Journal of Information Technology and Computer Science (INTECOMS)
Volume 9 Nomor 1, Tahun 2026
e-ISSN : 2614-1574
p-ISSN : 2621-3249

ANALISIS SISTEM DETEKSI DINI FRAUD PADA TRANSAKSI PERBANKAN MENGGUNAKAN LONG SHORT-TERM MEMORY (LSTM) DAN TRANSFORMER

ANALYSIS OF EARLY FRAUD DETECTION SYSTEMS IN BANKING TRANSACTIONS USING LONG SHORT-TERM MEMORY (LSTM) AND TRANSFORMER

Arken Abdullah[1], Arya Adhyaksa Waskita[2], Murni Handayani[3]
Universitas Pamulang, Tangerang Selatan, Banten[1,2,3]
arken.abdullah@yahoo.com[1]

ABSTRACT

The increasing use of digital payment channels such as QRIS, BI-Fast, and online transfers has significantly increased the volume of digital banking transactions, thereby elevating the risk of fraud. In addition, the imbalanced nature of transaction data further increases the complexity of fraud detection. This study aims to design an adaptive early fraud detection model based on deep learning, analyze the performance of Long Short-Term Memory (LSTM) and Transformer models. The data were processed through data cleansing, behavioral feature aggregation, and clustering based on historical transaction characteristics. Fraud modeling was then performed separately for each cluster using LSTM and Transformer models. The results indicate that the Transformer model outperformed LSTM in two clusters. In the first cluster, the PR-AUC was 0.773 with a precision of 0.826, and in the second cluster, the PR-AUC reached 0.877 with a precision of 0.826. Meanwhile, LSTM achieved the best performance in one cluster with a PR-AUC of 0.901 and a precision of 0.954. These findings demonstrate that Transformer provides superior overall performance in detecting fraud in digital banking transactions. Future research is recommended to incorporate additional behavioral fraud parameters, explore alternative modeling architectures beyond LSTM and Transformer, and evaluate other models to further enhance system adaptability and performance.

***Keywords**: Fraud Detection, Deep Learning, LSTM, Transformer, Bank*

ABSTRAK

Peningkatan penggunaan kanal pembayaran digital seperti QRIS, BI-Fast, dan transfer online telah secara signifikan meningkatkan volume transaksi perbankan digital, sehingga turut meningkatkan risiko terjadinya fraud. Selain itu, sifat data transaksi yang tidak seimbang semakin menambah kompleksitas dalam proses deteksi fraud. Penelitian ini bertujuan untuk merancang model deteksi dini fraud yang adaptif berbasis deep learning serta menganalisis kinerja model Long Short-Term Memory (LSTM) dan Transformer. Data diproses melalui tahapan pembersihan data, agregasi fitur perilaku, serta pengelompokan (clustering) berdasarkan karakteristik historis transaksi. Pemodelan fraud kemudian dilakukan secara terpisah pada setiap cluster menggunakan model LSTM dan Transformer. Hasil penelitian menunjukkan bahwa model Transformer mengungguli LSTM pada dua cluster. Pada cluster pertama, nilai PR-AUC mencapai 0,773 dengan precision sebesar 0,826, dan pada cluster kedua, PR-AUC mencapai 0,877 dengan precision sebesar 0,826. Sementara itu, model LSTM menunjukkan kinerja terbaik pada satu cluster dengan PR-AUC sebesar 0,901 dan precision sebesar 0,954. Temuan ini menunjukkan bahwa Transformer memberikan performa yang lebih unggul secara keseluruhan dalam mendeteksi fraud pada transaksi perbankan digital. Penelitian selanjutnya disarankan untuk menambahkan parameter perilaku fraud yang lebih beragam, mengeksplorasi arsitektur pemodelan lain di luar LSTM dan Transformer, serta mengevaluasi model-model alternatif guna meningkatkan adaptabilitas dan kinerja sistem secara lebih optimal.

