fraud-is-increasing-in-the-age-of-ai/.

[7] Jeffry Collins, "Cryptocurrencies and Financial Crimes: The Role of Decentralized Cryptocurrency in Facilitating Money Laundering and the Challenges Posed on Anti–Money Laundering Regulations," *University of Miami Business Law Review* 34, no. 1 (2025): 71; Chainalysis Team, "2023 Crypto Crime Trends: Illicit Cryptocurrency Volumes Reach All-Time Highs Amid Surge in Sanctions Designations and Hacking," Chainalysis, last modified January 12, 2023, https://www.chainalysis.com/blog/2025-crypto-crime-report-introduction/.

[8] UNODC, *The Nexus Between Cybercrime and Corruption* (Vienna: United Nations Office on Drugs and Crime, 2025).

[9] World Bank, "Corrupt Money Concealed in Shell Companies and Other Opaque Legal Entities, Finds New StAR Study," World Bank, last modified October 24, 2011, https://doi.org/10/24/corrupt-money-concealed-in-shell-companies-and-other-opaque-legal-entities-finds-new-star-study.

palsu dan/atau sintetis yang mampu menembus kelemahan mekanisme *Know Your Customer* (KYC) digital;[10] (5) penyalahgunaan celah pengaturan oleh *Politically Exposed Persons* (PEPs) untuk mencuci hasil kejahatan;[11] dan (6) skema berbasis perdagangan (*trade-based money laundering*) yang menyamarkan pergerakan aset hasil tindak pidana.[12]

Seiring dengan semakin kompleks dan canggihnya kejahatan keuangan dalam sistem keuangan yang secara inheren bersifat kompleks, metode deteksi dan pencegahan tradisional tidak lagi sepenuhnya memadai untuk mengidentifikasi aktivitas ilegal tersebut. Dalam beberapa tahun terakhir, teori graf dan analitik graf telah muncul sebagai instrumen yang kuat untuk menganalisis jaringan kompleks, termasuk jaringan yang terkait dengan kejahatan keuangan. Basis data graf dan model pembelajaran mesin berbasis graf memiliki kemampuan unik untuk memetakan serta menelaah hubungan antarentitas, sehingga sangat efektif dalam mengidentifikasi pola dan anomali dalam transaksi keuangan. Dengan memanfaatkan metrik graf seperti ukuran sentralitas (misalnya *degree centrality* dan *eigenvector centrality*) serta analitik berbasis graf, lembaga keuangan dapat mengungkap jaringan tersembunyi dan mendeteksi aktivitas mencurigakan yang mengindikasikan terjadinya pencucian uang.[13] Lebih lanjut, perkembangan dalam *graph neural networks* (GNNs) telah memungkinkan pembentukan *embedding* yang merepresentasikan topologi dan karakteristik simpul dalam suatu graf, sehingga secara signifikan meningkatkan kinerja deteksi dengan mengagregasikan jaringan transaksi ke dalam proses observasi.[14]

Namun demikian, masih terdapat sejumlah kesenjangan dalam penerapan teori graf dan pembelajaran mesin untuk deteksi fraud dan Anti-Pencucian Uang. Pertama, diperlukan dataset yang lebih komprehensif yang mampu merepresentasikan keberagaman dan kompleksitas tipologi pencucian uang. Kedua, aspek keterjelasan (*explainability*) dari model berbasis graf, khususnya GNN, masih menjadi tantangan, karena proses pengambilan keputusannya kerap bersifat tidak transparan (*opaque*). Terakhir, masih terbatasnya model prediktif yang mampu melakukan intersepsi terhadap entitas mencurigakan secara waktu nyata (*real-time*), padahal hal tersebut sangat krusial bagi upaya AML yang bersifat proaktif.

Artikel ini merespons kesenjangan tersebut dengan mengkaji tipologi dan skema pencucian uang melalui representasi berbasis graf dan klasifikasi menggunakan jaringan saraf. Penelitian ini mengidentifikasi dan menganalisis pola pencucian uang dengan memanfaatkan teori graf yang didukung oleh teknik kecerdasan buatan dan pembelajaran mesin (AI/ML), mengusulkan suatu kerangka analitis untuk mengevaluasi risiko AML dalam jaringan transaksi, serta mengembangkan model prediktif yang menilai apakah suatu segmen jaringan berpotensi merefleksikan aktivitas kejahatan keuangan.

Tinjauan Pustaka

Kejahatan keuangan dan pencucian uang telah muncul sebagai tantangan krusial terhadap stabilitas dan integritas perekonomian global. Namun demikian, implementasi kerangka regulasi AML menimbulkan tuntutan operasional yang signifikan bagi lembaga keuangan, sehingga mengharuskan adopsi langkah-langkah yang lebih maju untuk mendeteksi dan

[10] Tom Vidovic, "The Rise of the Synthetic Identity: A Growing Threat in the Digital Age," Global Compliance Institute, last modified July 5, 2024, https://www.gci-ccm.org/.

[11] Costa, "Research Case Study 3."

[12] FATF - Egmont Group, *FATF/Egmont Trade-Based Money Laundering: Trends and Developments* (Paris: FATF - Egmont Group, 2020).

[13] Milind Tiwari, Jamie Ferrill, and Vishal Mehrotra, "Using Graph Database Platforms to Fight Money Laundering: Advocating Large Scale Adoption," *Journal of Money Laundering Control* 26, no. 3 (2022): 474–87, https://doi.org/10.1108/JMLC-03-2022-0047.

[14] Dawei Cheng et al., "Anti-Money Laundering by Group-Aware Deep Graph Learning," *IEEE Transactions on Knowledge and Data Engineering* 35, no. 12 (2023): 12444–57, https://doi.org/10.1109/TKDE.2023.3272396.

mencegah aktivitas ilegal.[15] Pencucian uang kerap melibatkan sindikat yang terorganisasi secara kompleks, sering kali didukung oleh praktik koruptif aparat atau pejabat, dengan memanfaatkan strategi keuangan yang canggih untuk menyamarkan dana hasil kejahatan. Aktivitas tersebut umumnya bersifat lintas batas dan menggunakan transaksi yang kompleks guna mengaburkan asal-usul dana. Meskipun kesadaran terhadap permasalahan ini terus meningkat, hubungan antara korupsi dan pencucian uang masih belum dipahami secara memadai, khususnya dalam hal struktur, mekanisme, dan jaringan yang memfasilitasi terjadinya kejahatan tersebut.[16]

Upaya untuk meningkatkan akurasi deteksi telah mendorong penerapan teknik pembelajaran mesin (*machine learning*) yang dilatih menggunakan fitur-fitur transaksi, seperti nilai transaksi, frekuensi, dan waktu. Model-model ini terbukti efektif dalam mengidentifikasi perilaku yang tidak lazim dalam catatan transaksi,[17] namun pada umumnya berangkat dari asumsi bahwa setiap transaksi bersifat independen. Akibatnya, pendekatan tersebut memberikan pemahaman yang terbatas terhadap struktur relasional atau skema yang melibatkan banyak entitas, yang justru sering dimanfaatkan dalam tahapan *placement, layering*, dan *integration* sebagaimana diuraikan dalam tipologi AML.[18]

