TEKNOBIS : Teknologi, Bisnis Dan Pendidikan
Volume 2, No. 2, September 2024
ISSN 9999−9999 (media online)
Hal 244-248

Analisis Penggunaan Machine Learning untuk Deteksi Penipuan di Sektor Keuangan: Tinjauan Literatur

Raka Permana[1], Ibrohim Syakur[2], Arif Rizqi Nugroho[3], Bagas Adi Kurniawan[4], Bagus Sampurno Kuncoroputro[5], Muhammad Ridwan Yazid[6], Ines Heidiani Ikasari[7*]

[1-7]Fakultas Teknik, Teknik Informatika, Universitas Pamulang, Jl. Raya Puspiptek No. 46, Kel. Buaran, Kec. Serpong, Kota Tangerang Selatan. Banten 15310, Indonesia
Email: [1]rakajkt47@gmail.com, [2]baiiim42@gmail.com, [3]arifrizqi1945@gmail.com, [4]bagasadikurniawan5@gmail.com, [5]bagussampurno8@gmail.com, [6]ridwanyazid30@gmail.com, [7*]dosen01374@unpam.ac.id
(* : coressponding author)

Abstrak − Machine Learning (ML) telah menjadi teknologi yang memainkan peran penting dalam berbagai sektor, termasuk sektor keuangan. Salah satu aplikasinya yang paling signifikan adalah deteksi penipuan, yang mencakup identifikasi transaksi mencurigakan, penyalahgunaan klaim asuransi, dan pencucian uang. Artikel ini menyajikan tinjauan literatur sistematis terhadap penerapan ML dalam deteksi penipuan di sektor keuangan, mencakup penelitian dari tahun 2015 hingga 2023. Beberapa algoritma utama yang digunakan meliputi *Random Forest*, *Gradient Boosting Machines*, *Neural Networks*, dan *Support Vector Machines*. Setiap algoritma memiliki keunggulan dan tantangan yang berbeda, seperti kemampuan menangani data tidak seimbang, akurasi tinggi dalam mendeteksi pola kompleks, namun dengan keterbatasan seperti kurangnya transparansi dan risiko overfitting. Penelitian ini juga menemukan bahwa ML memungkinkan deteksi penipuan secara otomatis dan real-time dengan tingkat akurasi yang lebih tinggi dibandingkan metode tradisional. Namun, tantangan utama termasuk keterbatasan data berkualitas, regulasi yang ketat, serta proses adopsi teknologi yang lambat. Untuk mengatasi tantangan tersebut, penelitian masa depan direkomendasikan untuk mengembangkan model yang lebih transparan (Explainable AI), meningkatkan solusi untuk data tidak seimbang, dan mempercepat integrasi ML dengan infrastruktur keuangan yang ada. Dengan langkah-langkah ini, ML memiliki potensi untuk merevolusi deteksi penipuan di sektor keuangan, membantu mengurangi kerugian finansial, dan meningkatkan keamanan sistem keuangan secara keseluruhan.

Kata Kunci: Machine Learning, Deteksi Penipuan, Sektor Keuangan, Random Forest, Explainable AI

Abstract *− Machine Learning (ML) has emerged as a critical technology across various sectors, including finance. One of its most significant applications is fraud detection, encompassing the identification of suspicious transactions, insurance claim abuse, and money laundering. This article presents a systematic literature review of ML applications in fraud detection within the financial sector, covering studies from 2015 to 2023. Key algorithms utilized include Random Forest, Gradient Boosting Machines, Neural Networks, and Support Vector Machines. Each algorithm offers distinct advantages and challenges, such as the ability to handle imbalanced data and achieve high accuracy in identifying complex patterns, while facing limitations like a lack of transparency and the risk of overfitting. This study also highlights that ML enables automated and real-time fraud detection with greater accuracy compared to traditional methods. However, significant challenges persist, including the lack of high-quality data, strict regulatory frameworks, and slow technology adoption processes. To address these challenges, future research is recommended to develop more transparent models (Explainable AI), enhance solutions for handling imbalanced data, and accelerate the integration of ML into existing financial infrastructures. With these advancements, ML has the potential to revolutionize fraud detection in the financial sector, mitigate financial losses, and strengthen the security of financial systems.*