Kata Kunci: Fraud Detection, Deep Learning, LSTM, Transformer, Bank

PENDAHULUAN

Perkembangan layanan perbankan digital telah meningkatkan kemudahan dan efisiensi transaksi keuangan, namun juga diiringi dengan meningkatnya risiko terjadinya fraud transaksi. Pola fraud pada transaksi digital bersifat dinamis dan terus berkembang, sehingga menyulitkan proses deteksi secara dini apabila hanya mengandalkan pendekatan konvensional yang bersifat statis.

Meskipun berbagai penelitian sebelumnya telah menerapkan model deep learning untuk deteksi fraud dan menunjukkan tingkat akurasi yang tinggi, sebagian besar pendekatan tersebut masih menggunakan satu model global tanpa mempertimbangkan perbedaan karakteristik perilaku antar nasabah. Pendekatan model tunggal ini berpotensi mengurangi sensitivitas dalam mengenali pola fraud yang bersifat heterogen dan dinamis, terutama pada lingkungan transaksi digital perbankan yang memiliki variasi perilaku nasabah yang signifikan.

Berdasarkan permasalahan tersebut, penelitian ini mengembangkan pendekatan deteksi dini fraud dengan mengadopsi pemodelan deep learning yang telah banyak digunakan pada penelitian sebelumnya, kemudian memperluasnya melalui mekanisme pengelompokan nasabah berdasarkan karakteristik perilaku historis transaksinya. Pemodelan fraud dilakukan secara spesifik pada setiap kelompok perilaku menggunakan model LSTM dan Transformer, sehingga proses pembelajaran menjadi lebih kontekstual dan adaptif terhadap karakteristik transaksi pada masing-masing klaster.

TINJAUAN PUSTAKA

Penelitian terkait deteksi fraud dalam sistem keuangan menunjukkan bahwa pendekatan berbasis deep learning, khususnya Long Short-Term Memory (LSTM), mampu memberikan kinerja yang relatif unggul dalam memodelkan pola transaksi yang bersifat kompleks dan temporal. Mahmud (2024) membuktikan bahwa LSTM mencapai akurasi hingga 98,5% dengan nilai AUC sebesar 0,94, mengungguli metode Logistic Regression dan Random Forest dalam mendeteksi transaksi fraud. Hasil serupa juga dilaporkan oleh Ghrib et al. (2024) melalui penerapan model ensembel BiLSTM-BiGRU yang dikombinasikan dengan SMOTE, yang menunjukkan performa stabil pada berbagai metrik evaluasi dalam kondisi data tidak seimbang.

Pengembangan lanjutan terhadap arsitektur LSTM menunjukkan peningkatan performa yang signifikan. Model X-LSTM berbasis Explainable AI mencatat akurasi hingga 99,8% dan menegaskan peran penting data sintetis dalam meningkatkan kinerja LSTM, dengan peningkatan deteksi fraud hingga 50% (Mahmud, 2024). Selain itu, Hasugian dan Suharjito (2023) menekankan kestabilan LSTM dalam memproses transaksi antarbank, sementara Jain et al. (2023) menunjukkan bahwa teknik preprocessing seperti SMOTE mampu meningkatkan performa model RNN dan GBoost meskipun tidak secara langsung berbasis LSTM. Studi lain juga mencatat efektivitas LSTM pada domain laporan keuangan dengan akurasi sebesar 95,6% (Prabha & Priscilla, 2024), serta kombinasi LSTM-XGBoost dengan optimasi AdaBound yang menunjukkan kinerja unggul dalam klasifikasi risiko kredit (Fan et al., 2024). Selain itu, Meng et al. (2023) melaporkan bahwa ensembel LSTM dengan SMOTE-ENN mampu mencapai sensitivitas sebesar 98,85%.

