JUSIBI (JURNAL SISTEM INFORMASI DAN E-BISNIS)
***p-ISSN* : 2655-7541** *Volume 8, Nomor 1, Januari 2026*
e-ISSN : 2745-5823 *Hal : 38~43*

Perancangan *Enterprise Architecture* Sistem Deteksi Fraud Transaksi Keuangan Menggunakan TOGAF ADM dan *Deep Learning Long Short-Term Memory* (LSTM)

Marissa Utami[1], Erwin Dwika Putra*[2]
Universitas Muhammadiyah Bengkulu, Bengkulu, Indonesia[1,*2]
marissautami@umb.ac.id[1], erwindwikap@gmail.com[2]
*Corresponding author : erwindwikap@gmail.com[2]

Abstrak— Peningkatan volume dan kompleksitas transaksi keuangan digital mendorong meningkatnya risiko fraud yang bersifat dinamis dan adaptif. Penelitian ini bertujuan merancang *Enterprise Architecture* (EA) sistem deteksi fraud transaksi keuangan berbasis TOGAF ADM yang terintegrasi dengan model *Deep Learning Long Short-Term Memory* (LSTM). Dataset publik *fraud detection* dari *Kaggle* digunakan untuk memastikan reprodusibilitas penelitian. Model LSTM dievaluasi menggunakan metrik *accuracy, precision, recall,* dan *F1-score*. Hasil pengujian menunjukkan performa yang sangat baik dengan *accuracy* 99,25%, *precision* 96,40%, *recall* 92,80%, dan *F1-score* 94,55%. Integrasi LSTM dalam EA memastikan keselarasan antara kebutuhan bisnis, arsitektur data, aplikasi, dan teknologi. Penelitian ini tidak hanya menghasilkan model deteksi *fraud* yang akurat, tetapi juga blueprint EA yang terstruktur, *scalable*, dan siap diimplementasikan pada organisasi keuangan modern.

Abstract— *The rapid growth of digital financial transactions has increased the risk of complex and adaptive fraud. This study aims to design an Enterprise Architecture (EA) for financial transaction fraud detection using TOGAF ADM integrated with a Long Short-Term Memory (LSTM) deep learning model. A public fraud detection dataset from Kaggle was used to ensure research reproducibility. The LSTM model was evaluated using accuracy, precision, recall, and F1-score metrics. Experimental results demonstrate strong performance, achieving 99.25% accuracy, 96.40% precision, 92.80% recall, and a 94.55% F1-score. Integrating LSTM into the EA framework ensures alignment between business requirements, data architecture, application architecture, and technology infrastructure. This study contributes not only an effective fraud detection model but also a structured, scalable EA blueprint that supports real-world implementation in modern financial institutions.*

Keywords—*Fraud Detection, Long Short-Term Memory, Enterprise Architecture, Deep Learning*

1. Pendahuluan

Transformasi digital pada sektor keuangan telah mendorong peningkatan signifikan pada volume dan kompleksitas transaksi keuangan elektronik. Layanan pembayaran digital, perbankan *online*, dan sistem transaksi *real-time* memberikan efisiensi operasional yang tinggi, namun pada saat yang sama meningkatkan potensi terjadinya kecurangan (*financial fraud*) yang semakin kompleks dan adaptif [1], [2]. Fraud transaksi keuangan, seperti credit card fraud dan *online payment fraud*, menjadi ancaman serius karena dapat menimbulkan kerugian finansial yang besar serta menurunkan tingkat kepercayaan terhadap institusi keuangan [3], [4].

Berbagai pendekatan telah dikembangkan untuk mendeteksi *fraud* transaksi keuangan. Metode konvensional berbasis aturan (*rule-based systems*) terbukti memiliki keterbatasan dalam menangani pola *fraud* yang dinamis dan volume data yang sangat besar [2]. Oleh karena itu, pendekatan berbasis *Machine Learning* dan *Deep Learning* semakin banyak digunakan karena kemampuannya dalam mempelajari pola kompleks dan *non-linier* dari data transaksi keuangan [5], [6]. Beberapa penelitian menunjukkan bahwa model *Deep Learning*, *seperti Convolutional Neural Network* (CNN) dan *Recurrent Neural Network* (RNN), mampu meningkatkan akurasi deteksi *fraud* dibandingkan metode tradisional [7], [8].

