Journal of Student Research Exploration

https://shmpublisher.com/index.php/josre
p-ISSN 2964-1691 | e-ISSN 2964-8246

Online payment fraud prediction with machine learning approach using naive bayes algorithm

Raihan Muhammad Rizki Rahman[1], Much Aziz Muslim[2]
[1]Department of Information System, Universitas Negeri Semarang, Indonesia
[2]Faculty of Technology Management, Universiti Tun Hussein Onn Malaysia, Malaysia

Article Info

Article history:

Received April 18, 2024
Revised July 02, 2024
Accepted month dd, yyyy

Keywords:

E-commerce
Naive bayes
Data mining
Online transactions
Payment fraud

ABSTRACT

The increase in e-commerce has provided easy access for the public, but it also opens up opportunities for fraud in online transactions. Payment fraud is also a problem that often arises in transactions through electronic media. This research aims to analyze payment fraud in e-commerce transactions. This research uses a machine learning approach using the Naive Bayes algorithm. This research uses online transaction datasets involving various attributes such as payment and shipping methods. The developed Naive Bayes model achieved an accuracy of 61.03% with K = 7. The evaluation shows a balance between precision (59.46%) and recall (62.05%), although this study is limited by data quality and basic assumptions of Naive Bayes. In future research, it is worth considering the use of additional features or more complex data processing to improve the performance of fraud detection in online transactions. This research provides important insights in the fight against financial crime in the context of electronic commerce.

1. Introduction

The development of information and communication technology today has made it easier for people in the process of providing and receiving information [1]. People can now communicate without being constrained by distance, space, and time

[1] ***Corresponding Author:***
Raihan Muhammad Rizki Rahman,
Departement of Information System,
Universitas Negeri Semarang,
Sekaran, Gunungpati, Semarang, Indonesia.
Email: raihanmuhammad22@students.unnes.ac.id
DOI: https://doi.org/10.52465/josre.v2i2.343

constraints [2]. Along with these technological advances, people are also expected to be able to keep up with ongoing developments [3]. Information technology has changed the public landscape, created new types of businesses, and opened up new career opportunities for workers[4]. One aspect of information technology that is experiencing rapid development is the internet, which was originally designed as a private channel for research and academic purposes, but is now widely used by businesses for various services. One of the results of internet advancement is electronic commerce (e-commerce) [5].

E-commerce can be defined as a business activity that connects consumers, manufacturers, service providers, and intermediaries through computer networks, namely the internet [6]. E-commerce consists of two main areas, namely trade between companies and trade between companies and consumers. The use of the internet in economic activity is increasing, including an increase in the number of people using online shopping platforms (e-commerce) as a way to make transactions [5].

Technological advances have two different sides: Facilitating its users in various aspects of life, it can also be used for harmful purposes, such as fraud in digital business [7], [8]. In the context of digital business (e-commerce), electronic commerce has become a popular phenomenon and if technological developments continue, there will be a massive shift from conventional trade to electronic commerce [9]. E-commerce applications are created to bring producers and consumers closer together. These applications allow interactions between producers and consumers to occur remotely, even between countries and continents [9]. People who purchase various goods and services through the internet media are referred to as e-commerce consumers [10]. The definition of a consumer in Law Regulation No. 8 of 1999 concerning Consumer Protection, Article 1 Paragraph 2, states that a consumer is any person who uses goods and/or services available in the community, both for the benefit of oneself, family, others, and other living beings and not for trade [9].

Payment fraud is also an issue that often arises in transactions through electronic media. According to eMarketer, worldwide e-commerce sales increased 27.6% in 2020 and will increase 14.3% in 2021, reaching nearly $5 trillion. Such a large amount of money attracts the attention of fraudsters, which can lead to huge monetary losses [11]. Several studies have investigated various strategies to mitigate the problem of fraud in e-commerce [12]-[14]. From some of the existing studies, machine learning approach becomes a fairly reliable method to analyze fraud in e-commerce.