Keywords*: Machine Learning, Fraud Detection, Financial Sector, Random Forest, Explainable AI*

1. PENDAHULUAN

Machine Learning (ML) telah mengalami perkembangan pesat dalam satu dekade terakhir, dengan berbagai aplikasi yang semakin luas di berbagai sektor. Teknologi ini memungkinkan komputer untuk belajar dari data dan membuat keputusan secara otomatis tanpa diprogram secara eksplisit. Di sektor keuangan, ML menawarkan potensi besar untuk meningkatkan efisiensi dan keamanan, terutama dalam mendeteksi penipuan. Dalam konteks ini, deteksi penipuan adalah salah satu aplikasi yang paling signifikan, dengan tujuan untuk mengidentifikasi transaksi mencurigakan, menganalisis risiko kredit, dan mengoptimalkan proses bisnis.

TEKNOBIS : Teknologi, Bisnis Dan Pendidikan
Volume 2, No. 2, September 2024
ISSN 9999–9999 (media online)
Hal 244-248

Kemampuan ML untuk menganalisis pola yang kompleks dan mendeteksi anomali dalam data keuangan telah menarik perhatian industri keuangan. Algoritma seperti *Random Forest*, *Gradient Boosting Machines, Neural Networks, dan Support Vector Machines* telah terbukti efektif dalam mendeteksi transaksi yang mencurigakan secara otomatis dan secara real-time. Misalnya, *Random Forest* dapat menangani data yang tidak seimbang dengan baik, sementara Neural Networks mampu mengenali pola-pola yang sangat kompleks dalam transaksi. *Gradient Boosting Machines* meningkatkan akurasi model dengan menggabungkan hasil dari beberapa pohon keputusan, dan SVM efektif dalam mendeteksi penipuan pada dataset dengan dimensi tinggi.

Namun, penerapan ML dalam deteksi penipuan di sektor keuangan tidak tanpa tantangan. Keterbatasan data berkualitas, ketatnya regulasi di industri keuangan, serta adopsi teknologi yang lambat menjadi hambatan utama. Data yang tidak seimbang dalam dataset keuangan dapat mempengaruhi performa model, membuatnya sulit untuk melatih model dengan akurasi tinggi. Selain itu, transparansi model yang digunakan dalam deteksi penipuan masih menjadi masalah, di mana beberapa algoritma ML seperti deep learning menghasilkan model yang bersifat *black-box* dan kurang dapat diinterpretasikan. Selain itu, isu terkait privasi dan keamanan data sangat penting dalam aplikasi ini, mengingat sensitivitas informasi yang terlibat.

Artikel ini bertujuan untuk meninjau literatur yang relevan tentang penerapan ML dalam deteksi penipuan di sektor keuangan, mulai dari algoritma yang digunakan hingga tantangan dan potensi pengembangannya di masa depan. Pendekatan *Systematic Literature Review* (SLR) diterapkan untuk mengumpulkan dan menganalisis penelitian dari tahun 2015 hingga 2023. Hasil tinjauan ini mengidentifikasi tren utama dalam aplikasi ML, kesenjangan penelitian yang ada, serta rekomendasi untuk penelitian di masa depan. Dengan memahami lebih dalam tentang potensi dan batasan dari ML, industri keuangan dapat mengoptimalkan penggunaan teknologi ini untuk meningkatkan deteksi penipuan, mengurangi kerugian finansial, dan meningkatkan keamanan sistem keuangan secara keseluruhan.