Penelitian terdahulu mengenai deteksi AML secara umum dapat dikelompokkan ke dalam tiga klaster utama: (i) pemantauan transaksi berbasis aturan (*rule-based transaction monitoring*), (ii) penerapan model *machine learning* dan *deep learning* yang dilatih menggunakan fitur-fitur transaksi,[19] dan (iii) pendekatan berbasis jaringan atau graf yang mengeksplorasi sifat relasional antarentitas.[20] Kelompok penelitian ini mencakup sejumlah survei dan tinjauan sistematis terbaru mengenai sistem AML dan analitik jaringan. Meningkatnya pengakuan terhadap keterbatasan pendekatan konvensional tersebut telah mendorong ketertarikan yang lebih besar terhadap pendekatan berbasis graf, yang memodelkan rekening atau entitas sebagai simpul (*nodes*) dan transaksi sebagai sisi (*edges*). Representasi ini memungkinkan analisis hubungan, pola aliran dana, serta struktur jaringan yang tidak dapat ditangkap hanya melalui atribut transaksi semata. Fondasi teori graf berakar dari karya Euler mengenai geometri sistem yang saling terhubung,[21] dan algoritma visualisasi graf modern telah mendukung interpretasi jaringan berskala besar di berbagai bidang.[22] Dalam penelitian AML, analitik graf telah digunakan untuk mengidentifikasi aktor sentral, perantara, serta pola perutean berlapis (*layered routing patterns*) dalam jaringan transaksi.[23]

Oleh karena itu, model berbasis graf semakin banyak diadopsi untuk memanfaatkan struktur relasional dari skema pencucian uang. Kontribusi penting dalam bidang ini mencakup kerangka pembelajaran graf yang skalabel untuk AML,[24] pendekatan *deep graph learning* yang

[15] Costa, "Research Case Study 3."
[16] Costa, "Research Case Study 3."
[17] Nazanin Bakhshinejad et al., "A Survey of Machine Learning Based Anti-Money Laundering Solutions," *Internet of Things—Applications and Future*, 2022, 73–87.
[18] Amel Muminovic and Festim Halili, "Money Laundering Prevention in the Digital Age: Leveraging Graph Databases for Effective Solutions," *Sciences (IJTNS)* 4, no. 1 (2024): 1–10.
[19] Bakhshinejad et al., "A Survey of Machine Learning Based Anti-Money Laundering Solutions."
[20] Ryan Weber et al., *A Spatial Analysis of City-Regions: Urban Form & Service Accessibility* (Stockholm: Nordregio, 2016); Bruno Deprez et al., "Network Analytics for Anti-Money Laundering—A Systematic Literature Review and Experimental Evaluation," *INFORMS Journal on Data Science* (2025), https://doi.org/10.1287/ijds.2024.0042.
[21] Leonhard Euler, "Solutio Problematis Ad Geometriam Situs Pertinentis," *Euler Archive - All Works* (1741): 128–40.
[22] Mathieu Jacomy et al., "ForceAtlas2, a Continuous Graph Layout Algorithm for Handy Network Visualization Designed for the Gephi Software," *PLoS One* 9, no. 6 (2014): e98679, https://doi.org/10.1371/journal.pone.0098679.
[23] Tiwari, Ferrill, and Mehrotra, "Using Graph Database Platforms to Fight Money Laundering."
[24] Weber et al., *A Spatial Analysis of City-Regions*.

peka terhadap tipologi (*typology-aware*),[25] serta model pengendalian fraud berbasis graf bagi lembaga keuangan.[26] Tinjauan sistematis oleh Deprez et al.[27] semakin menegaskan perkembangan tersebut dengan menyoroti perluasan metodologis analitik jaringan dalam konteks AML serta meningkatnya penekanan pada pemodelan relasional. Tabel 1 merangkum kerangka perbandingan berbagai pendekatan AML.

Tabel 1. Matriks Perbandingan Metodologi AML (berbagai sumber)

Pendekatan	Kelebihan	Keterbatasan	Studi Representatif	Keterkaitan dengan Studi Ini
Monitoring berbasis peraturan / scenario	Transparan; mudah diimplementasikan; selaras dengan model regulasi	Tingkat *false positive* yang tinggi; lemah dalam mendeteksi pencucian uang yang terstruktur atau melibatkan banyak entitas	FATF, panduan APG	Menegaskan kebutuhan akan metode analitik yang melampaui pendekatan ambang batas (*threshold-based*)
ML berbasis fitur transaksi	Mampu mempelajari pola non-linear; mengurangi beban penelaahan manual	Mengabaikan hubungan antarentitas; memiliki kapasitas terbatas dalam mendeteksi struktur jaringan	Bakhshinejad dkk. (2022)[28]	Mendukung penggunaan metrik graf relasional sebagai fitur pelengkap dalam analisis
Graph analytics (analisis struktural jaringan)	Mampu menangkap topologi jaringan; mengidentifikasi perantara, simpul pusat (*hubs*), dan motif pencucian uang	Cenderung bersifat deskriptif; pemetaan tipologi pencucian uang secara prediktif masih terbatas	Tiwari dkk. (2022);[29] Muminovic dan Halili (2024);[30] Oztas dkk. (2023)[31]	Penelitian ini menguji apakah metrik graf mampu membedakan tipologi pencucian uang secara signifikan secara statistik

[25] Cheng et al., "Anti-Money Laundering by Group-Aware Deep Graph Learning."
[26] Atif Usman, Nasir Naveed, and Saima Munawar, "Intelligent Anti-Money Laundering Fraud Control Using Graph-Based Machine Learning Model for the Financial Domain," *Journal of Cases on Information Technology (JCIT)* 25, no. 1 (2023): 1–20, https://doi.org/10.4018/JCIT.316665.
[27] Deprez et al., "Network Analytics for Anti-Money Laundering—A Systematic Literature Review and Experimental Evaluation."
[28] Bakhshinejad et al., "A Survey of Machine Learning Based Anti-Money Laundering Solutions."
[29] Tiwari, Ferrill, and Mehrotra, "Using Graph Database Platforms to Fight Money Laundering."
[30] Muminovic and Halili, "Money Laundering Prevention in the Digital Age."
[31] Berkan Oztas et al., "Enhancing Anti-Money Laundering: Development of a Synthetic Transaction Monitoring Dataset," *2023 IEEE International Conference on E-Business Engineering (ICEBE)*, November 2023, 47–54, https://doi.org/10.1109/ICEBE59045.2023.00028.

Pendekatan	Kelebihan	Keterbatasan	Studi Representatif	Keterkaitan dengan Studi Ini
Graph-based ML / GNN	Mampu mempelajari pola relasional secara langsung dari struktur graf	Biaya komputasi relatif tinggi; tingkat keterjelasan (*interpretability*) model lebih rendah	Weber dkk. (2018);[32] Cheng dkk. (2023);[33] Usman dkk. (2023);[34] Deprez dkk. (2025)[35]	Model MLP dipilih karena tingkat keterjelasan (*interpretability*) dan efisiensinya dalam mengolah metrik graf sintetis

GNN menawarkan kemampuan analisis jaringan yang kuat untuk data relasional dan telah digunakan secara luas dalam berbagai penelitian bertema AML,[36] Namun demikian, metode ini memerlukan sumber daya komputasi yang besar serta memiliki tingkat transparansi penalaran yang lebih rendah akibat karakteristiknya sebagai black box. Dalam penelitian ini, penulis memilih menggunakan model *Multilayer Perceptron* (MLP)[37] sebagai pendekatan analitis, karena MLP juga mampu menangkap hubungan nonlinier antarfitur, tetap efisien secara komputasional, serta memungkinkan atribusi pengaruh masing-masing metrik graf secara lebih jelas. Dengan demikian, MLP berfungsi sebagai alternatif metodologis yang tepat terhadap model berbasis graf yang secara inheren lebih kompleks.