Naive Bayes classification is one of the machine learning algorithms that can be implemented in data analysis to classify data into appropriate categories. This method is based on Bayes' theorem which assumes that all data are independent

of each other [15]. By applying this algorithm, we can identify patterns or characteristics that indicate whether there is fraud in online transactions.

This research aims to analyze payment fraud in e-commerce transactions. This research uses a machine learning approach using the Naive Bayes algorithm. In addition, a holistic approach in data collection, data cleaning and data analysis is implemented to produce a machine learning model with maximum performance

2. Method

Data Collection

The method used in this study begins with data collection and preparation consisting of a fake dataset that includes various attributes of online transactions such as product price, shipping cost, payment method, and delivery speed. This dataset can be accessed online on the Kaggle platform. The source of the dataset used in this research can be accessed at the link https://www.kaggle.com/datasets/ealaxi/paysim1. The dataset has been used by several previous studies, so the validity of the dataset can be trusted. This dataset is generated using a simulator called PaySim as an approach to the problem.

Data Preprocessing

The data then undergoes a preprocessing stage which includes handling missing values, encoding categorical features to enable processing by the model, and splitting the data into features that will be used for classification model building and the target to be predicted, which is the fraudulent status of the transaction.

Modelling

Once the data is ready, the next step is to create a classification model using the Naive Bayes algorithm. This model aims to learn patterns in the data relating to fraudulent or non-cheating transactions. Naïve Bayes is a straightforward probabilistic machine learning algorithm that relies on Bayes' theorem and assumes independence between features [16], [17]. The classifier calculates the posterior probability for each class and selects the class with the highest probability as the prediction class [18]. The Naive Bayes algorithm was chosen because of its good ability to handle categorical data and its simple yet effective assumption in many cases [19].

After modelling, validation was performed using the K-Fold cross-validation method. K-Fold cross validation divides the dataset into k equal subsets, where each subset is used as test data once while using the other k-1 subsets as training

data [20]. This helps ensure that the resulting model is able to generalize patterns from the data as well as analyze new data or inputs well.

Model Evaluation

Finally, model evaluation is performed using various metrics such as accuracy, precision, recall, F-measure, and area under the ROC curve. These metrics provide a comprehensive understanding of the model's performance in detecting fraud in online payment transactions. The metrics are calculated using the confusion matrix. The confusion matrix table can be seen in Table 1.

Table 1. Confusion matrix table

Classification		Predicted class		
		Yes	No	Amount
Actual Class	Yes	TP	FN	P
	No	FP	TN	N

Each metric is defined as follows:

- Accuracy: the number of visits that are correctly classified.
- Precision: the number of visits correctly classified by the system divided by the number of all visits correctly classified by the system [21].

$$Precision = \frac{TruePositive\ (TP)}{TruePositive\ (TP) + FalsePositive\ (FP)} \quad (1)$$

- Recall: the number of visits correctly classified by the system divided by the number of positive visits in the test set.

$$Recall = \frac{TruePositive\ (TP)}{TruePositive\ (TP) + FalseNegative\ (FP)} \quad (2)$$

- F-measure: measures Recall and Precision simultaneously, it represents a balance between the two.

$$F - Score = \frac{2 * Precision * Recall}{Precision + Recall} \quad (3)$$

- ROC (Receiver Operating Characteristic): measures classification performance at various threshold settings by showing how well the model is able to classify visits. It considers the trade-off between precision and recall.
- Computation time: The training and evaluation time of the algorithm.

