The Indonesian Journal of Computer Science
www.ijcs.net
Volume 14, Issue 2, April 2025
https://doi.org/10.33022/ijcs.v14i2.4202

Analisis Prediktif untuk Mendeteksi Penipuan E-Commerce Menggunakan Algoritma Pembelajaran Mesin

Achmad Achsarul Karim[1], Faisal Fahmi[2*]
faisalfahmi@fisip.unair.ac.id[2]
[1,2] Departemen Informasi dan Perpustakaan, Universitas Airlangga
*corresponding author

Informasi Artikel

Diterima : 26 Jun 2024
Direview : 26 Apr 2025
Disetujui : 30 Apr 2025

Kata Kunci

Penipuan Online, E-Commerce, Pembelajaran Mesin, Deteksi Penipuan

Abstrak

Perkembangan e-commerce secara pesat memberikan tantangan baru yang dihadapi oleh masyarakat, salah satunya adalah penipuan dalam transaksi e-commerce. Kerugian yang diakibatkan oleh penipuan e-commerce secara global diperkirakan akan melebihi 48 miliar USD pada tahun 2023. Penggunaan teknologi canggih seperti machine learning dapat menjadi sebuah solusi dalam upaya mendeteksi dan mencegah penipuan e-commerce. Penelitian ini bertujuan untuk mengevaluasi beberapa algoritma machine learning, seperti deep learning, naive bayes, logistic regression, decision tree, dan neural network, untuk mendeteksi penipuan e-commerce. Dataset yang digunakan terdiri dari 1.472.952 transaksi. Penelitian ini terdiri dari beberapa tahapan, yaitu: pengambilan data, pembobotan, seleksi fitur, normalisasi, pembagian data dan analisis data. Pada tahapan analsis, algoritma dibandingkan menggunakan confussion matrix yang terdiri dari sensitivity, precision, accuracy, dan F1 Score. Hasil penelitian menunjukkan bahwa setiap algoritma yang digunakan mendapatkan nilai pengujian yang sangat tinggi dengan persentase lebih dari 90%.

Keywords

Online Fraud, E-Commerce, Machine Learning, Fraud Detection

Abstract

The rapid development of e-commerce provides new challenges faced by society, one of them is fraudulent e-commerce transactions. Losses caused by e-commerce fraud globally are expected to exceed 48 billion USD by 2023. The use of advanced technology such as machine learning can be a solution in an effort to detect and prevent e-commerce fraud. This research aims to evaluate several machine learning algorithms, such as deep learning, naive bayes, logistic regression, decision tree, and neural network, to detect e-commerce fraud. The dataset used consists of 1,472,952 transactions. This research consists of several stages, namely: data retrieval, weighting, feature selection, normalization, data sharing and data analysis. At the analysis stage, the algorithms were compared using a confusion matrix consisting of sensitivity, precision, accuracy, and F1 Score. The results show that each algorithm used gets a very high test value with a percentage of more than 90%.

A. Pendahuluan

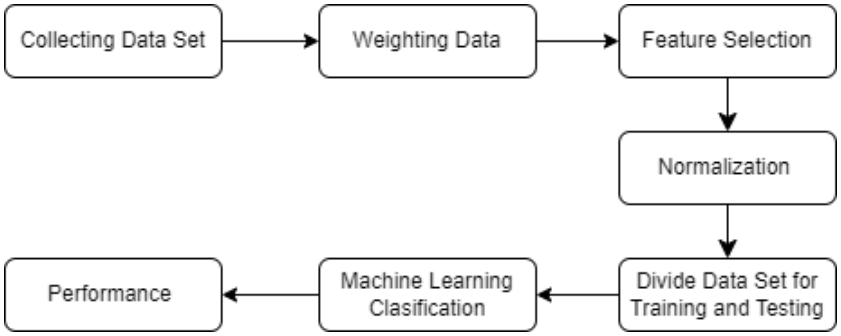
Pendahuluan Perkembangan e-commerce secara pesat dalam beberapa tahun terakhir memberikan berbagai kemudahan bagi konsumen dan peluang besar bagi pelaku bisnis. Namun, terdapat berbagai tantangan baru yang dihadapi oleh masyarakat. Salah satunya adalah penipuan dalam transaksi online melalui e-commerce. Penipuan dalam e-commerce mengacu pada berbagai aktivitas yang dilakukan oleh individu atau kelompok yang terlibat dalam transaksi secara ilegal [1]. Dampaknya, sebagian besar organisasi dan konsumen mengalami kerugian finansial yang besar akibat tindakan penipuan ini [2]. Berdasarkan data yang dilansir dari Juniper Research, kerugian yang diakibatkan oleh penipuan e-commerce secara global diperkirakan akan melebihi 48 miliar USD pada tahun 2023, dari yang sebelumnya hanya sekitar 41 miliar USD [3]. Berdasarkan dampak yang sangat merugikan ini, penggunaan teknologi canggih seperti machine learning dapat menjadi sebuah solusi dalam upaya mendeteksi dan mencegah penipuan e-commerce.