Data dan Metodologi

Statistik Graf

Metrik graf seperti *eccentricity, centrality*, dan *degree* dapat digunakan untuk mengukur serta merepresentasikan perilaku suatu simpul (*node*) dalam graf, sekaligus menunjukkan tingkat signifikansi simpul tersebut dalam jaringan transaksi keuangan. Penelitian ini menggunakan ukuran sentralitas sebagaimana dikemukakan oleh Newman,[38] yang meliputi *betweenness, eigenvector, closeness*, dan *degree*. Secara rinci, statistik graf yang dianalisis dalam penelitian ini adalah sebagai berikut:

a. *Eccentricity*: Eksentrisitas didefinisikan sebagai jarak terpendek terpanjang dari suatu simpul ke simpul lainnya dalam jaringan. Metrik ini digunakan untuk mengidentifikasi aktor perifer (nilai eksentrisitas tinggi) yang cenderung "tersembunyi" dalam jaringan dan memiliki jarak yang tidak lazim dari entitas lain, seperti perusahaan cangkang dengan koneksi terbatas.
b. *Closeness Centrality*: Sentralitas kedekatan mengukur tingkat kedekatan relatif suatu simpul terhadap seluruh simpul lain dalam jaringan, berdasarkan rata-rata jarak terpendek. Simpul dengan nilai *closeness* tinggi umumnya berperan sebagai pusat jaringan (*central hub*),

[32] Weber et al., *A Spatial Analysis of City-Regions*.
[33] Cheng et al., "Anti-Money Laundering by Group-Aware Deep Graph Learning."
[34] Usman, Naveed, and Munawar, "Intelligent Anti-Money Laundering Fraud Control Using Graph-Based Machine Learning Model for the Financial Domain."
[35] Deprez et al., "Network Analytics for Anti-Money Laundering—A Systematic Literature Review and Experimental Evaluation."
[36] Cheng et al., "Anti-Money Laundering by Group-Aware Deep Graph Learning"; Usman, Naveed, and Munawar, "Intelligent Anti-Money Laundering Fraud Control Using Graph-Based Machine Learning Model for the Financial Domain."
[37] Marius-Constantin Popescu et al., "Multilayer Perceptron and Neural Networks," *WSEAS Transactions on Circuits and Systems* 8, no. 7 (2009): 579–88.
[38] Mark E. J. Newman, *Networks—An Introduction* (Oxford: Oxford University Press, 2012).

misalnya sebagai fasilitator pembayaran. Sebaliknya, nilai *closeness* yang rendah dapat mengindikasikan akun yang terisolasi, seperti money mules atau akun yang digunakan dalam tahapan *layering*.

c. *Harmonic Closeness Centrality*: varian dari *closeness centrality* yang memberikan bobot lebih besar pada simpul-simpul terdekat, sehingga lebih sesuai digunakan pada graf yang tidak sepenuhnya terhubung atau terdiri atas komunitas yang terpisah. Metrik ini efektif untuk mendeteksi perantara kunci (*key intermediaries*) meskipun jaringan bersifat terfragmentasi, suatu kondisi yang umum dijumpai dalam transaksi berlapis (*layered transactions*).
d. *Betweenness Centrality*: Sentralitas perantara mengukur seberapa sering suatu simpul berada pada jalur terpendek antara dua simpul lainnya. Metrik ini berfungsi untuk mengidentifikasi simpul-simpul strategis yang berperan sebagai titik penghubung atau titik kritis (*nexus/choke points*), seperti *money service businesses*, kasino, atau entitas penjaga gerbang (*gatekeepers*) yang memfasilitasi aliran dana. Nilai *betweenness* yang tinggi berpotensi mengindikasikan akun yang digunakan dalam proses *layering* atau *structuring*.
e. *Weighted Degree* (*in-degree* dan *out-degree*): mengukur jumlah total sisi masuk (*in-degree*) dan sisi keluar (*out-degree*) dari suatu simpul, dengan mempertimbangkan bobot transaksi. Metrik ini membantu mengidentifikasi simpul dengan aktivitas transaksi yang tidak wajar atau berintensitas tinggi, yang berpotensi terkait dengan aktivitas pencucian uang.

SAML-D Dataset

Dataset sintetis, seperti kerangka kerja SAML-D[39] memberikan sarana bagi peneliti untuk mempelajari berbagai tipologi pencucian uang. Dataset ini mengintegrasikan beragam fitur yang memungkinkan simulasi skenario pencucian uang yang kompleks. Tabel 2 menunjukkan bahwa dataset SAML-D dikembangkan berdasarkan informasi yang tersedia, kajian literatur akademik, serta wawancara dan laporan primer dari para spesialis AML. Dataset ini terdiri dari 9.504.852 transaksi, di mana 0,104% di antaranya diberi label sebagai aktivitas "mencurigakan".

Tabel 2. Fitur Dataset SAML-D

No.	Fitur	Deskripsi
1	*a.Time* *b.Date*	Esensial untuk melacak kronologi transaksi.
2	*a.Sender_Bank_Account* *b.Receiver_Bank_Account*	Membantu mengungkap pola perilaku dan hubungan perbankan yang kompleks. Berfungsi sebagai simpul (*nodes*) dalam pembentukan fungsi graf.
3	*Transaction_Amount*	Menunjukkan nilai transaksi untuk mengidentifikasi aktivitas yang mencurigakan.
4	*Payment_Type*	Mencakup berbagai metode pembayaran seperti kartu kredit, kartu debit, uang tunai, transfer ACH, lintas batas (*cross-border*), dan cek. Direpresentasikan sebagai label sisi (*edges*) dalam fungsi graf pada penelitian ini.
5	*a.Sender_bank_location*	Menunjukkan wilayah berisiko tinggi, termasuk Meksiko, Turki, Maroko, dan Uni Emirat Arab.

[39] Oztas et al., "Enhancing Anti-Money Laundering."

	b.Receiver_bank_location	
6	*a.Payment_Currency* *b.Received_Currency*	Selaras dengan fitur lokasi, serta menambah kompleksitas analisis apabila terjadi ketidaksesuaian mata uang.
7	*Is_Suspicious*	Indikator Boolean [0, 1] yang masing-masing merepresentasikan "tidak" dan "ya", untuk membedakan transaksi normal dan transaksi mencurigakan.
8	*Type*	Mengklasifikasikan metode dan tipologi pencucian uang sebagai berikut: a. *Smurfing*: Pemecahan dana dalam jumlah besar menjadi transaksi yang lebih kecil dan tampak kurang mencurigakan (misalnya setoran berulang di bawah ambang batas pelaporan). b. *Cash_Withdrawal*: Penarikan dana ilegal untuk kemudian dimasukkan kembali ke dalam sistem keuangan melalui saluran yang tampak sah. c. *Single_large*: Penempatan langsung satu transaksi besar (berisiko tetapi cepat). d. *Structuring*: Mirip dengan *smurfing* tetapi dilakukan dengan pola terstruktur (misalnya jumlah tetap dalam interval waktu tertentu). e. *Layered_Fan_In*: Dana dialirkan ke satu rekening pusat dari berbagai sumber (menyerupai pola "roda dengan jari-jari"). f. *Layered_Fan_Out*: Dana didistribusikan dari satu rekening pusat ke banyak tujuan akhir (kebalikan dari Fan_In). g. *Scatter-Gather*: Dana dipecah menjadi jumlah kecil, dialirkan melalui perantara, kemudian digabungkan kembali. h. *Gather-Scatter*: Kebalikan dari *Scatter-Gather*, yaitu dana digabung terlebih dahulu lalu dipecah kembali. i. *Cycle*: Transaksi melingkar antar rekening untuk menyamarkan asal dana (misalnya A → B → C → A). j. *Bipartite/Stacked Bipartite*: Dana bergerak antara dua kelompok rekening yang berbeda (misalnya perusahaan cangkang ↔ *money mules*). k. *Behavioural_Change*: Perubahan mendadak pola transaksi (misalnya rekening pasif tiba-tiba menjadi sangat aktif). l. *Over-Invoicing*: Penggelembungan nilai faktur perdagangan untuk melegitimasi dana ilegal. m. *Deposit-Send*: Menyetorkan dana "bersih" ke suatu rekening, kemudian mengirimkannya ke penerima manfaat akhir. n. *Fan_In/Fan_Out*: Agregasi akhir (*Fan_In*) atau distribusi