3. Results and Discussion

Of the total 200 transactions in Table 2, 51.5% (103 transactions) were not fraudulent, while the remaining 48.5% (97 transactions) were detected as fraudulent. In terms of delivery method, there are two main categories: express and standard delivery. Out of 200 transactions, 29% (58 transactions) of them were identified as fraud in express delivery, while the remaining 18.5% (37 transactions) were detected as fraud in standard delivery. Data was blank on the shipping method for 1% (2 transactions) of fraud. Meanwhile, in the payment method analysis, there were two main options: credit card and PayPal. Out of a total of 97 fraudulent transactions, 46.39% (45 transactions) were related to credit card usage, while 52.58% (51 transactions) were related to PayPal. 1.03% (1 transaction) of frauds were not identified with a clear payment method. It should be noted that the percentage of fraud varies between payment and shipping methods, with PayPal tending to have a slightly higher percentage of fraud than credit cards, and express shipping having a higher percentage of fraud than standard shipping.

Table 2. Description of Dataset Characteristics (N = 200)

Count of transaction_id	Fraud		
Row Labels	No	Yes	Grand Total
<0 or (blank)	2	1	3
0-199	101	96	197
Grand Total	103	97	200
Count of delivery_speed	Fraud		
Row Labels	No	Yes	Grand Total
Express	42	58	100
Standard	61	37	98
(blank)		2	2
Grand Total	103	97	200
Count of payment_method	Fraud		
Row Labels	No	Yes	Grand Total
Credit Card	53	45	98
PayPal	49	51	100
(blank)	1	1	2
Grand Total	103	97	200

In this study, we apply the Naive Bayes classification method to predict whether a transaction is fraudulent or not. After dividing the dataset into training set and testing set, we train the model using the training set, and then test its performance using the testing set.

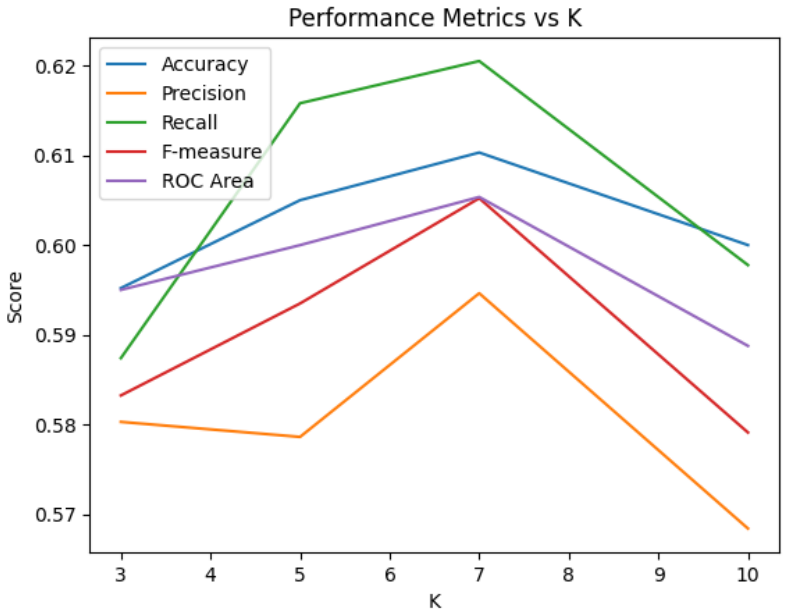

Figure 1. Comparison chart of evaluation results on accuracy, precision, recall, f-measurements, and ROC area metrics

Figure 2. Comparison of the time taken by the model to analyze training and testing data

The evaluation results in Figure 1 show that when we use a value of K = 7 in the Naive Bayes algorithm, we achieve the best performance with an accuracy of 61.03%. The performance was evaluated using standard evaluation metrics such as precision, recall, F-measure, and area under the ROC curve. A comparison of the results of each matrix can be seen in Table 3.

Table 3. Comparison of evaluation matrix results

K	Accuracy	Precision	Recall	F-Measure	ROC Area
3	0,595	0,580	0,587	0,583	0,595
5	0,605	0,579	0,616	0,593	0,600
7	0,610	0,595	0,621	0,605	0,605
10	0,600	0,568	0,579	0,579	0,589

In this study, we found that the precision of 59.46% indicates that most of the transactions predicted as fraudulent by the model are actually fraudulent. Meanwhile, the recall of 62.05% indicates that the model can identify most of the actual fraudulent transactions. The F-measure of 60.52% reflects the balance between precision and recall.