Meskipun LSTM terbukti andal, keterbatasan dalam efisiensi komputasi dan ketergantungan pada urutan waktu mendorong berkembangnya Transformer sebagai alternatif yang lebih fleksibel. Transformer memanfaatkan mekanisme self-attention untuk memahami hubungan antar fitur tanpa ketergantungan eksplisit pada urutan sekuensial. Xiu (2025) menunjukkan bahwa Transformer mampu memberikan performa yang lebih unggul dibandingkan pendekatan konvensional dalam deteksi fraud transaksi finansial. Model BankSafeNet yang mengombinasikan dual autoencoder dengan Transformer juga mencatat precision sebesar 99,54% dan recall sebesar 99,37%, membuktikan efektivitasnya dalam aplikasi nyata (Ayyadurai et al., 2025). Selain itu, Transformer terbukti mampu menangani data tidak seimbang secara efisien dan mencapai nilai recall

yang tinggi pada kelas minoritas (Reddy Polu, 2023).

Ulasan sistematis oleh Chen et al. (2025) menyoroti tren peningkatan adopsi Transformer sejak tahun 2022 dalam domain deteksi fraud. Transformer juga berperan penting dalam proses feature extraction, terutama dalam menangani distribusi data non-linear (Pushpakumar R, 2025), serta menunjukkan efisiensi parameter yang lebih baik dibandingkan LSTM pada data finansial terstruktur (Huang & B, 2023). Kombinasi Transformer dengan Variational Autoencoder (VAE) bahkan mampu mencapai precision sebesar 99,39%, recall sebesar 99,55%, dan false positive rate hanya 0,599%, menjadikannya solusi yang efektif dalam mendeteksi pola anomali yang kompleks (Pushpakumar R, 2025). Secara keseluruhan, penelitian-penelitian tersebut menunjukkan perkembangan signifikan dalam penerapan LSTM dan Transformer untuk deteksi fraud, sehingga membuka peluang bagi pendekatan hibrida yang mengombinasikan keunggulan kedua model.

METODE

a. Analisis Kebutuhan

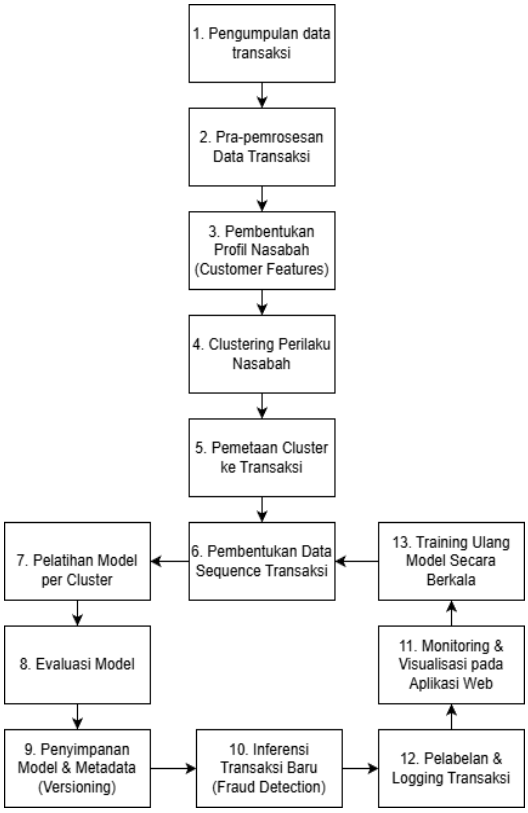
Penelitian ini dilakukan pada sebuah institusi perbankan swasta di Indonesia. Fokus penelitian diarahkan pada kebutuhan pengembangan sistem deteksi dini fraud pada transaksi BI-Fast, QRIS, dan transfer online. Kebutuhan tersebut dilatarbelakangi oleh keterbatasan Fraud Detection System (FDS) yang masih berbasis aturan statis (rule-based), sehingga kurang adaptif dalam mendeteksi pola fraud baru yang bersifat kompleks dan dinamis. Oleh karena itu, diperlukan pendekatan berbasis deep learning, khususnya menggunakan model Long Short-Term Memory (LSTM) dan Transformer, yang diharapkan mampu meningkatkan akurasi serta adaptivitas sistem dalam mendeteksi potensi fraud transaksi perbankan.