	akhir (*Fan_Out*) dana hasil pencucian uang agar tampak sah.

Sumber: Oztas et al.[40]

Kerangka analitis dan pemodelan

a. Akuisisi dan persiapan data. Pengumpulan data mentah dari repositori SAML-D. Tahapan ini mencakup pengumpulan data, pembersihan data, dan prapemrosesan untuk mentransformasikan data ke dalam format yang sesuai untuk analisis.
b. Rekayasa fitur (*feature engineering)*. Pemilihan, modifikasi, atau pembuatan fitur baru berdasarkan data yang telah diperoleh guna meningkatkan akurasi dan keterjelasan (*interpretability*) model.
c. Analisis graf dan algoritma tata letak (*layouting*). Penerapan teknik berbasis graf untuk memodelkan hubungan dan interaksi dalam data. Penelitian ini menggunakan algoritma tata letak Multigravity Force Atlas[41] yang diimplementasikan dalam perangkat lunak sumber terbuka Gephi untuk pemrosesan graf. Algoritma ini meningkatkan visualisasi jaringan dengan menerapkan gaya gravitasi yang dapat disesuaikan untuk memisahkan klaster, meminimalkan tumpang tindih antar simpul guna meningkatkan keterlihatan, serta memiliki kemampuan untuk menangani jaringan berskala besar.
d. Uji Statistik (*Welch's Paired T-Test*). Uji *paired t-test*[42] merupakan metode statistik untuk membandingkan nilai rata-rata dari dua kelompok sampel independen dan tidak mengasumsikan kesamaan varians, sehingga lebih sesuai digunakan untuk data dunia nyata di luar kondisi sampel yang terkontrol.
   Hipotesis yang diuji adalah sebagai berikut:

   1. Hipotesis Nol (H_0): $\mu_1 = \mu_2$ (rata-rata populasi statistik graf dari kedua kelompok adalah sama).
   2. Hipotesis Alternatif (H_1): $\mu_1 \neq \mu_2$ (dua arah) or $\mu_1 > \mu_2$ / $\mu_1 < \mu_2$ (satu arah), di mana karakteristik statistik graf tidak sama secara statistik.
      Dengan demikian, aturan pengambilan keputusan dapat dirumuskan sebagai berikut:

   Tolak H_0 apabila p-value < α (dengan $\alpha = 0.05$).

   Model yang dikembangkan pada tahap awal harus mampu membedakan ruang sampel, dengan s_1 merepresentasikan aktor yang melakukan fraud dan/atau pencucian uang, serta s_2 merepresentasikan aktor yang sah atau nasabah normal dari suatu platform keuangan.
e. Analisis heuristik. Melengkapi metode statistik berbasis graf dengan mengintegrasikan aturan berbasis domain dan indikator perilaku (*behavioral red flags*) untuk mengidentifikasi aktivitas yang mencurigakan.
f. Implementasi model: Untuk mengklasifikasikan transaksi yang berpotensi terkait dengan pencucian uang, penelitian ini mengimplementasikan model MLP menggunakan kerangka kerja PyTorch. Model dilatih menggunakan data transaksi yang telah diperkaya dengan fitur berbasis graf, termasuk ukuran sentralitas dan bobot sisi (*edge weight*). Arsitektur MLP terdiri atas beberapa lapisan tersembunyi dengan fungsi aktivasi ReLU dan lapisan keluaran dengan fungsi aktivasi *sigmoid* atau *softmax*, bergantung pada skema klasifikasi yang digunakan. Proses optimasi dilakukan dengan menggunakan *optimizer* Adam yang dikombinasikan dengan fungsi kerugian *binary cross-entropy*.

[40] Oztas et al., "Enhancing Anti-Money Laundering."
[41] Jacomy et al., "ForceAtlas2, a Continuous Graph Layout Algorithm for Handy Network Visualization Designed for the Gephi Software."
[42] B. L. Welch, "The Generalization of 'Student's' Problem When Several Different Population Varlances Are Involved," *Biometrika* 34, no. 1–2 (1947): 28–35, https://doi.org/10.1093/biomet/34.1-2.28.

g. Evaluasi & interpretasi: Model dievaluasi menggunakan metrik klasifikasi standar, termasuk *precision*, *recall*, dan *F1-score*. Hasil klasifikasi menunjukkan kemampuan model dalam mengidentifikasi pola-pola tipikal dari tipologi pencucian uang, seperti *layering* dan *smurfing*.

Hasil dan Pembahasan

Bagian ini menyajikan temuan analitis yang selaras dengan tiga tujuan utama penelitian, yaitu: (1) menguji apakah metrik graf menunjukkan perbedaan antara jaringan yang mengandung aktivitas fraud dan jaringan non-fraud, (2) menganalisis bagaimana tipologi pencucian uang direpresentasikan melalui topologi dan struktur jaringan, serta (3) mengevaluasi kinerja klasifikasi model MLP yang dilatih menggunakan fitur berbasis graf.

Analisis Statistik Graf pada Dua Ruang Sampel

Hasil analisis menunjukkan bahwa indikator yang diturunkan dari graf mampu menangkap perbedaan struktural antara segmen jaringan yang bersifat ilegal dan segmen jaringan normal, yaitu antara ruang sampel Fraud (s_1) dan Non-fraud (s_2). Temuan ini memberikan dukungan empiris terhadap hipotesis bahwa aktivitas pencucian uang menampilkan divergensi topologis yang dapat diukur secara kuantitatif.

1. Perbandingan statistik deskriptif

Tabel 3a dan 3b di bawah ini menyajikan hasil pengukuran statistik graf deskriptif dari ruang sampel $s_1 = s_2$. Analisis komparatif menunjukkan bahwa graf yang mengandung aktivitas fraud dan graf non-fraud menampilkan karakteristik yang berbeda dalam hal eksentrisitas kolektif, sentralitas, dan derajat (*degree*).