From the explanation of the research results above, it is known that the machine learning model created using the Naive Nayes algorithm generally has a fairly good performance. However, this study has several limitations, namely dependence on the quality of the data used, the basic assumptions of the Naive Bayes method, and the size of the dataset can affect the performance of the model. In future research, it is recommended to consider using additional features or more complex data processing to improve the predictive ability of our model.

4. Conclusion

This research aims to analyze the possibility of fraudulent transactions in e-commerce. This research uses a machine learning approach with the Naïve Bayes algorithm to create a payment fraud analysis model. In this study, applying Naive Bayes classification to predict fraudulent transactions we found that by using a value of K = 7, our model achieved the best accuracy of 61.03%. Nonetheless, the evaluation of other metrics such as precision, recall, and F-measure shows that the model has a balanced performance in identifying fraudulent transactions. However, this study has limitations in data quality and basic assumptions of the Naive Bayes method. In future research, it is recommended to consider using additional features or more complex data processing to improve the predictive ability of our model.

REFERENCES

[1] L. Y. Siregar and M. I. P. Nasution, "Perkembangan Teknologi Informasi Terhadap

Peningkatan Bisnis Online," *HIRARKI J. Ilm. Manaj. Dan Bisnis*, vol. 2, no. 1, 2020.
[2] A. G. Gani, "PENGENALAN TEKNOLOGI INTERNET SERTA DAMPAKNYA," *J. Sist. Inf. Univ. Suryadarma*, vol. 2, no. 2, Jun. 2014, doi: 10.35968/jsi.v2i2.49.
[3] T. Y. Rahmanto, "Penegakan Hukum terhadap Tindak Pidana Penipuan Berbasis Transaksi Elektronik," *J. Penelit. Huk. Jure*, vol. 19, no. 1, p. 31, Mar. 2019, doi: 10.30641/dejure.2019.V19.31-52.
[4] N. S. Lubis and M. I. P. Nasution, "PERKEMBANGAN TEKNOLOGI INFORMASI DAN DAMPAKNYA PADA MASYARAKAT," *Kohesi J. Sains Dan Teknol.*, vol. 1, no. 12, pp. 41–50, 2023, doi: https://doi.org/10.3785/kohesi.v1i12.1311.
[5] A. E. Saragih, M. F. Bagaskara, and Mulyadi, "PERLINDUNGAN HUKUM TERHADAP KONSUMEN DALAM TRANSAKSI E-COMMERCE," *Civilia J. Kaji. Huk. Dan Pendidik. Kewarganegaraan*, vol. 2, no. 1, pp. 145–155, 2023, doi: https://doi.org/10.572349/civilia.v2i2.414.
[6] J. Solim, M. S. Rumapea, Agung Wijaya, B. M. Manurung, and W. Lionggodinata, "UPAYA PENANGGULANGAN TINDAK PIDANA PENIPUAN SITUS JUAL BELI ONLINE DI INDONESIA," *J. Huk. Samudra Keadilan*, vol. 14, no. 1, pp. 97–110, May 2019, doi: 10.33059/jhsk.v14i1.1157.
[7] A. A. Fauzi *et al.*, *PEMANFAATAN TEKNOLOGI INFORMASI DI BERBAGAI SEKTOR PADA MASA SOCIETY 5.0*. Jambi: PT. Sonpedia Publishing Indonesia, 2023.
[8] S. Kadir, "Keuangan Terdesentralisasi (DeFi) Dan Teknologi Keuangan (FinTech) Syariah Dalam Sistem Keuangan Abad 21," *J. Account. Financ.*, vol. 5, no. 2, 2023.