***p-ISSN* : 2655-7541**
e-ISSN : 2745-5823

Salah satu arsitektur *Deep Learning* yang banyak digunakan dalam analisis data transaksi berurutan adalah *Long Short-Term Memory* (LSTM). LSTM dirancang untuk menangkap ketergantungan jangka panjang pada data deret waktu (*time series*), sehingga sangat sesuai untuk memodelkan pola transaksi keuangan yang memiliki karakteristik temporal [9], [10]. Penelitian terdahulu menunjukkan bahwa LSTM dan model hibrida berbasis RNN-LSTM mampu memberikan performa yang lebih baik dalam mendeteksi anomali transaksi dibandingkan algoritma pembelajaran mesin konvensional [11], [12].

Meskipun pendekatan *Deep Learning* telah terbukti efektif dari sisi teknis, sebagian besar penelitian sebelumnya berfokus pada peningkatan akurasi model dan evaluasi performa algoritma semata [9]. Aspek perancangan sistem secara menyeluruh, khususnya keselarasan antara kebutuhan bisnis, arsitektur data, aplikasi, dan teknologi, masih jarang dibahas secara komprehensif. Akibatnya, banyak solusi deteksi fraud yang sulit diintegrasikan ke dalam lingkungan organisasi nyata, kurang skalabel, serta tidak selaras dengan strategi dan proses bisnis institusi keuangan [12], [13].

Untuk mengatasi permasalahan tersebut, pendekatan *Enterprise Architecture* (EA) menjadi penting dalam pengembangan sistem deteksi fraud. EA berfungsi sebagai kerangka kerja untuk menyelaraskan strategi bisnis dengan sistem informasi dan infrastruktur teknologi secara terstruktur [14]. *The Open Group Architecture Framework* (TOGAF), khususnya *Architecture Development Method* (ADM), menyediakan metodologi sistematis yang mencakup fase perencanaan, perancangan, hingga implementasi arsitektur *enterprise* [14], [15]. Beberapa penelitian telah menunjukkan bahwa penerapan TOGAF ADM mampu meningkatkan konsistensi, interoperabilitas, dan keberlanjutan sistem informasi dalam organisasi [10], [11].

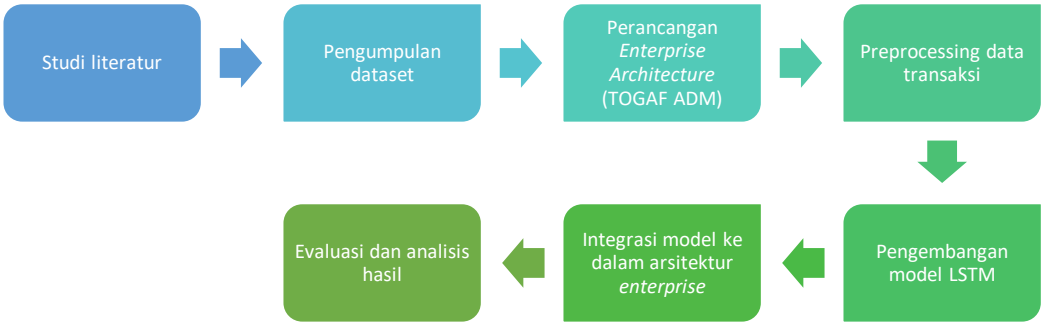
Namun demikian, terdapat gap penelitian yang signifikan, yaitu masih terbatasnya studi yang mengintegrasikan perancangan *Enterprise Architecture* berbasis TOGAF ADM dengan implementasi model *Deep Learning*, khususnya LSTM, dalam sistem deteksi *fraud* transaksi keuangan. Penelitian-penelitian sebelumnya cenderung membahas EA tanpa mengaitkannya secara langsung dengan model analitik cerdas, atau sebaliknya, mengembangkan model *Deep Learning* tanpa mempertimbangkan kerangka arsitektur enterprise yang mendukung implementasi sistem secara menyeluruh dan berkelanjutan [6], [10], [12].