Tabel 3a. Statistik Graf Data Fraud

Metrik	Min.	Kuartil 1 (Q1)	Median	Rata-rata	Kuartil 3 (Q3)	Maks
Eksentrisitas (*Eccentricity*)	0.00	0.00	1.00	1.19	1.00	14.00
Sentralitas Kedekatan (*Closeness centrality*)	0.00	0.00	0.57	0.53	1.00	1.00
Sentralitas Kedekatan Harmonik (*Harmonic closeness centrality*)	0.00	0.00	0.63	0.55	1.00	1.00
Sentralitas Perantara (*Betweenness centrality*)	0.00	0.00	0.00	0.00	0.00	0.00
Derajat Masuk Berbobot (*Weighted Indegree)*	0.00	0.00	0.00	0.41	0.00	37.00
Derajat Keluar Berbobot (*Weighted Outdegree)*	0.00	0.00	0.00	0.41	0.00	37.00

Derajat Berbobot (*Weighted Degree*)	0.00	0.00	0.00	0.82	0.00	37.00

Tabel 3b. Statistik Graf Data Non-Fraud

Metrik	Min.	Kuartil 1 (Q1)	Median	Rata-rata	Kuartil 3 (Q3)	Maks
Eksentrisitas (*Eccentricity*)	0.00	0.00	0.00	0.17	0.00	2.00
Sentralitas Kedekatan (*Closeness centrality*)	0.00	0.00	0.00	0.17	0.00	1.00
Sentralitas Kedekatan Harmonik (*Harmonic closeness centrality*)	0.00	0.00	0.00	0.17	0.00	1.00
Sentralitas Perantara (*Betweenness centrality*)	0.00	0.00	0.00	0.01	0.00	15.00
Derajat Masuk Berbobot (*Weighted Indegree)*	0.00	1.00	1.00	2.62	3.00	24.00
Derajat Keluar Berbobot (*Weighted Outdegree)*	0.00	0.00	0.00	2.62	0.00	281.00
Derajat Berbobot (*Weighted Degree*)	1.00	1.00	2.00	5.24	4.00	281.00

Hasil uji t-test Welch

Tabel 4 menjelaskan hasil perhitungan uji dua sampel antara ruang sampel s_1: *fraud* dan s_2: *non-fraud*. Perbandingan antara dua populasi menggunakan uji Welch's t-test pada Tabel 4 mengonfirmasi adanya perbedaan yang signifikan secara statistik (di mana p-value < 0,05) pada lima dari enam metrik graf antara transaksi yang bersifat fraud dan non-fraud. Metrik eksentrisitas (t = 41,14) dan sentralitas kedekatan (*closeness centrality*) (t = 45,27) menunjukkan daya pembeda yang paling kuat, yang menegaskan kegunaannya dalam mengidentifikasi transaksi berlapis (*layered transactions*) dan simpul pusat (*central hubs*). Selanjutnya, metrik derajat berbobot (*weighted degree*)—baik *indegree* (t = -34,46) maupun outdegree (t = -9,67)—mampu membedakan secara jelas tahapan *placement* dan *integration* dalam skema pencucian uang. Sebaliknya, sentralitas perantara (*betweenness centrality*) tidak menunjukkan perbedaan yang signifikan secara statistik (p = 0,094), yang mengindikasikan keterbatasan perannya dalam mengisolasi perilaku yang secara spesifik berkaitan dengan pencucian uang. Secara keseluruhan, hasil ini menunjukkan bahwa indikator yang diturunkan dari graf mampu menangkap perbedaan struktural antara segmen jaringan yang bersifat ilegal dan segmen jaringan normal, sehingga memberikan dukungan empiris terhadap hipotesis bahwa aktivitas pencucian uang menampilkan divergensi topologis yang dapat diukur secara kuantitatif.

Tabel 4. Statistik uji t Welch dan corresponding p-value

No.	Variabel	*t-statistic*	*p-value*	Putusan
1	*Eccentricity*	41.1395	0.0000	Perbedaan signifikan
2	*Closeness centrality*	45.2665	0.0000	Perbedaan signifikan
3	*Betweenness centrality*	-1.6736	0.0943	Tidak terdapat perbedaan signifikan
4	*Weighted indegree*	-34.4598	0.0000	Perbedaan signifikan
5	*Weighted outdegree*	-9.6737	0.0000	Perbedaan signifikan
6	*Weighted Degree*	-19.2556	0.0000	Perbedaan signifikan

Tabel 5. Ringkasan Karakteristik Statistik Graf yang Dikelompokkan Berdasarkan Tipologi Pencucian Uang

No.	Topologi ML	*Eccentricity*		*Closeness centrality*		*Harmonic closeness centrality*		*Weighted indegree*		*Weighted outdegree*		*Weighted Degree*	
		mean	median	mean	Median	mean	median	mean	median	mean	median	mean	median
1	*Behavioural Change*	1.00	1.00	1.00	1.00	1.00	1.00	0.00	0.00	0.02	0.00	0.02	0.00
2	*Bipartite*	1.00	1.00	1.00	1.00	1.00	1.00	0.00	0.00	0.55	0.00	0.55	0.00
3	*Cash Withdrawal*	1.00	1.00	1.00	1.00	1.00	1.00	0.00	0.00	15.16	15.00	15.16	15.00
4	*Cycle*	9.75	10.00	0.21	0.18	0.32	0.29	0.99	1.00	1.00	1.00	1.99	2.00
5	*Deposit Send*	1.84	2.00	0.62	0.55	0.65	0.58	0.00	0.00	0.00	0.00	0.00	0.00
6	*Fan In*	1.00	1.00	1.00	1.00	1.00	1.00	0.00	0.00	0.02	0.00	0.02	0.00
7	*Fan Out*	1.00	1.00	1.00	1.00	1.00	1.00	0.00	0.00	0.00	0.00	0.00	0.00
8	*Gather Scatter*	1.81	2.00	0.64	0.56	0.67	0.60	0.00	0.00	0.01	0.00	0.01	0.00
9	*Layered Fan In*	1.63	2.00	0.82	0.75	0.87	0.83	0.20	0.00	0.25	0.00	0.45	0.00
10	*Layered Fan Out*	1.19	1.00	0.92	1.00	0.94	1.00	0.06	0.00	0.96	1.00	1.02	1.00
11	*Over Invoicing*	1.50	1.50	0.83	0.83	0.88	0.88	0.50	0.50	1.00	1.00	1.50	1.50
12	*Scatter Gather*	1.18	1.00	0.97	1.00	0.98	1.00	0.13	0.00	0.27	0.00	0.40	0.00
13	*Single large*	1.00	1.00	1.00	1.00	1.00	1.00	0.00	0.00	0.33	0.00	0.33	0.00
14	*Smurfing*	1.00	1.00	1.00	1.00	1.00	1.00	0.00	0.00	14.79	15.00	14.79	15.00
15	*Stacked Bipartite*	1.36	1.00	0.92	1.00	0.94	1.00	0.11	0.00	0.40	0.00	0.50	0.00
16	*Structuring*	1.00	1.00	1.00	1.00	1.00	1.00	0.00	0.00	0.00	0.00	0.00	0.00

Analisis Tipologi Pencucian Uang Menggunakan Metrik Graf

Pengukuran metrik graf terhadap tipologi pencucian uang sebagaimana ditampilkan dalam Tabel 5 menunjukkan adanya pola jaringan yang berbeda secara jelas di antara berbagai metode pencucian uang.