b. Sumber Data

Populasi penelitian mencakup seluruh transaksi e-banking, khususnya transaksi BI-Fast, QRIS, dan transfer online pada kanal internet banking dan mobile banking selama periode satu tahun terakhir, dengan jumlah sekitar 300.000 transaksi. Penentuan ukuran sampel mengacu pada teori Cochran (1977), dengan tingkat kepercayaan 95% dan margin of error 1–2%, yang menghasilkan kebutuhan minimal sampel antara 2.400 hingga 9.300 transaksi. Namun, dalam konteks pemodelan deep learning, penggunaan data dalam jumlah besar sangat dianjurkan untuk mencegah overfitting dan meningkatkan kemampuan generalisasi model. Oleh karena itu, penelitian ini menggunakan seluruh data transaksi yang tersedia. Pembagian data dilakukan menggunakan pendekatan time-aware split, dengan 80% data awal digunakan sebagai data pelatihan dan 20% data pada periode waktu selanjutnya digunakan sebagai data pengujian.

c. Perancangan Penelitian

Alur penelitian dan tahapan sistem deteksi dini fraud yang dikembangkan dalam penelitian ini disajikan pada gambar dibawah ini, yang menggambarkan proses mulai dari pengolahan data transaksi hingga inferensi dan pembaruan model secara berkala.



Gambar 1. Alur Proses Penelitian

Perancangan penelitian ini mencakup keseluruhan alur sistem deteksi dini fraud yang dimulai dari pengumpulan data transaksi historis pada kanal e-banking hingga tahap pembentukan data berurutan. Data transaksi yang dikumpulkan terlebih dahulu melalui tahap pra-pemrosesan untuk memastikan kualitas data, meliputi pembersihan nilai tidak valid, normalisasi format waktu, dan standarisasi atribut numerik. Selanjutnya, dilakukan ekstraksi fitur untuk membentuk profil perilaku nasabah yang merepresentasikan karakteristik statistik dan temporal transaksi. Profil perilaku tersebut kemudian dikelompokkan melalui proses clustering untuk mengidentifikasi segmentasi perilaku nasabah yang serupa. Hasil clustering dipetakan kembali ke setiap transaksi sehingga informasi perilaku terintegrasi pada data transaksi. Data transaksi yang telah berlabel cluster selanjutnya disusun menjadi data berurutan (sequence) berbasis waktu menggunakan pendekatan sliding window guna menangkap pola temporal transaksi.

Tahap selanjutnya mencakup proses pemodelan, evaluasi, dan implementasi sistem deteksi fraud. Pelatihan model dilakukan secara terpisah pada setiap cluster menggunakan model Long Short-Term Memory (LSTM) dan Transformer agar model dapat mempelajari pola transaksi yang lebih spesifik. Model yang telah dilatih kemudian dievaluasi menggunakan metrik klasifikasi untuk menilai kemampuan deteksi fraud. Seluruh model beserta metadata pendukung disimpan dalam sistem versioning untuk mendukung pengelolaan model. Pada tahap operasional, transaksi baru dianalisis melalui proses inferensi untuk menghasilkan skor risiko fraud yang ditampilkan melalui aplikasi web. Hasil inferensi dicatat dalam sistem logging dan dimanfaatkan sebagai umpan balik untuk pelatihan ulang model secara berkala, sehingga sistem tetap adaptif terhadap perubahan pola transaksi nasabah.