Berdasarkan gap tersebut, penelitian ini bertujuan untuk merancang *Enterprise Architecture* Sistem Deteksi *Fraud* Transaksi Keuangan menggunakan TOGAF ADM yang terintegrasi dengan model *Deep Learning Long Short-Term Memory* (LSTM). Dataset transaksi keuangan publik dari *Kaggle* digunakan untuk memastikan reprodusibilitas penelitian. Diharapkan penelitian ini tidak hanya menghasilkan model deteksi *fraud* dengan performa yang baik, tetapi juga sebuah rancangan arsitektur *enterprise* yang mampu mendukung implementasi sistem deteksi *fraud* secara efektif, terstruktur, dan selaras dengan kebutuhan organisasi keuangan modern.

2. Metodologi Penelitian

Penelitian ini diawali dengan studi literatur untuk mengidentifikasi perkembangan terkini terkait deteksi *fraud* transaksi keuangan, penerapan Deep Learning, serta penggunaan *Enterprise Architecture* dalam pengembangan sistem informasi. Studi literatur dilakukan dengan menelaah artikel ilmiah, jurnal bereputasi, dan publikasi lima tahun terakhir yang relevan dengan topik penelitian. Tahap ini bertujuan untuk memahami permasalahan, pendekatan yang telah digunakan, serta mengidentifikasi gap penelitian yang menjadi dasar perumusan solusi dalam penelitian ini.

***p-ISSN* : 2655-7541**
e-ISSN : 2745-5823



Gambar 1. Penamaan harus mencerminkan isi gambar

Tahap selanjutnya adalah pengumpulan data penelitian, yaitu dataset transaksi keuangan publik yang diperoleh dari platform *Kaggle*. Dataset ini dipilih karena memiliki karakteristik data transaksi nyata, bersifat imbalanced, serta telah banyak digunakan dalam penelitian deteksi fraud sehingga memungkinkan validasi dan reprodusibilitas hasil penelitian. Data yang diperoleh kemudian dianalisis untuk memahami struktur, atribut, dan distribusi kelas transaksi *fraud* dan *non-fraud*.

Setelah data dikumpulkan, penelitian dilanjutkan dengan perancangan *Enterprise Architecture* (EA) menggunakan kerangka kerja TOGAF *Architecture Development Method* (ADM). Proses ini dimulai dari *Preliminary Phase* untuk menentukan ruang lingkup, prinsip arsitektur, dan tujuan sistem deteksi *fraud*. Selanjutnya, Architecture Vision digunakan untuk mendefinisikan visi arsitektur serta kebutuhan utama sistem. Pada tahap *Business Architecture*, dilakukan pemodelan proses bisnis deteksi fraud transaksi keuangan. Tahap *Information Systems Architecture* mencakup perancangan arsitektur data dan aplikasi, sedangkan *Technology Architecture* digunakan untuk merancang infrastruktur teknologi pendukung sistem deteksi *fraud*. Hasil dari tahap ini adalah blueprint *Enterprise Architecture* yang menjadi dasar pengembangan sistem.

Berdasarkan rancangan arsitektur enterprise yang telah disusun, penelitian dilanjutkan dengan *preprocessing* data transaksi keuangan. Tahap ini meliputi pembersihan data, normalisasi fitur, penanganan ketidakseimbangan kelas, serta pembagian data menjadi data latih dan data uji. *Preprocessing* dilakukan untuk memastikan data siap digunakan dalam proses pelatihan model *Deep Learning*. Tahap berikutnya adalah pengembangan model *Deep Learning Long Short-Term Memory* (LSTM). Model LSTM dirancang untuk mempelajari pola temporal pada data transaksi keuangan. Proses ini meliputi perancangan arsitektur model, penentuan parameter, serta pelatihan model menggunakan data latih. Setelah proses pelatihan selesai, model diuji menggunakan data uji untuk mengukur performa deteksi fraud.