[9] P. R. Silalahi, A. S. Daulay, T. S. Siregar, and A. Ridwan, "Analisis Keamanan Transaksi E-Commerce Dalam Mencegah Penipuan Online," *Profit J. Manajemen, Bisnis Dan Akunt.*, vol. 1, no. 4, 2022, doi: https://doi.org/10.58192/profit.v1i4.481.
[10] E. S. Widyastuti, T. R. Kamila, and P. A. A. Putra, "Perlindungan Konsumen dalam Transaksi e-Commerce: suatu Perspektif Hukum Islam," *Milkiyah J. Huk. Ekon. Syariah*, vol. 1, no. 2, 2022, doi: 10.46870/milkiyah.v1i2.161.
[11] C. J. L. Murray *et al.*, "Global burden of 87 risk factors in 204 countries and territories, 1990–2019: a systematic analysis for the Global Burden of Disease Study 2019," *Lancet*, vol. 396, no. 10258, pp. 1223–1249, Oct. 2020, doi: 10.1016/S0140-6736(20)30752-2.
[12] G. Tong and J. Shen, "Financial transaction fraud detector based on imbalance learning and graph neural network," *Appl. Soft Comput.*, vol. 149, p. 110984, Dec. 2023, doi: 10.1016/j.asoc.2023.110984.
[13] Y. Zhang, J. Bian, and W. Zhu, "Trust fraud: A crucial challenge for China's e-commerce market," *Electron. Commer. Res. Appl.*, vol. 12, no. 5, pp. 299–308, Sep. 2013, doi: 10.1016/j.elerap.2012.11.005.
[14] J. Song, X. Qu, Z. Hu, Z. Li, J. Gao, and J. Zhang, "A subgraph-based knowledge reasoning method for collective fraud detection in E-commerce," *Neurocomputing*, vol. 461, pp. 587–597, Oct. 2021, doi: 10.1016/j.neucom.2021.03.134.
[15] Alvina Felicia Watratan, Arwini Puspita. B, and Dikwan Moeis, "Implementasi Algoritma Naive Bayes Untuk Memprediksi Tingkat Penyebaran Covid-19 Di Indonesia," *J. Appl. Comput. Sci. Technol.*, vol. 1, no. 1, pp. 7–14, Jul. 2020, doi: 10.52158/jacost.v1i1.9.
[16] H. A. Ahmad, A. Novianti Winarlie, and E. Miranda, "Indonesia Covid-19 Pandemic Social Media Analysis With Text Mining," in *2022 International Conference on Information Management and Technology (ICIMTech)*, IEEE, Aug. 2022, pp. 94–99. doi: 10.1109/ICIMTech55957.2022.9915051.
[17] M. AminiMotlagh, H. Shahhoseini, and N. Fatehi, "A reliable sentiment analysis for classification of tweets in social networks," *Soc. Netw. Anal. Min.*, vol. 13, no. 1, p. 7, Dec. 2022, doi: 10.1007/s13278-022-00998-2.
[18] A. V. D. Sano, A. A. Stefanus, E. D. Madyatmadja, H. Nindito, A. Purnomo, and C. P. M. Sianipar, "Proposing a visualized comparative review analysis model on tourism domain using Naïve Bayes classifier," *Procedia Comput. Sci.*, vol. 227, pp. 482–489, 2023, doi: 10.1016/j.procs.2023.10.549.
[19] Ö. F. Arar and K. Ayan, "A feature dependent Naive Bayes approach and its application to the software defect prediction problem," *Appl. Soft Comput.*, vol. 59, pp. 197–209, Oct. 2017,

doi: 10.1016/j.asoc.2017.05.043.
[20] B. G. Marcot and A. M. Hanea, "What is an optimal value of k in k-fold cross-validation in discrete Bayesian network analysis?," *Comput. Stat.*, vol. 36, no. 3, pp. 2009–2031, Sep. 2021, doi: 10.1007/s00180-020-00999-9.
[21] S. Patil, V. Nemade, and P. K. Soni, "Predictive Modelling For Credit Card Fraud Detection Using Data Analytics," *Procedia Comput. Sci.*, vol. 132, pp. 385–395, 2018, doi: 10.1016/j.procs.2018.05.199.