d. Teknik Analisis

Analisis dilakukan menggunakan pendekatan klasifikasi terawasi (supervised learning), di mana setiap transaksi diberi label fraud atau non-fraud. Evaluasi model dilakukan secara terpisah untuk setiap cluster nasabah guna menangkap perbedaan karakteristik perilaku transaksi. Dasar evaluasi menggunakan confusion matrix yang terdiri dari true positive, true negative, false positive, dan false negative. Berdasarkan matriks tersebut dihitung metrik precision, recall, dan F1-score untuk mengukur keseimbangan antara kemampuan model dalam mendeteksi transaksi fraud dan meminimalkan kesalahan klasifikasi. Selain itu, digunakan metrik Area Under Receiver Operating Characteristic Curve (ROC-AUC) dan Area Under Precision–Recall Curve (PR-AUC). PR-AUC digunakan sebagai metrik utama karena

lebih representatif pada data dengan ketidakseimbangan kelas yang signifikan. Penentuan ambang batas klasifikasi dilakukan secara adaptif berdasarkan nilai F1-score maksimum pada data validasi. Seluruh metrik evaluasi dan threshold optimal disimpan dalam basis data untuk mendukung audit, replikasi eksperimen, dan analisis lanjutan.

HASIL DAN PEMBAHASAN

a. Hasil Pemodelan

Pengujian model LSTM dan Transformer dilakukan melalui variasi parameter epoch dan panjang sequence untuk mengevaluasi pengaruh kedalaman pembelajaran dan konteks historis transaksi terhadap kinerja deteksi fraud. Panjang sequence divariasikan dari 20 hingga 50 transaksi untuk merepresentasikan konteks historis pendek hingga panjang, sementara jumlah epoch ditingkatkan secara bertahap dalam rentang 5 hingga 30 guna memastikan proses pembelajaran model berlangsung optimal.

Untuk menganalisis dampak ketidakseimbangan data terhadap kinerja model, penelitian ini mengevaluasi dua skenario pelatihan, yaitu tanpa oversampling dan dengan oversampling menggunakan Synthetic Minority Over-sampling Technique (SMOTE). SMOTE digunakan sebagai skenario pembanding.

Tabel 1. Ringkasan Metrik Evaluasi Model LSTM Dengan SMOTE

Ep	Seq	Cls	PR-AUC	ROC-AUC	Prec	Rec	F1
5	20	0	0,6136	0,9971	0,7045	0,4921	0,5794
		1	0,5132	0,9960	0,5763	0,6182	0,5965
		2	0,8685	0,9986	0,8953	0,6875	0,7778
10	30	0	0,5873	0,9618	0,7556	0,5667	0,6476
		1	0,4370	0,9667	0,5294	0,7200	0,6102
		2	0,7810	0,9981	0,8152	0,7353	0,7732
15	40	0	0,477	0,972	0,618	0,607	0,613
		1	0,499	0,936	0,636	0,622	0,629
		2	0,670	0,990	0,773	0,739	0,756
20	50	0	0,446	0,956	0,622	0,571	0,596
		1	0,484	0,925	0,708	0,459	0,557
		2	0,738	0,985	0,800	0,753	0,776
30	50	0	0,413	0,979	0,592	0,592	0,592
		1	0,538	0,948	0,789	0,405	0,536
		2	0,734	0,989	0,775	0,729	0,752

Ep = Epoch, **Seq** = Sequence Length, **Cls** = Cluster, **Prec** = Precision, **Rec** = Recall, **F1** = F1-Score

Tabel 2. Ringkasan Metrik Evaluasi Model LSTM Tanpa SMOTE

Ep	Seq	Cls	PR-AUC	ROC-AUC	Prec	Rec	F1-Score
5	20	0	0,7943	0,9991	0,8511	0,6349	0,7273
		1	0,7400	0,9988	0,7778	0,6364	0,7000
		2	0,9112	0,9989	0,9630	0,6964	0,8083
10	30	0	0,7461	0,9990	0,8919	0,5500	0,6804
		1	0,6255	0,9986	0,7073	0,5800	0,6374
		2	0,9063	0,9989	0,9459	0,6863	0,7955
15	40	0	0,735	0,999	0,826	0,679	0,745
		1	0,617	0,998	0,765	0,578	0,658
		2	0,897	0,999	0,969	0,674	0,795
20	50	0	0,755	0,999	0,871	0,551	0,675
		1	0,762	0,999	0,880	0,595	0,710
		2	0,898	0,999	0,964	0,624	0,757
30	50	0	0,694	0,999	0,875	0,571	0,691
		1	0,663	0,998	0,842	0,432	0,571
		2	0,895	0,999	0,928	0,753	0,831