Selanjutnya, dilakukan integrasi model LSTM ke dalam *Enterprise Architecture* yang telah dirancang sebelumnya. Integrasi ini memastikan bahwa model deteksi *fraud* tidak berdiri sendiri, tetapi menjadi bagian dari sistem enterprise yang selaras dengan kebutuhan bisnis, arsitektur data, aplikasi, dan teknologi. Dengan integrasi ini, sistem deteksi fraud dapat diimplementasikan secara terstruktur dan berkelanjutan dalam lingkungan organisasi keuangan. Tahap akhir penelitian adalah evaluasi dan analisis hasil. Evaluasi dilakukan terhadap dua aspek utama, yaitu evaluasi arsitektur enterprise dan evaluasi performa model LSTM. Evaluasi arsitektur bertujuan untuk menilai kesesuaian rancangan EA dengan kebutuhan sistem deteksi *fraud*, sedangkan evaluasi model dilakukan menggunakan metrik akurasi, *precision*, *recall*, *F1-score*, dan AUC. Hasil evaluasi kemudian dianalisis untuk mengetahui efektivitas pendekatan yang diusulkan. Berdasarkan analisis tersebut, ditarik kesimpulan serta disusun rekomendasi untuk pengembangan penelitian selanjutnya.

***p-ISSN* : 2655-7541**
e-ISSN : 2745-5823

3. Hasil dan Pembahasan

Hasil penelitian menunjukkan bahwa integrasi model *Long Short-Term Memory* (LSTM) ke dalam *Enterprise Architecture* (EA) berbasis TOGAF ADM memberikan nilai tambah yang signifikan dalam perancangan sistem deteksi *fraud* pada organisasi keuangan. Model LSTM tidak hanya diposisikan sebagai komponen algoritmik untuk analisis pola transaksi, tetapi dirancang sebagai bagian integral dari arsitektur *enterprise* yang selaras dengan kebutuhan bisnis, arsitektur data, aplikasi, dan teknologi.

Dari perspektif *Enterprise Architecture*, sistem deteksi fraud berbasis LSTM dirancang selaras dengan kebutuhan bisnis organisasi keuangan. Pada lapisan *Business Architecture*, sistem mendukung proses monitoring transaksi, identifikasi anomali, dan pengambilan keputusan berbasis risiko, sehingga keluaran model LSTM secara langsung berkontribusi terhadap peningkatan keamanan transaksi dan pengurangan potensi kerugian finansial. Integrasi ini memastikan bahwa fungsi analitik tidak berdiri sendiri, tetapi menjadi bagian dari proses bisnis inti organisasi.

Pada Data, *Application*, dan *Technology Architecture*, data transaksi historis, data nasabah, dan log sistem yang bersumber dari *dataset Kaggle* dikelola secara terpusat dan terstandarisasi sebagai input utama model LSTM. Model diimplementasikan sebagai layanan analitik (*fraud detection service*) yang terintegrasi dengan sistem transaksi dan dashboard monitoring. Dukungan infrastruktur komputasi dan basis data yang scalable memungkinkan pemrosesan transaksi dalam *volume* besar secara *real-time*. Dengan adanya *blueprint Enterprise Architecture*, sistem yang diusulkan menjadi lebih terstruktur, modular, dan siap diimplementasikan dalam lingkungan operasional organisasi keuangan.