Observasi Kunci

a. Pola Transaksi
   Metode seperti *Cycle* dan *Deposit-Send* menunjukkan rantai transaksi yang memanjang (eksentrisitas tinggi) serta nilai sentralitas yang lebih rendah, yang mengindikasikan perilaku layering melalui beberapa tahapan. Sebaliknya, *Cash Withdrawal* dan *Smurfing* memperlihatkan pergerakan dana tunai yang terkonsentrasi (eksentrisitas rendah) namun dengan volume transaksi keluar yang tinggi.

b. Peran Jaringan

   Teknik seperti *Layered_Fan_Out* dan *Scatter-Gather* menempati posisi perantara dalam jaringan, dengan ukuran sentralitas yang relatif seimbang dan bobot transaksi yang moderat. Hal ini selaras dengan fungsinya sebagai mekanisme redistribusi dana dalam skema pencucian uang.

c. Karakteristik Pembeda

   Metode *Over-Invoicing* menonjol dengan bobot transaksi masuk dan keluar yang relatif seimbang, yang menunjukkan penggunaannya dalam manipulasi nilai secara sirkular. Sementara itu, *Behavioural_Change* dan *Fan_Out* cenderung muncul sebagai titik akhir dalam rantai pencucian uang, yang ditandai dengan aktivitas transaksi masuk yang minimal.

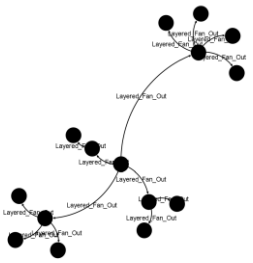
Interpretasi

Karakteristik metrik graf yang terukur tersebut berkorelasi dengan tipologi pencucian uang sebagai berikut:

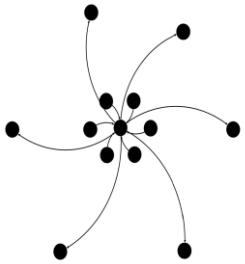
a. Tahap penempatan (*placement)* termanifestasi dalam bentuk volume transaksi keluar yang tinggi dari rekening atau sumber asal.
   Tipologi Placement (misalnya *Smurfing* dan *Cash Withdrawal*) menunjukkan nilai outdegree yang tinggi (rata-rata: 14,79–15,16) dan eksentrisitas yang rendah (1,0), yang mencerminkan pola penyebaran dana secara terkonsentrasi.

Gambar 1. Skema *Cash-withdrawal*

b. *Layering* tampak sebagai rantai transaksi yang kompleks untuk menyamarkan transaksi yang mendasarinya.
   Tipologi *Layering* (misalnya *Layered Fan-Out* dan *Deposit-Send*) menunjukkan jalur transaksi yang memanjang (eksentrisitas: 9,75) serta nilai sentralitas yang rendah, yang konsisten dengan strategi pengaburan (*obfuscation strategies*).



Gambar 2. Skema *Cycle*



Gambar 3. Skema *Deposit-Send*

c. Tahap Integrasi Akhir (*Integration*) muncul sebagai simpul terminal atau titik akhir dalam jaringan dengan aliran dana yang tidak seimbang.
Tipologi *Integration* (misalnya *Fan_Out* dan *Behavioural_Change*) dicirikan oleh nilai indegree yang minimal (0,0), yang menandai posisi sebagai titik akhir dalam rantai pencucian uang.

Gambar 4. Skema *Fan-out*

Konsistensi karakteristik dan pola graf pada berbagai tipologi di atas menunjukkan bahwa metrik graf dapat secara efektif menandai perilaku keuangan yang mencurigakan apabila dikalibrasi secara tepat. Dengan demikian, analisis ini memperlihatkan bahwa metrik graf seperti sentralitas dan tingkat keterhubungan (*degree of connectivity*) dapat dimanfaatkan untuk identifikasi pencucian uang yang melampaui sistem pemantauan berbasis aturan atau skenario yang bersifat statis.

Implementasi dan Evaluasi Model

Dalam penelitian ini, tugas klasifikasi diturunkan dari seperangkat atribut topologis, yaitu *betweenness centrality, degree centrality, in-degree*, dan *out-degree*, yang digunakan sebagai fitur masukan. Pendekatan ini memungkinkan penyederhanaan proses pembelajaran berbasis graf. Untuk melakukan klasifikasi, penelitian ini mengimplementasikan model jaringan saraf feedforward, yaitu *Multilayer Perceptron* (MLP), dengan menggunakan kerangka kerja deep learning PyTorch. Arsitektur model terdiri atas lapisan masukan yang sesuai dengan jumlah fitur yang diekstraksi, diikuti oleh satu lapisan tersembunyi, serta lapisan keluaran yang merepresentasikan label kelas. Pendekatan berbasis MLP ini memungkinkan model untuk mempelajari hubungan non-linear antara fitur-fitur yang diturunkan dari graf dan kelas simpul (*node classes*) dalam skema pembelajaran terawasi (*supervised learning*). Arsitektur model didefinisikan sebagai berikut:

```
class MLP(nn.Module):
    def __init__(self, input_dim, hidden_dim, output_dim):
    super(MLP, self).__init__()
    self.fc1 = nn.Linear(input_dim, hidden_dim)
```

```
        self.fc2 = nn.Linear(hidden_dim, output_dim)
    def forward(self, x):
        x = F.relu(self.fc1(x))
        return self.fc2(x)
```

Lapisan masukan (*input layer*) menerima fitur dengan dimensi *input_dim*, yang merepresentasikan jumlah fitur dalam dataset. Lapisan tersembunyi (*hidden layer*) terdiri atas *hidden_dim* neuron dan menggunakan fungsi aktivasi ReLU untuk memperkenalkan sifat non-linear dalam proses pembelajaran. Lapisan keluaran (*output layer*) terdiri atas *output_dim* neuron, yang merepresentasikan jumlah kelas target. Parameter model dioptimalkan menggunakan Adam Optimizer dengan *learning rate* sebesar 0,01. Fungsi kerugian *Cross-Entropy Loss* digunakan sebagai fungsi objektif karena kesesuaiannya untuk tugas klasifikasi multikelas. Konfigurasi pelatihan model ditetapkan sebagai berikut.

```
model = MLP(
  input_dim=X.shape[1],
  hidden_dim=64,
  output_dim=len(encoder.classes_)
      )
optimizer = torch.optim.Adam(model.parameters(), lr=0.01)
criterion = nn.CrossEntropyLoss()
```

Model MLP beroperasi sebagai jaringan saraf *feedforward* standar, di mana setiap lapisan terhubung sepenuhnya (*fully connected*) dengan lapisan berikutnya. Transformasi linear pertama memetakan fitur masukan ke dalam suatu representasi laten, yang kemudian diikuti oleh fungsi aktivasi ReLU untuk memungkinkan model mempelajari pola-pola kompleks yang bersifat non-linear. Lapisan linear kedua memproyeksikan representasi tersebut ke dalam ruang keluaran yang merepresentasikan probabilitas kelas. Arsitektur ini sesuai untuk permasalahan klasifikasi di mana hubungan antara fitur masukan dan kelas keluaran bersifat potensial non-linear dan berdimensi tinggi. Pemilihan algoritma optimasi Adam memungkinkan penyesuaian learning rate secara adaptif, sehingga meningkatkan kecepatan konvergensi dan stabilitas selama proses pelatihan. Dalam penelitian ini, model jaringan saraf MLP digunakan untuk mengklasifikasikan jenis pencucian uang. Model MLP diterapkan untuk mengklasifikasikan 17 kelas tipologi pencucian uang.