Ep = Epoch, **Seq** = Sequence Length, **Cls** = Cluster, **Prec** = Precision, **Rec** = Recall, **F1** = F1-Score

Berdasarkan perbandingan hasil evaluasi LSTM dengan dan tanpa penggunaan SMOTE, dapat disimpulkan bahwa pendekatan tanpa SMOTE memberikan performa yang lebih unggul dan stabil pada seluruh cluster dan variasi epoch serta sequence length. Model tanpa SMOTE secara konsisten menghasilkan nilai PR-AUC, precision, dan F1-score yang lebih tinggi, menunjukkan kemampuan pemisahan kelas fraud dan non-fraud yang lebih baik dengan tingkat false positive yang lebih rendah. Sebaliknya, penggunaan SMOTE cenderung meningkatkan recall namun tidak diikuti

oleh peningkatan precision, sehingga secara keseluruhan tidak efektif untuk dataset dengan karakteristik fraud berbasis histori transaksi nasabah. Oleh karena itu, pendekatan LSTM tanpa SMOTE dipilih sebagai konfigurasi utama dalam penelitian ini, sementara SMOTE diposisikan sebagai pendekatan pembanding.

Tabel 3. Ringkasan Metrik Evaluasi Model Transformer Dengan SMOTE

Ep	Seq	Cls	PR-AUC	ROC-AUC	Prec	Rec	F1
5	20	0	0,6364	0,9985	0,6949	0,6508	0,6721
		1	0,6445	0,9961	0,6909	0,6909	0,6909
		2	0,7995	0,9974	0,7798	0,7589	0,7692
10	30	0	0,7155	0,9859	0,7805	0,5333	0,6337
		1	0,5447	0,9707	0,5806	0,7200	0,6429
		2	0,8531	0,9978	0,9125	0,7157	0,8022
15	40	0	0,667	0,978	0,766	0,643	0,699
		1	0,508	0,986	0,700	0,467	0,560
		2	0,778	0,983	0,844	0,707	0,769
20	50	0	0,646	0,993	0,698	0,612	0,652
		1	0,576	0,964	0,600	0,730	0,659
		2	0,845	0,997	0,849	0,729	0,785
30	50	0	0,666	0,979	0,771	0,551	0,643
		1	0,622	0,923	0,867	0,351	0,500
		2	0,777	0,991	0,871	0,718	0,787

Ep = Epoch, **Seq** = Sequence Length, **Cls** = Cluster, **Prec** = Precision, **Rec** = Recall, **F1** = F1-Score

Tabel 4. Ringkasan Metrik Evaluasi Model Transformer Tanpa SMOTE

Ep	Seq	Cls	PR-AUC	ROC-AUC	Prec	Rec	F1
5	20	0	0,7689	0,9990	0,8070	0,7302	0,7667
		1	0,4870	0,9982	0,5769	0,8182	0,6767
		2	0,8975	0,9988	0,9512	0,6964	0,8041
10	30	0	0,7409	0,9990	0,7963	0,7167	0,7544
		1	0,6578	0,9986	0,8750	0,4200	0,5676
		2	0,8803	0,9984	0,9310	0,7941	0,8571
15	40	0	0,804	0,999	0,837	0,732	0,781
		1	0,570	0,998	0,684	0,578	0,627
		2	0,845	0,998	0,907	0,739	0,814
20	50	0	0,753	0,999	0,864	0,776	0,817
		1	0,645	0,999	0,786	0,595	0,677
		2	0,887	0,999	0,930	0,776	0,846
30	50	0	0,797	0,993	0,825	0,673	0,742
		1	0,617	0,998	0,727	0,649	0,686
		2	0,876	0,998	0,901	0,753	0,821