Machine learning menawarkan berbagai model dan algoritma yang dapat mengidentifikasi pola-pola tertentu dari data yang sangat besar dan beragam. Dari data tersebut, memungkinkan algoritma machine learning untuk dapat menemukan pola yang lebih halus dan membuat prediksi yang lebih akurat daripada sebelumnya [4]. Kemampuan ini dapat digunakan untuk mendeteksi penipuan e-commerce, di mana data transaksi yang sangat kompleks dan beragam, mencakup berbagai jenis informasi seperti detail pembayaran, riwayat pembelian, dan jumlah transaksi yang dilakukan. Namun, tidak semua algoritma machine learning memiliki performa yang sama dalam mendeteksi penipuan e-commerce. Setiap metode, model, algoritma memiliki kelebihan dan keterbatasan masing-masing [5]. Oleh karena itu, pemilihan model dan algoritma yang tepat menjadi sangat krusial.

Salah satu model machine learning yang secara efektif digunakan untuk mendeteksi penipuan adalah dengan supervised learning. Model ini menggunakan data training yang telah diberi label yang dikategorikan sebagai transaksi asli dan transaksi penipuan [6]. Kemudian data training tersebut digunakan untuk melatih algoritma dalam mempelajari karakteristik data yang telah dikategorikan ke dalam transaksi asli atau transaksi penipuan. Setelah melalui data training, model ini dapat digunakan untuk memprediksi data baru ke dalam kategori transaksi asli atau transaksi penipuan.

Dalam penelitian ini, akan mengevaluasi beberapa algoritma machine learning yang umum digunakan dalam analisis prediktif seperti, deep learning, naïve bayes, logistic regression, desicion tree, dan neural network. Setelah itu, akan dilakukan perbandingan kinerja dari setiap algoritma berdasarkan hasil confussion matrix guna menetapkan algoritma yang paling optimal dalam mendeteksi transaksi penipuan e-commerce. Dengan demikian, penggunaan teknologi machine learning dalam deteksi penipuan e-commerce diharapkan dapat memberikan hasil prediksi dengan tingkat akurasi yang tinggi dan dapat digunakan secara efektif untuk mendeteksi penipuan dalam e-commerce.

B. Metode Penelitian



Gambar 1. Kerangka Penelitian

Dalam penelitian ini, langkah pertama yang dilakukan adalah dengan mencari dataset penipuan yang dilakuakn dalam e-commerce. Kemudian, dilakukan pembobotan data dengan menggunakan algoritma random forest dan weighting by tree importance untuk mendapatkan feature paling efektif dengan nilai tertinggi yang dapat digunakan dalam proses olah data. Setelah dilakukan pembobotan, terdapat lima feature yang memperoleh nilai lebih dari 1 yang akan digunakan pada tahapan selanjutnya. Feature yang digunakan dapat dilihat pada tabel berikut ini.

Tabel 1. Feature yang digunakan

No	Identitas	*Size*
1	Transaction Amount	7.361
2	Transaction Date	3.748
3	Customer Age	2.080
5	Account Age Days	1.769
6	Transaction Hour	1.387

Selanjutnya, dari feature tersebut akan dilakukan normalisasi data dengan mentransformasikan nilai dari berbagai feature dalam dataset sehingga memiliki skala atau rentang nilai yang seragam atau terstandarisasi. Hal ini dilakukan agar setiap feature berkontribusi secara seimbang tanpa adanya dominasi oleh feature dengan rentang nilai yang lebih besar dibandingkan dengan yang lainnya. Kemudian, analisis prediktif dilakukan dengan menggunakan lima algortima yang terdiri dari deep learning, naïve bayes, logistic regression, desicion tree, dan neural network. Hasil dari prediksi tersebut akan dievaluasi dengan menggunakan confussion matrix yang akan dibandingkan dari nilai sensitivity, precision, accuracy, dan F1 Score.