2. METODE PENELITIAN

Pendekatan *Systematic Literature Review* (SLR) digunakan untuk meninjau literatur dari tahun 2015 hingga 2023. Database yang digunakan meliputi *Google Scholar, IEEE Xplore*, dan *Scopus*. Kata kunci pencarian meliputi *Fraud Detection using Machine Learning*, *Financial Fraud Prevention*, dan *Machine Learning in Finance*. Kriteria inklusi mencakup artikel jurnal dan konferensi yang berbahasa Inggris dan Indonesia, serta relevan dengan topik deteksi penipuan. Total 40 artikel dipilih berdasarkan relevansi dan kualitas penelitian.

Hasil analisis literatur tentang penggunaan algoritma *Machine Learning* (ML) untuk deteksi penipuan di sektor keuangan disajikan di sini. Tinjauan dilakukan untuk mendapatkan pemahaman tentang teknik yang digunakan, studi kasus penerapan, dan manfaat dan kekurangan.

2.1 Algoritma yang Digunakan untuk Deteksi Penipuan

Machine Learning menawarkan berbagai algoritma untuk mendeteksi penipuan di sektor keuangan, termasuk:

a. *Random Forest (RF)*: Algoritma ini populer untuk deteksi penipuan karena mampu menangani data tidak seimbang dengan baik.
b. *Gradient Boosting Machines (GBM)*: Digunakan untuk meningkatkan akurasi dalam klasifikasi transaksi mencurigakan (Zhang & Li, 2021).
c. *Neural Networks*: Digunakan untuk analisis pola yang kompleks dalam transaksi.
d. *Support Vector Machines (SVM)*: Efektif dalam mendeteksi penipuan pada dataset dengan dimensi tinggi.

2.2 Aplikasi Deteksi Penipuan dalam Berbagai Kasus

a. Transaksi Kartu Kredit: Algoritma seperti RF dan GBM digunakan untuk mendeteksi transaksi mencurigakan secara real-time.
b. Penyalahgunaan Klaim Asuransi: *Neural Networks* membantu memprediksi klaim yang tidak sah berdasarkan pola data historis.

TEKNOBIS : Teknologi, Bisnis Dan Pendidikan
Volume 2, No. 2, September 2024
ISSN 9999–9999 (media online)
Hal 244-248

c. Deteksi Pencucian Uang (*Money Laundering*): Model berbasis Clustering membantu mengidentifikasi transaksi mencurigakan yang melibatkan jumlah besar uang dalam waktu singkat.

2.3 Keunggulan dan Tantangan

a. Keunggulan: ML memungkinkan identifikasi penipuan secara otomatis dengan tingkat akurasi yang lebih tinggi dibandingkan metode tradisional. Analisis real-time dapat dilakukan untuk mencegah kerugian finansial lebih lanjut.
b. Tantangan:
   1) Data Tidak Seimbang: Sebagian besar dataset keuangan memiliki proporsi yang jauh lebih kecil untuk transaksi penipuan dibandingkan yang sah.
   2) Black-box Nature: Beberapa algoritma ML seperti Deep Learning sulit untuk diinterpretasikan, sehingga kurang transparan bagi regulator.
   3) Privasi dan Keamanan Data: Penggunaan data sensitif memerlukan pengelolaan yang hati-hati untuk menjaga kerahasiaan.

2.4 Tantangan dan Kesenjangan Penelitian

a. Keterbatasan Data Berkualitas: Banyak penelitian terkendala kurangnya data berkualitas yang representatif untuk melatih model ML.
b. Regulasi yang Ketat: Industri keuangan sangat diatur, sehingga implementasi algoritma harus mematuhi kebijakan privasi dan transparansi.
c. Adopsi Teknologi: Integrasi ML dengan sistem tradisional sering memerlukan waktu dan sumber daya yang besar.

3. ANALISA DAN PEMBAHASAN

Penerapan Machine Learning untuk deteksi penipuan di sektor keuangan memberikan berbagai solusi yang efektif dalam mengidentifikasi transaksi mencurigakan. Namun, tantangan seperti ketidakseimbangan data, transparansi model, dan privasi data masih menjadi hambatan signifikan.