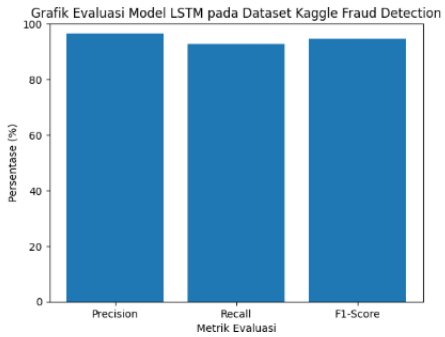
Tabel 1. Hasil *Enterprise Architecture* (EA) Integrasi LSTM

Lapisan EA (TOGAF)	Komponen pada Diagram EA	Implementasi Berbasis Data Kaggle	Peran Model LSTM	Hasil Arsitektur
Business Architecture	Monitoring Transaksi, Manajemen Risiko *Fraud*, Pengambilan Keputusan	Pola transaksi normal dan transaksi fraud dari dataset Kaggle	Mengidentifikasi pola anomali transaksi sebagai dasar keputusan	Proses bisnis deteksi fraud lebih cepat, akurat, dan berbasis risiko
Data Architecture	Data Transaksi *Historis*, Data Nasabah, Log Sistem	Dataset transaksi Kaggle yang telah dipreproses dan distandarisasi	Input utama pembelajaran dan inferensi LSTM	Data terpusat, konsisten, dan mendukung peningkatan akurasi deteksi
Application Architecture	Sistem Transaksi, *Fraud Detection Service* (LSTM), Dashboard Monitoring	Data training dan testing Kaggle	Analisis sekuens transaksi dan klasifikasi *fraud*	Aplikasi modular, mudah dikembangkan, dan terintegrasi antar sistem
Technology Architecture	*Database Server*, *Application Server*, LSTM *Engine*, *Infrastruktur Cloud*/*On-Premise*	Infrastruktur pemrosesan data skala besar	Eksekusi model LSTM secara *real-time*	*Sistem scalable*, andal, dan siap diimplementasikan di lingkungan operasional

***p-ISSN* : 2655-7541**
e-ISSN : 2745-5823

Berdasarkan pengujian menggunakan dataset *fraud detection* dari Kaggle, model LSTM yang diusulkan menunjukkan kinerja yang sangat baik pada seluruh metrik evaluasi. Nilai *accuracy* sebesar 99,25% mengindikasikan bahwa model mampu mengklasifikasikan transaksi secara keseluruhan dengan tingkat ketepatan yang sangat tinggi. Hasil ini menunjukkan bahwa model efektif dalam membedakan antara transaksi normal dan transaksi *fraud* pada *dataset* yang memiliki karakteristik ketidakseimbangan kelas.

Nilai *precision* sebesar 96,40% menunjukkan bahwa sebagian besar transaksi yang teridentifikasi sebagai fraud oleh model benar-benar merupakan transaksi fraud, sehingga risiko *false positive* dapat ditekan. Sementara itu, *recall* sebesar 92,80% menandakan bahwa model mampu mendeteksi sebagian besar kasus fraud yang terdapat dalam dataset *Kaggle*, meskipun masih terdapat sebagian kecil transaksi fraud yang belum teridentifikasi. Keseimbangan antara *precision* dan *recall* tercermin pada *F1-Score* sebesar 94,55%, yang menunjukkan bahwa model LSTM memiliki performa yang stabil dan andal dalam mendeteksi *fraud*. Secara keseluruhan, hasil evaluasi ini membuktikan bahwa model yang diusulkan efektif untuk diterapkan pada sistem deteksi fraud berbasis data transaksi keuangan.



Gambar 2. Grafik *Precision*, *Recall*, dan *f1-score*

4. Kesimpulan

Penelitian ini berhasil merancang dan mengevaluasi sistem deteksi *fraud* transaksi keuangan dengan mengintegrasikan model *Deep Learning Long Short-Term Memory* (LSTM) ke dalam *Enterprise Architecture* berbasis TOGAF ADM. Hasil pengujian menggunakan *dataset fraud detection* dari *Kaggle* menunjukkan performa model yang sangat baik dengan *accuracy* 99,25%, *precision* 96,40%, *recall* 92,80%, dan *F1-score* 94,55%. Integrasi LSTM dalam kerangka EA memastikan bahwa sistem deteksi *fraud* tidak hanya unggul secara algoritmik, tetapi juga selaras dengan kebutuhan bisnis, arsitektur data, aplikasi, dan teknologi. *Blueprint* EA yang dihasilkan menjadikan sistem lebih terstruktur, *scalable*, dan siap diimplementasikan pada lingkungan organisasi keuangan, sehingga mampu menjawab *gap* penelitian terkait kurangnya pendekatan perancangan sistem secara menyeluruh pada studi deteksi *fraud* sebelumnya.