C. Algoritma Machine Learning

Deep Learning

Deep Learning merupakan sub-bidang dari machine learning yang menggunakan jaringan saraf tiruan dengan banyak lapisan (deep neural networks) untuk memodelkan data yang kompleks dan beragam [6]. Keunggulan utama dari

Deep Learning adalah kemampuannya untuk menangkap dan mempelajari feature-feature yang sangat rumit dan tidak linier dari data transaksi e-commerce. Dengan struktur jaringan yang mendalam, Deep Learning dapat mengekstraksi berbagai feature penting yang sangat efektif dalam mendeteksi berbagai pola penipuan.

Naïve Bayes

Naïve Bayes adalah algoritma klasifikasi probabilistik yang didasarkan pada Teorema Bayes dengan asumsi independensi antar feature yang digunakan [5]. Meskipun asumsi independensi ini jarang sepenuhnya terpenuhi dalam konteks dunia nyata, Naïve Bayes tetap efektif dalam berbagai aplikasi karena kesederhanaannya dan kemampuannya untuk bekerja dengan baik pada dataset dengan jumlah yang besar dengan waktu yang relative singkat.

Logistic Regression

Logistic Regression adalah algoritma yang digunakan untuk memodelkan probabilitas terjadinya suatu peristiwa dengan satu atau lebih variabel dependent dan terdapat korelasi antar feature yang dapat berkontribusi dalam meprediksi data baru [7]. Algoritma ini sangat efektif untuk memprediksi data binominal, seperti menentukan apakah suatu transaksi termasuk kedalam transaksi penipuan atau bukan.

Decision Tree

Decision Tree adalah algoritma yang menggunakan struktur pohon untuk membuat keputusan berdasarkan serangkaian aturan yang diperoleh dari data feature. Setiap node dalam pohon mewakili keputusan berdasarkan suatu feature, dan cabang mewakili hasil dari keputusan tersebut. Decision Tree sangat intuitif dan mudah diinterpretasikan [4]. Hal ini memungkinkan pemahaman yang lebih baik tentang proses pengambilan keputusan dalam mendeteksi penipuan.

Neural Network

Neural Network, yang merupakan dasar dari Deep Learning, menggunakan lapisan neuron yang terinspirasi oleh jaringan syaraf manusia untuk menyelesaikan masalah tertentu seperti pengenalan pola dan klasifiaksi dengan data training [8]. Algoritma ini sangat kuat dalam memodelkan hubungan kompleks dan non-linier dalam data transaksi. Neural Network dapat dilatih untuk mengenali pola-pola yang sangat halus yang mungkin tidak dapat ditangkap oleh algoritma lain.

D. Hasil dan Pembahasan

Penelitian ini dilakukan dengan menggunakan dataset yang diperoleh dari situs Kaggle sejumlah 1,472,952 dataset sintesis. Dalam dataset terdapat label yang terdiri dari dua kategori yaitu sebagai transaksi penipuan dan transaksi asli. Dari 1,472,952 dataset, dibagi menjadi dua dengan rasio 80:20. Sehingga didapatkan data training sejumlah 1.178.361 data training dan 294.591 data testing. Selanjutnya dilakukan pengujian model dengan menggunakan lima

algoritma yang terdiri dari deep learing, naïve bayes, logistic regreseion, decision tree, dan neural network.

Tabel 2. Hasil Confussion Matrix

Alghoritm	*Accuracy*	*Sensitivity*	*Precision*	*F1 Score*
Deep Learning	0.9361	0.9670	0.9658	0.9664
Naïve Bayes	0.9431	0.9818	0.9592	0.9704
Logistic Regression	0.9319	0.9647	0.9637	0.9642
Desicion Tree	0.9547	0.9992	0.9552	0.9767
Neural Network	0.9555	0.9978	0.9572	0.9770

Dalam hasil analisis confussion matrix, dilakukan beberapa metode untuk mengukur tingkat prediksi yang dihasilkan dari berbagai algoritma yang telah digunakan. Metode-metode ini memberikan sudut pandang yang berbeda dari hasil olah data yang telah dilakukan.