Ep = Epoch, **Seq** = Sequence Length, **Cls** = Cluster, **Prec** = Precision, **Rec** = Recall, **F1** = F1-Score

Berdasarkan hasil evaluasi model Transformer dengan dan tanpa penggunaan SMOTE, dapat disimpulkan bahwa pendekatan tanpa SMOTE memberikan performa yang lebih konsisten dan unggul pada sebagian besar cluster dan variasi epoch serta sequence length. Pada skenario tanpa SMOTE, model Transformer menghasilkan nilai PR-AUC, precision, dan F1-score yang lebih tinggi dan stabil, menunjukkan kemampuan yang lebih baik dalam membedakan transaksi fraud dan non-fraud dengan tingkat false positive yang lebih rendah. Sebaliknya, penggunaan SMOTE cenderung meningkatkan recall pada beberapa konfigurasi, namun sering diikuti dengan penurunan precision dan fluktuasi PR-AUC, yang mengindikasikan bahwa oversampling tidak selalu efektif untuk dataset dengan karakteristik fraud sebagai pencilan ekstrem berbasis histori transaksi. Oleh karena itu, pendekatan Transformer tanpa SMOTE dipilih sebagai konfigurasi utama dalam penelitian ini, sementara SMOTE digunakan sebagai pendekatan pembanding untuk menganalisis dampak penanganan imbalance data

b. Pembahasan Hasil Pemodelan

Hasil pengujian menunjukkan bahwa baik pada model LSTM maupun Transformer, pendekatan tanpa oversampling (non-SMOTE) memberikan performa yang lebih baik dan stabil dibandingkan dengan penggunaan SMOTE. Skenario non-SMOTE menghasilkan nilai PR-AUC, precision, dan F1-score yang lebih

tinggi, menandakan pemisahan kelas fraud dan non-fraud yang lebih efektif dengan risiko false positive yang lebih rendah. Sebaliknya, SMOTE cenderung meningkatkan recall namun tidak meningkatkan kinerja keseluruhan model. Oleh karena itu, pendekatan tanpa SMOTE dipilih sebagai konfigurasi utama dalam penelitian ini.

Tabel 5. Perbandingan Kinerja LSTM dan Transformer per Cluster

Cls	Model	PR-AUC (avg)	Prec (avg)	Rec (avg)	F1 (avg)
0	LSTM	0.745	**0.863**	0.597	0.704
0	Transformer	**0.773**	0.826	**0.726**	**0.772**
1	LSTM	**0.682**	**0.794**	0.564	**0.655**
1	Transformer	0.596	0.730	**0.612**	0.647
2	LSTM	**0.901**	**0.954**	0.687	0.797
2	Transformer	0.877	0.924	**0.752**	**0.829**

Berdasarkan tabel perbandingan, terlihat bahwa tidak terdapat satu model yang secara absolut unggul pada seluruh cluster. Transformer menunjukkan performa yang lebih seimbang pada Cluster 0 dan Cluster 2 dengan nilai F1-score yang lebih tinggi, sementara LSTM lebih stabil pada Cluster 1 dengan precision dan PR-AUC yang lebih baik. Temuan ini menegaskan bahwa pemilihan model terbaik sebaiknya dilakukan secara cluster-aware, dengan menyesuaikan karakteristik pola fraud pada masing-masing kelompok nasabah.

SIMPULAN

Penelitian ini menunjukkan bahwa pendekatan cluster-aware efektif dalam merepresentasikan perbedaan perilaku nasabah dan meningkatkan kinerja deteksi fraud pada transaksi perbankan. Berdasarkan hasil penelitian, sistem deteksi dini fraud pada transaksi digital perbankan berhasil dikembangkan menggunakan pendekatan deep learning berbasis data transaksi sekuensial yang mampu memanfaatkan pola perilaku historis nasabah dan tetap efektif pada data yang tidak seimbang. Hasil evaluasi menunjukkan bahwa Transformer unggul pada dua klaster dengan nilai PR-AUC sebesar 0,773 dan 0,877 serta precision 0,826 pada masing-masing klaster, sementara LSTM menunjukkan performa terbaik pada satu klaster dengan PR-AUC sebesar 0,901 dan precision sebesar 0,954. Secara keseluruhan, temuan ini menunjukkan bahwa Transformer memberikan performa yang lebih konsisten dalam mendeteksi fraud pada transaksi perbankan digital yang memiliki pola kompleks dan heterogen, meskipun LSTM tetap sangat efektif pada karakteristik klaster tertentu.