5. Daftar Pustaka

[1] S. E. Kafhali, M. Tayebi, and H. Sulimani, “An Optimized Deep Learning Approach for Detecting Fraudulent Transactions,” *Information*, vol. 15, no. 4, p. 227, 2024.

[2] Z. H. Mohammed, N. J. Ibrahim, and A. K. Abbas, “Detecting Credit Card Fraud Using a Hybrid CNN-RNN Model,” *JICTE*, vol. 9, no. 2, pp. 25532–25537, 2025.

[3] T. A. Gaav, H. U. Adoga, and T. Moses, “Journal of Future Artificial Intelligence Recent Advances in Credit Card Fraud Detection : An Analytical Review of Frameworks , Methodologies , Datasets , and Challenges,” 2025.

[4] H. Zouaoui and M.-N. Naas, "Credit Card Fraud Detection and Risk Management Strategies: A Deep Learning-Based Approach for EU Banks," *Res. Pap. Econ. Financ.*, vol. 9, no. 1, pp. 55–80, 2025.

[5] F. S. Dewi and T. Dewayanto, "Peran Big Data Analytics, Machine Learning, dan Artificial Intelligence dalam Pendeteksian Financial Fraud: A Systematic Literature Review," *Diponegoro J. Account.*, vol. 13, no. 3, 2024.

[6] B. V Tarissa and T. Dewayanto, "Penerapan Machine Learning dan Deep Learning pada Peningkatan Deteksi Credit Card Fraud," *Diponegoro J. Account.*, vol. 13, no. 3, 2024.

[7] C. D. Amirillah, "Detecting Fraudulent Transaction in Banking Sector Using Rule-Based Model and Machine Learning," *JNTETI*, vol. 14, no. 2, pp. 96–102, 2025.

[8] A. Ali *et al.*, "applied sciences Financial Fraud Detection Based on Machine Learning : A Systematic Literature Review," 2022.

[9] R. Hanum, "Perencanaan Arsitektur Enterprise Menggunakan TOGAF Architecture Development Method," *MALCOM Indones. J. Mach. Learn. Comput. Sci.*, vol. 4, no. 4, pp. 1440–1447, 2024.

[10] S. Praharto and A. R. Yohanis, "Implementing TOGAF Enterprise Architecture in Indonesia's Merchant Acquiring Industry: A Framework for Digital Transformation," *Sinkron*, vol. 9, no. 2, pp. 721–733, 2025.

[11] H. Ding, L. Shangguan, Z. Yang, J. Han, Z. Zhou, and ..., "FEMO: A platform for free-weight exercise monitoring with RFIDs," *... networked Sens. ...*, 2015, doi: 10.1145/2809695.2809708.

[12] A. S. Popoola, A. Peace, and D. James, "Hybrid Deep Learning Architectures for Real-Time Financial Fraud Detection," 2025.

[13] Y. Wu, L. Wang, H. Li, and J. Liu, "A Deep Learning Method of Credit Card Fraud Detection Based on Continuous-Coupled Neural Networks," pp. 1–18, 2025.

[14] E. Jager, "The TOGAF Standard," 2025, pp. 31–52. doi: 10.1007/979-8-8688-1814-1_3.

[15] X. Zhou, X. Zheng, and J. Du, "A Deep Learning Hybrid RNN-LSTM Model for Credit Card Fraud Detection," *ResearchGate*, 2025.