Accuracy

Accuracy mengukur proporsi total prediksi yang benar dan salah dari keseluruhan transaksi yang dievaluasi [9]. Dalam mendeteksi transaksi penipuan di e-commerce, akurasi memberikan gambaran umum tentang sejauh mana model mampu mengidentifikasi transaksi yang benar-benar penipuan (True Positives) serta transaksi yang benar-benar bukan penipuan (True Negatives), dibandingkan dengan jumlah total transaksi yang dievaluasi. Berdasarkan data hasil analisis, Neural Network dan Decision Tree menunjukkan nilai accuracy tertinggi masing-masing sebesar (0.9555) dan (0.9547). Naïve Bayes berada di posisi berikutnya dengan accuracy sebesar (0.9431), diikuti oleh Deep Learning (0.9361) dan Logistic Regression (0.9319). Accuracy memberikan gambaran umum tentang seberapa baik model bekerja dalam semua aspek klasifikasi.

Sensitivity

Sensitivity digunakan untuk mengukur kemampuan model dalam meprediksi transaksi penipuan yang benar-benar terjadi. Hal ini dihitung berdasarkan proporsisi antara prediksi benar-benar penipuan, dan semua prediksi penipuan [10]. Algoritma Decision Tree menunjukkan sensitivity tertinggi sebesar 0.9992. Neural Network juga memiliki sensitivity yang sangat tinggi yaitu 0.9978, disusul oleh Naïve Bayes dengan nilai 0.9818, Deep Learning 0.9670, dan Logistic Regression 0.9647. Model dengan sensitivitas tinggi mampu mendeteksi hampir semua transaksi penipuan.

Precision

Precision mengukur proporsi transaksi yang diklasifikasikan sebagai penipuan yang benar-benar merupakan penipuan dibandingkan dengan hasil prediksi penipuan. Deep Learning memiliki precision sebesar 0.9658, sedikit lebih tinggi dibandingkan Logistic Regression (0.9637), tetapi sedikit lebih rendah dari Naïve Bayes (0.9592), Decision Tree (0.9552), dan Neural Network (0.9572). Precision yang tinggi mengurangi jumlah false positive, yaitu transaksi yang sebenarnya sah

tetapi salah diprediksi sebagai penipuan, yang dapat mengganggu pengalaman pengguna.

F1 Score

F1 Score adalah matrix yang menggabungkan precision dan sensitivity, memberikan keseimbangan antara keduanya. Neural Network menunjukkan F1 Score tertinggi sebesar 0.9770, diikuti oleh Decision Tree dengan 0.9767, menunjukkan keseimbangan yang sangat baik antara mendeteksi penipuan dan mengurangi false positive. Naïve Bayes memiliki F1 Score sebesar 0.9704, Deep Learning sebesar 0.9664, dan Logistic Regression sebesar 0.9642. Nilai F1 Score yang tinggi menunjukkan kinerja yang kuat dan seimbang dari model.

E. Kesimpulan

Hasil confussion matrix menunjukkan bahwa dalam evaluasi berbagai algoritma untuk mendeteksi transaksi penipuan di e-commerce, akurasi, sensitivitas, presisi, dan F1 Score memberikan sudut pandang yang berbeda dalam menilai suatu algoritma. Akurasi memberikan gambaran umum tentang kemampuan model yang secara keseluruhan mengidentifikasi transaksi penipuan dan non-penipuan dengan benar. Algoritma Neural Network dan Decision Tree menunjukkan nilai akurasi tertinggi, menandakan bahwa kedua model ini memiliki performa keseluruhan yang sangat baik dalam mendeteksi dan mengklasifikasikan transaksi dengan benar.