Tabel 6. Kinerja Prediktif MLP pada Tipologi Pencucian Uang

Kelas	Presisi	Recall	Skor F1
Behavioural_Change_1	0.41	0.75	0.53
Behavioural_Change_2	0.57	0.67	0.62
Bipartite	0.54	0.86	0.67
Cash_withdrawal	0.40	1.00	0.57
Cycle	1.00	0.98	0.99
Deposit-Send	0.53	0.90	0.67
Fan_In	0.35	0.30	0.32
Fan_Out	0.00	0.00	0.00
Gather-Scatter	1.00	0.03	0.06
Layered_Fan_In	0.91	0.65	0.76
Layered_Fan_Out	0.88	0.88	0.88
Over-Invoicing	1.00	0.50	0.67
Scatter-Gather	0.90	0.87	0.88
Single_Large	0.00	0.00	0.00
Smurfing	0.00	0.00	0.00
Stacked Bipartite	0.98	0.82	0.88
Structuring	1.00	0.99	0.99

Model MLP berbasis *deep learning* menunjukkan kinerja yang kuat dalam sejumlah kasus pendeteksian aktivitas pencucian uang serta klasifikasi transaksi mencurigakan, dengan tingkat akurasi dan nilai *F1-score* yang relatif tinggi. Hasil evaluasi menunjukkan bahwa *MLP Classifier* memiliki efektivitas keseluruhan yang baik dengan tingkat akurasi sebesar 80%. Namun demikian, beberapa tipologi seperti *Fan_Out, Gather-Scatter, Single_Large, Smurfing*, dan *Fan In* menunjukkan kinerja klasifikasi yang kurang optimal, yang dapat dikaitkan dengan ketidakseimbangan kelas (*class imbalance*) yang signifikan dalam dataset. Model mengalami kesulitan dalam mempelajari pola-pola pembeda yang khas untuk tipologi-tipologi yang jarang muncul tersebut. Selain itu, terdapat pula sejumlah tipologi yang berada dalam kategori kinerja menengah, di mana model mampu mengenali pola tertentu meskipun nilai *precision* yang dihasilkan masih belum konsisten. Di luar faktor ketidakseimbangan data, kesalahan klasifikasi pada beberapa tipologi juga dapat disebabkan oleh adanya kemiripan tersembunyi dalam pola perilaku atau struktur jaringan. Karena MLP mempelajari hubungan berdasarkan fitur masukan, karakteristik yang saling tumpang tindih antar tipologi dapat mengurangi kemampuan model dalam membedakannya secara tegas. Temuan ini mengindikasikan perlunya pengembangan fitur yang lebih terperinci atau penggunaan model pelengkap (*complementary models*) guna menangkap perbedaan yang lebih halus secara lebih efektif. Tipologi seperti *Behavioural_Change_1, Bipartite,* dan *Deposit_Send* menunjukkan bahwa meskipun model mampu mengidentifikasi sebagian karakteristiknya, peningkatan lebih lanjut masih diperlukan untuk mencapai tingkat precision yang lebih andal. Sebaliknya, terdapat pula kelas-kelas dengan kinerja yang kuat, yaitu *Structuring, Layered_Fan_Out*, dan *Scatter-Gather*, yang memiliki jumlah sampel relatif lebih besar serta menampilkan pola yang lebih mudah dikenali dan dipelajari oleh model, sehingga berkontribusi terhadap kinerja prediktif yang lebih tinggi.

Penelitian-penelitian terdahulu yang melibatkan penggunaan MLP pada umumnya berfokus pada fitur-fitur yang diturunkan secara langsung dari data transaksi, dengan sebagian

di antaranya mengintegrasikan *hyperparameter tuning* untuk meningkatkan efektivitas model.[43] Sebaliknya, penelitian ini menggabungkan variabel berbasis graf, seperti sentralitas simpul (*node centrality*) dan koefisien pengelompokan (*clustering coefficient*), guna merepresentasikan aspek struktural dan relasional dari jaringan transaksi. Dengan pendekatan tersebut, model mampu menangkap pola perilaku yang melampaui transaksi individual yang terisolasi, serta menghadirkan perspektif analisis pada tingkat jaringan secara keseluruhan (*network-wide perspective*), yang hingga saat ini masih relatif kurang dieksplorasi dalam penerapan MLP konvensional.

Kesimpulan

Analisis komparatif terhadap statistik deskriptif menunjukkan bahwa graf yang merepresentasikan transaksi fraud dan non-fraud memiliki karakteristik yang berbeda dalam hal eksentrisitas kolektif, sentralitas, dan derajat konektivitas. Uji t-test Welch memberikan dukungan empiris terhadap hipotesis bahwa aktivitas pencucian uang menampilkan perbedaan topologis yang dapat diukur secara kuantitatif. Analisis tipologi pencucian uang menggunakan metrik graf memperlihatkan bahwa metrik seperti sentralitas dan derajat konektivitas dapat dimanfaatkan untuk identifikasi pencucian uang melampaui sistem pemantauan statis berbasis aturan atau skenario. Karena model MLP dalam penelitian ini hanya bergantung pada fitur yang diturunkan dari graf, tipologi dengan karakteristik jaringan yang tidak tegas atau ambigu menjadi lebih sulit untuk diberi label. Meski demikian, temuan MLP menunjukkan bahwa metrik graf dapat diimplementasikan dalam model pembelajaran terawasi dan mampu mengklasifikasikan tipologi pencucian uang dengan kinerja yang baik pada baseline yang terkontrol.

Penelitian ini menunjukkan bahwa analisis berorientasi graf menyediakan sarana yang terstruktur untuk mengidentifikasi skema pencucian uang dalam jaringan transaksi keuangan. Dengan memanfaatkan metrik graf, temuan penelitian mengindikasikan bahwa eksentrisitas, *closeness, weighted indegree, weighted outdegree,* dan *weighted degree* dapat mengekstrapolasi tipologi pencucian uang, sekaligus menunjukkan nilai fitur struktural bagi deteksi AML. Hasil penelitian juga memberikan wawasan mengenai keterkaitan perilaku dalam konfigurasi jaringan. Pola seperti dispersi dana, konsolidasi, dan *multi-path layering* berkorespondensi dengan variasi topologi graf yang terukur, sehingga mendukung pandangan bahwa aliran dana ilegal menghasilkan *graph signature* yang khas.

Perlu dicatat pula bahwa data sintetis yang digunakan sebagai *baseline* pemodelan mungkin belum sepenuhnya merepresentasikan variabilitas yang dijumpai dalam skenario dunia nyata, sehingga membatasi penerapan hasil penelitian. Penelitian selanjutnya disarankan untuk memvalidasi temuan ini menggunakan dataset operasional, menelaah konteks lintas yurisdiksi, serta mengeksplorasi pendekatan hibrida yang mengombinasikan metrik graf dengan teknik lain, seperti model berbasis GNN atau *pipeline* deteksi waktu nyata. Dengan demikian, eksperimen lanjutan perlu disesuaikan dengan data dunia nyata untuk mengakomodasi berbagai variasi kondisi. Salah satu keterbatasan model saat ini adalah kemampuannya yang terbatas dalam membedakan tipologi yang memiliki pola dasar yang serupa.

Mengingat MLP merupakan model *feedforward* yang bergantung pada keterpisahan fitur masukan, model ini dapat mengalami kesulitan ketika tipologi yang berbeda memiliki karakteristik perilaku yang tersembunyi atau saling tumpang tindih. Keterbatasan ini menyoroti perlunya representasi fitur yang lebih ekspresif atau pendekatan pemodelan alternatif yang mampu menangkap perbedaan halus di antara pola pencucian uang yang berdekatan.

[43] Hitarth Gandhi et al., "Navigating the Complexity of Money Laundering: Anti–Money Laundering Advancements with AI/ML Insights," *International Journal on Smart Sensing and Intelligent Systems* 17, no. 1 (2024): 1–29, https://doi.org/10.2478/ijssis-2024-0024.