Tabel 1. Perbandingan Algoritma *Machine Learning* dalam Deteksi Penipuan

Algoritma	Keunggulan	Tantangan	Contoh Aplikasi
Random Forest (RF)	Akurat dalam data tidak seimbang	Memerlukan tuning parameter	Transaksi kartu kredit
Gradient Boosting Machines	Akurasi tinggi dalam klasifikasi	Lebih lambat dalam pelatihan	Deteksi transaksi mencurigakan
Neural Networks	Mampu mendeteksi pola kompleks	Black-box, sulit diinterpretasi	Klaim asuransi
Support Vector Machines	Efektif pada data berdimensi tinggi	Tidak cocok untuk dataset besar	Deteksi pencucian uang
Clustering	Identifikasi pola anomali tanpa label	Membutuhkan optimasi jumlah kluster	Transaksi mencurigakan

Tabel ini membandingkan algoritma Machine Learning yang umum digunakan untuk deteksi penipuan di sektor keuangan. Keunggulan, tantangan, dan aplikasi dari setiap algoritma dipaparkan untuk memberikan gambaran menyeluruh tentang efektivitasnya. Random Forest unggul pada data tidak seimbang, sedangkan Gradient Boosting Machines menawarkan akurasi tinggi namun membutuhkan waktu lebih lama dalam pelatihan. Sementara itu, Neural Networks efektif mendeteksi pola kompleks, tetapi memiliki keterbatasan interpretasi.

TEKNOBIS : Teknologi, Bisnis Dan Pendidikan
Volume 2, No. 2, September 2024
ISSN 9999–9999 (media online)
Hal 244-248

Tabel 2. Tantangan Implementasi *Machine Learning*

Tantangan	Penjelasan	Solusi
Data Tidak Seimbang	Transaksi penipuan lebih sedikit dibandingkan transaksi sah	Oversampling (*SMOTE*), Cost-Sensitive Learning
Interpretasi Model	Model seperti Neural Networks sulit dipahami	Explainable AI (XAI)
Privasi dan Keamanan Data	Data keuangan bersifat sensitif dan rentan disalahgunakan	Enkripsi data, kebijakan keamanan siber

Tabel ini menunjukkan berbagai masalah yang dihadapi dalam penggunaan pembelajaran mesin, bersama dengan solusi yang mungkin. Teknik oversampling seperti SMOTE dapat menyelesaikan masalah seperti ketidakseimbangan data, dan pendekatan kecerdasan buatan yang dapat dijelaskan (XAI) dapat meningkatkan transparansi. Kebijakan keamanan siber yang ketat dan enkripsi dapat menyelesaikan masalah keamanan dan privasi data.

Tabel 3. Studi Kasus Penggunaan ML untuk Deteksi Penipuan

Penelitian	Algoritma	Kasus	Hasil
Gupta et al. (2020)	*Random Forest*	Transaksi kartu kredit	Akurasi 95% dalam deteksi penipuan
Zhang & Li (2021)	GBM	Klaim asuransi	Peningkatan efisiensi 30%
Chen et al. (2018)	*Neural Networks*	Transaksi keuangan kompleks	Deteksi pola tersembunyi berhasil

Tabel ini menunjukkan studi kasus dari berbagai penelitian yang menggunakan algoritma pembelajaran mesin untuk deteksi penipuan. Hasil penelitian menunjukkan bahwa GBM dapat mendeteksi klaim asuransi dengan lebih baik, dan algoritma seperti Random Forest dapat melakukan transaksi kartu kredit dengan sangat akurat. Meskipun demikian, Neural Networks memiliki kemampuan untuk menemukan pola tersembunyi dalam transaksi keuangan yang kompleks.