Sensitivitas mengukur kemampuan model untuk mendeteksi transaksi penipuan yang sebenarnya terjadi, dengan Decision Tree menunjukkan sensitivitas tertinggi, diikuti oleh Neural Network dan Naïve Bayes. Presisi, digunakan untuk mengukur ketepatan prediksi penipuan, sangat penting untuk mengurangi jumlah false positives yang dapat memberikan alarm palsu. Deep Learning dan Logistic Regression menunjukkan nilai presisi yang tinggi. F1 Score, yang menggabungkan precision dan sensitivity, menunjukkan bahwa Neural Network dan Decision Tree memiliki keseimbangan terbaik dalam mendeteksi penipuan dan mengurangi false positives. Keseluruhan hasil ini menunjukkan bahwa pemilihan algoritma harus mempertimbangkan kebutuhan spesifik dari sistem mendeteksi penipuan, termasuk memperhatikan antara kemampuan prediksi yang akurat dan meminimalisir adanya alarm palsu.

F. Keterbatasan dan Saran Penelitian Selanjutnya

Salah satu keterbatasan utama dari penelitian ini terletak pada ketergantungan terhadap data sintetis untuk pelatihan dan validasi model. Meskipun data sintetis menyediakan lingkungan yang terkontrol untuk menguji kinerja algoritma, data tersebut mungkin tidak sepenuhnya menangkap kompleksitas dan variasi dari transaksi penipuan di dunia nyata. Keterbatasan ini dapat menyebabkan model memiliki performa yang baik dalam studi eksperimental tetapi mungkin kurang sesuai ketika diterapkan dalam lingkungan e-commerce nyata. Dalam penelitian selanjutnya, sebaiknya berfokus pada penggunaan data asli untuk mendapatkan hasil yang lebih relevan.

G. Referensi

[1] M. Gölyeri, S. Çelik, F. Bozyiğit, and D. Kılınç, "Fraud detection on e-commerce transactions using machine learning techniques," *Artif. Intell. Theory Appl.*, vol. 3, no. 1, pp. 45–50, 2023, [Online]. Available: https://www.boyner.com.tr/

[2] E.-A. Minastireanu and G. Mestina, "An Analysis of the Most Used Machine Learning Algorithms for Online Fraud Detection," *Inform. Econ.*, vol. 23, no. 1/2019, pp. 5–16, 2019, doi: 10.12948/issn14531305/23.1.2019.01.

[3] Juniper Research, "eCommerce Losses to Online Payment Fraud to Exceed $48 Billion Globally in 2023," Juniper Research. Accessed: Jun. 21, 2024. [Online]. Available: https://www.juniperresearch.com/press/ecommerce-losses-online-payment-fraud-48bn

[4] A. H. Nasrullah, "Implementasi Algoritma Decision Tree Untuk Klasifikasi Data Peserta Didik," *J. Pilar Nusa Mandiri*, vol. 7, no. 2, p. 217, 2021.

[5] E. Nazarenko, V. Varkentin, and T. Polyakova, "Features of Application of Machine Learning Methods for Classification of Network Traffic (Features, Advantages, Disadvantages)," *2019 Int. Multi-Conference Ind. Eng. Mod. Technol.*, pp. 1–5, 2019, doi: 10.1109/FarEastCon.2019.8934236.

[6] S. Khatri, A. Arora, and A. P. Agrawal, "Card Fraud Detection : A Comparison," *2020 10th Int. Conf. Cloud Comput. Data Sci. Eng.*, pp. 680–683, 2020.

[7] F. Itoo, Meenakshi, and S. Singh, "Comparison and analysis of logistic regression, Naïve Bayes and KNN machine learning algorithms for credit card fraud detection," *Int. J. Inf. Technol.*, vol. 13, no. 4, pp. 1503–1511, 2021, doi: 10.1007/s41870-020-00430-y.

[8] V. Y. P. Ardhana *et al.*, "Prediksi Flight Delay Berbasis Algoritma Neural Network," *J. Informatics, Electr. Electron. Eng.*, vol. 2, no. 1, pp. 26–30, 2022, doi: 10.47065/jieee.v2i1.429.

[9] J. Xu, Y. Zhang, and D. Miao, "Three-way confusion matrix for classification: A measure driven view," *Inf. Sci. (Ny).*, vol. 507, pp. 772–794, 2020, doi: 10.1016/j.ins.2019.06.064.

[10] D. Valero-Carreras, J. Alcaraz, and M. Landete, "Comparing two SVM models through different metrics based on the confusion matrix," *Comput. Oper. Res.*, vol. 152, no. December 2022, p. 106131, 2023, doi: 10.1016/j.cor.2022.106131.