Secara keseluruhan, artikel ini memberikan landasan bagi pengembangan penerapan teori graf dalam praktik industri AML serta menegaskan potensi struktur jaringan sebagai tuas analitis untuk mendeteksi aktivitas pencucian uang dalam ekosistem keuangan yang terdigitalisasi.

Daftar Pustaka

Alkaabi, Ali, George Mohay, Adrian McCullagh, and Nicholas Chantler. "A Comparative Analysis of the Extent of Money Laundering in Australia, UAE, UK and the USA." SSRN Scholarly Paper No. 1539843. Rochester, NY: Social Science Research Network, 2010. https://doi.org/10.2139/ssrn.1539843.

APG. "About Anti-Money Laundering and Counter Terrorism Financing | Asia / Pacific Group On Money Laundering." Last modified 2021. https://www.apgml.org/about-us/about-anti-money-laundering-and-counter-terrorism-financing.

Bakhshinejad, Nazanin, Reza Soltani, U. Nguyen, and Paul Messina. "A Survey of Machine Learning Based Anti-Money Laundering Solutions." *Internet of Things—Applications and Future* (2022): 73–87.

Chainalysis Team. "2023 Crypto Crime Trends: Illicit Cryptocurrency Volumes Reach All-Time Highs Amid Surge in Sanctions Designations and Hacking." Chainalysis. Last modified January 12, 2023. https://www.chainalysis.com/blog/2025-crypto-crime-report-introduction/.

Cheng, Dawei, Yujia Ye, Sheng Xiang, Zhenwei Ma, Ying Zhang, and Changjun Jiang. "Anti-Money Laundering by Group-Aware Deep Graph Learning." *IEEE Transactions on Knowledge and Data Engineering* 35, no. 12 (2023): 12444–57. https://doi.org/10.1109/TKDE.2023.3272396.

Cloud, Katherine, and Ilya Brovin. "How Identity Fraud Is Changing in the Age of AI." World Economic Forum. Last modified December 11, 2025. https://www.weforum.org/stories/2025/12/how-identity-fraud-is-increasing-in-the-age-of-ai/.

Collins, Jeffry. "Cryptocurrencies and Financial Crimes: The Role of Decentralized Cryptocurrency in Facilitating Money Laundering and the Challenges Posed on Anti–Money Laundering Regulations." *University of Miami Business Law Review* 34, no. 1 (2025): 71.

Costa, Jacopo. "Research Case Study 3: Exposing the Networks behind Transnational Corruption and Money Laundering Schemes." Basel Institute on Governance. Last modified May 31, 2023. https://baselgovernance.org/publications/research-case-3.

Deprez, Bruno, Toon Vanderschueren, Bart Baesens, Tim Verdonck, and Wouter Verbeke. "Network Analytics for Anti-Money Laundering—A Systematic Literature Review and Experimental Evaluation." *INFORMS Journal on Data Science* (2025), https://doi.org/10.1287/ijds.2024.0042.

Euler, Leonhard. "Solutio Problematis Ad Geometriam Situs Pertinentis." *Euler Archive - All Works* (1741): 128–40.

FATF - Egmont Group. *FATF/Egmont Trade-Based Money Laundering: Trends and Developments*. Paris: FATF - Egmont Group, 2020.

Gandhi, Hitarth, Kevin Tandon, Shilpa Gite, Biswajeet Pradhan, and Abdullah Alamri. "Navigating the Complexity of Money Laundering: Anti–Money Laundering Advancements with AI/ML Insights." *International Journal on Smart Sensing and Intelligent Systems* 17, no. 1 (2024): 1–29. https://doi.org/10.2478/ijssis-2024-0024.

Jacomy, Mathieu, Tommaso Venturini, Sebastien Heymann, and Mathieu Bastian. "ForceAtlas2, a Continuous Graph Layout Algorithm for Handy Network Visualization Designed for the Gephi Software." *PLoS One* 9, no. 6 (2014): e98679. https://doi.org/10.1371/journal.pone.0098679.

Miralis, Dennis, Harry Sultan, Henry Yu, and Zanthi Jordan. *Anti-Money Laundering Laws and Regulations Anti-Money Laundering in the Asia-Pacific Region: An Overview 2025*. London: International Comparative Legal Guides (ICLG), 2025.

Muminovic, Amel, and Festim Halili. "Money Laundering Prevention in the Digital Age: Leveraging Graph Databases for Effective Solutions." *Sciences (IJTNS)* 4, no. 1 (2024): 1–10.

Newman, Mark E. J. *Networks—An Introduction*. Oxford: Oxford University Press, 2012.

Oztas, Berkan, Deniz Cetinkaya, Festus Adedoyin, Marcin Budka, Huseyin Dogan, and Gokhan Aksu. "Enhancing Anti-Money Laundering: Development of a Synthetic Transaction Monitoring Dataset." *2023 IEEE International Conference on E-Business Engineering (ICEBE)*, November 2023, 47–54. https://doi.org/10.1109/ICEBE59045.2023.00028.

Popescu, Marius-Constantin, Valentina E. Balas, Liliana Perescu-Popescu, and Nikos Mastorakis. "Multilayer Perceptron and Neural Networks." *WSEAS Transactions on Circuits and Systems* 8, no. 7 (2009): 579–88.

Rogers, Sam. "Cyber-Fraud, Underground Banking, and Technological Innovation Fuels Crime in SE Asia." GASA. Last modified December 17, 2024. https://www.gasa.org/post/unodc-cyber-fraud-underground-banking-and-technological-innovation-fuels-crime-in-se-asia.

Tiwari, Milind, Jamie Ferrill, and Vishal Mehrotra. "Using Graph Database Platforms to Fight Money Laundering: Advocating Large Scale Adoption." *Journal of Money Laundering Control* 26, no. 3 (2022): 474–87. https://doi.org/10.1108/JMLC-03-2022-0047.

UNODC. *The Nexus Between Cybercrime and Corruption*. Vienna: United Nations Office on Drugs and Crime, 2025.

Usman, Atif, Nasir Naveed, and Saima Munawar. "Intelligent Anti-Money Laundering Fraud Control Using Graph-Based Machine Learning Model for the Financial Domain." *Journal of Cases on Information Technology (JCIT)* 25, no. 1 (2023): 1–20. https://doi.org/10.4018/JCIT.316665.

Vidovic, Tom. "The Rise of the Synthetic Identity: A Growing Threat in the Digital Age." Global Compliance Institute. Last modified July 5, 2024. https://www.gci-ccm.org/.

Weber, Ryan, Iilpo Tammi, Shinan Wang, and Timothy Anderson. *A Spatial Analysis of City-Regions: Urban Form & Service Accessibility*. Stockholm: Nordregio, 2016.

Welch, B. L. "The Generalization of 'Student's' Problem When Several Different Population Varlances Are Involved." *Biometrika* 34, no. 1–2 (1947): 28–35. https://doi.org/10.1093/biomet/34.1-2.28.

World Bank. "Corrupt Money Concealed in Shell Companies and Other Opaque Legal Entities, Finds New StAR Study." World Bank. Last modified October 24, 2011. https://doi.org/10/24/corrupt-money-concealed-in-shell-companies-and-other-opaque-legal-entities-finds-new-star-study.

World Economic Forum. *Digital Transformation: Powering the Great Reset*. Switzerland: World Economic Forum, 2020.