DAFTAR PUSTAKA

Mahmud, F. (2024). *Transforming Banking Security : The Role Of Deep Learning In Fraud*. *06*, 20–32.

Ghrib, T., Khaldi, Y., Pandey, P. S., & Abusal, Y. A. (2024). Advanced Fraud Detection in Card-Based Financial Systems Using a Bidirectional Lstm-Gru Ensemble Model. *Applied Computer Science*, *20*(3), 51–66. https://doi.org/10.35784/acs-2024-28

Hasugian, L. S., & Suharjito, S. (2023). Fraud Detection for Online Interbank Transaction Using Deep Learning. *Syntax Literate ; Jurnal Ilmiah Indonesia*, *8*(6), 4263–4275. https://doi.org/10.36418/syntax-literate.v8i6.12627

Jain, S., Chaudhary, K., & Chougule, P. (2023). *Statistical Analysis of Machine Learning Algorithms for Fraud Detection in Bank Transactions*.

Prabha, D. P., & Priscilla, C. V. (2024). A combined framework based on LSTM autoencoder and XGBoost with adaptive threshold classification for credit card fraud detection. *The*

Scientific Temper, *15*(02), 2216–2224. https://doi.org/10.58414/scientifictemper.2024.15.2.34

Fan, L., Wang, C., & Lu, Z. (2024). Application of AdaBound-Optimized XGBoost-LSTM Model for Consumer Credit Assessment in Banking Industries. *Journal of Organizational and End User Computing*, *36*(1), 1–24. https://doi.org/10.4018/JOEUC.343256

Meng, C. C., Lim, K. M., Lee, C. P., & Lim, J. Y. (2023). Credit Card Fraud Detection using TabNet. *2023 11th International Conference on Information and Communication Technology, ICoICT 2023*, *2023-Augus*, 394–399. https://doi.org/10.1109/ICoICT58202.2023.10262711

Xiu, Z. (2025). Financial Transaction Anomaly Detection Based on Transformer Model. *Procedia Computer Science*, *262*, 1209–1216. https://doi.org/10.1016/j.procs.2025.05.162

Ayyadurai, R., Parthasarathy, K., Kumar, N., Panga, R., Bobba, J., & Bolla, R. L. (2025). *Research Article Banksafenet : A Dual-Autoencoder And Transformer-Based Anomaly Detection System For Financial Fraud*. *12(03), 10888–10893*.

Reddy Polu, O. (2023). AI-Based Fake Transaction Detection in Credit Card Payments. *International Journal of Science and Research (IJSR)*, *12*(12), 2205–2210. https://doi.org/10.21275/sr23126171341

Chen, Y., Zhao, C., Xu, Y., & Nie, C. (2025). *Year-over-Year Developments in Financial Fraud Detection via Deep Learning: A Systematic Literature Review*. *Ml*, 1–21. http://arxiv.org/abs/2502.00201

Pushpakumar R. (2025). Cloud-Assisted Batch Learning for Financial Risk Detection Using LSTM, Transformer, and 1D-CNN. *Contemp. Res. in Multi*, *4*(2), 72. https://doi.org/10.5281/zenodo.15069991

Huang, M., & B, W. L. (2023). Proceedings of the 2022 3rd International Conference on E-commerce and Internet Technology (ECIT 2022). In *Proceedings of the 2022 3rd International Conference on E-commerce and Internet Technology (ECIT 2022)*. Atlantis Press International BV. https://doi.org/10.2991/978-94-6463-005-3