Tabel 4. Teknologi Pendukung ML dalam Deteksi Penipuan

Teknologi	Fungsi	Aplikasi
Big Data Analytics	Mengolah data dalam volume besar	Analisis real-time transaksi
Cloud Computing	Menyediakan kapasitas komputasi	Pemrosesan algoritma *Machine Learning*
Blockchain	Menjamin transparansi data	Keamanan transaksi digital

Pengolahan data skala besar secara real-time dibantu oleh teknologi seperti Big Data Analytics, yang merupakan komponen penting dari machine learning, seperti yang digambarkan dalam tabel ini. Blockchain meningkatkan transparansi dan keamanan transaksi digital, sementara Cloud Computing memberikan kapasitas komputasi yang diperlukan untuk menjalankan algoritma ML.

4. KESIMPULAN

Penerapan Machine Learning dalam deteksi penipuan di sektor keuangan menunjukkan perkembangan yang signifikan. Algoritma seperti *Random Forest, Gradient Boosting Machines, Neural Networks*, dan metode berbasis *Clustering* telah terbukti efektif dalam mengidentifikasi transaksi mencurigakan dan pola anomali. Keunggulan utama dari pendekatan ini adalah peningkatan akurasi deteksi, kemampuan analisis real-time, dan pengolahan data dalam skala besar.

Namun, beberapa tantangan masih dihadapi, termasuk ketidakseimbangan data, keterbatasan interpretasi model (*black-box nature*), serta isu privasi dan keamanan data. Solusi seperti teknik *oversampling* (misalnya SMOTE), pendekatan *Explainable AI* untuk meningkatkan interpretabilitas model, serta penerapan kebijakan keamanan data yang ketat menjadi kunci dalam mengatasi hambatan tersebut.

Penelitian di masa depan disarankan untuk berfokus pada pengembangan algoritma yang transparan, aman, dan adaptif, sehingga dapat memenuhi kebutuhan industri keuangan yang semakin kompleks. Dengan penerapan teknologi pendukung seperti *Big Data Analytics*, *Cloud Computing*, *dan Blockchain*, *Machine Learning* memiliki potensi untuk menjadi solusi utama dalam mendeteksi dan mencegah penipuan keuangan secara lebih efektif.

UCAPAN TERIMA KASIH

Saya dan tim mengucapkan terima kasih kepada para peneliti sebelumnya yang telah menyelesaikan berbagai penelitian dan publikasi ilmiah yang mendasari tinjauan literatur ini. Sumber-sumber yang digunakan dalam penelitian ini sangat penting untuk memperluas pemahaman kita dan memberikan pemahaman yang lebih mendalam tentang penggunaan pembelajaran mesin untuk deteksi penipuan di sektor keuangan. Kami berharap tinjauan ini akan menjadi bagian penting dari proses pengembangan penelitian di masa depan.

REFERENCES

Gupta, R., et al. (2020). "Application of Machine Learning in Fraud Detection." *Journal of Financial Systems.*

Choi, J., et al. (2019). "Predictive Analytics in Fraud Detection Using Machine Learning." *IEEE Transactions on Financial Informatics.*

Zhang, H., & Li, F. (2021). "Fraud Detection Using Machine Learning Techniques." *Finance Research Letters.*

Chen, X., et al. (2018). "Challenges in Implementing ML for Financial Fraud Detection." *Journal of Financial Systems.*

Wilson, P., et al. (2022). "Advanced Fraud Detection Systems Using AI and ML." *Computers & Security.*

Awoyemi, J.O., et al. (2017). "Credit Card Fraud Detection Using Machine Learning Techniques." *IEEE International Conference on Systems, Man, and Cybernetics.*

Lu, C., et al. (2020). "A Comparative Study of Machine Learning Algorithms for Fraud Detection." *Procedia Computer Science.*

Pang, G., et al. (2021). "Deep Learning for Anomaly Detection: A Review." *ACM Computing Surveys.*

Vives, X., (2017). "Digital Disruption in Financial Markets." *Annual Review of Financial Economics.*

Arpit, D., et al. (2019). "Privacy-Preserving Methods for Fraud Detection in Financial Transactions." *Journal of Artificial Intelligence Research.*