Journal of Leadership and Staff
Vol X No X Month Year
ISSN: XXXX-XXXX (Print) ISSN: XXXX-XXXX (Electronic)
Open Access: https://ejurnal-copus.sespimpolri.id/jls/index

Fraud Accounts Identification Modelling on Multi-Platform E-Commerce

Grawas Sugiharto
School of Electrical Engineering and Informatic Bandung Institute of Technology
Bandung,grawas@students.itb.ac.id
Yudistira Dwi Wardhana Asnar
School of Electrical Engineering and Informatic Bandung Institute of Technology Bandung, yudis@itb.ac.id

Riwayat artikel:
Diterima 05/09/2025
Direvisi 05/09/2025
Disetujui 05/09/2025

ABSTRAK

Abstract— Nowadays, cybercrime is increasingly prevalent in society. Based on data compiled by the Indonesia National Police, the number of cybercrimes increases by 6.46% annually, with online fraud as the most reported crime with 7.892 cases or 44.40% out of the total cases handled. The modus operandi in online fraud primarily uses manipulated profile account to gain the victims' trust. Therefore, it is necessary to have a common detection model for fraud accounts on multi-platform e- commerce to avoid online fraud. This research uses the Naïve Bayes classification, Decision Tree, and K-NN as the modeling algorithms. The classification test result showed that the optimal performance with the highest accuracy differs among the platform. The green platform reaches the highest accuracy using the K-NN algorithm (90.51%), the red platform went to the optimal performance using the Decision Tree algorithm (96.89%), and the multi-platform reached the optimal performance using the Naïve Bayes algorithm (90.02%).

Keywords— Cybercrime, E-Commerce Fraud, Naïve Bayes, Decision Tree, K-NN, Multi-Platform

INTRODUCTION

Nowadays, cybercrime is increasingly prevalent in society. Based on data compiled by the Indonesia National Police, the number of cybercrimes handled by the National Police over the past four years has increased by 6.46% annually [1]. In the mentioned data, the type of crime most widely reported by the public is online fraud, with a total of 7.892 cases or 44.40% of the total cases handled during the last four years, as shown in Table 1:

Table 1. Number of cybercrimes in Indonesia (2015-2019)

Year	2015	2016	2017	2018	2019	Total
Total	2,609	3,110	3,109	4,360	4,586	17,774

The total loss of online fraud in 2019 is Rp 235 million that occurred from 2551 cases. These cases took place in four platforms, namely: email (1.92%), website (13.09%), telecommunication (28.66%), and social media (56.33%), which the primary modus operandi is by selling the item on e- commerce at much lower prices below the market price. Many factors influence the increased number of public reports on online fraud. One of them is the development of technology that drives changes in people's economic lives towards the digital economy [2]. The development can also be observed from a surge in e-commerce application visitors with a total of 3 million users from 2017 to 2019 [3].

RELATED WORK

Fraud account identification has been an exciting topic in e-commerce research and studies, especially in fraud identification. There were many approaches to classify the fraud accounts, such as Clustering, Naïve Bayes (NB), Decision Tree (DT), K-Nearest Neighbor (K-NN), Support

Vector Machine (SVM). This paper decided to build the classification of the fraud account using the basic algorithm in classification such as NB, DT, and K-NN. Despite the advantages of other techniques, the research conducted using a limited resource, so the limitation of the hardware and software used in this research has to count before settling on a classification strategy. SVM and Clustering were deemed unacceptable for this research because they were too costly and processor intensive.

The research from Sahid et al. [4] built an end-to-end classification system for e-commerce websites using DT, K- NN, NB, SVM, Multilayer Perceptron, Logistic Regression from 866 e-commerce websites. It yielded a website classification system with the best achieved F-score of 0.83.

Zhou et al. [5] used DT to classify actual and fraud transactions of credit cards from a Chinese e-commerce company. The research uses Apache Spark on Yarn as the infrastructure to process the data sets. It performs better with a higher detection precision rate, recall rate, accuracy, and F1- score than the existing relative models.

Luo and Wan [6] research designed a conceptual framework to extract the characteristics of fraud transactions, such as seller activity, product value, buyer age, seller's reputation, and details from comments. These characteristics then underlies the selection of features used in this research.

Based on the previous researches on online fraud, all of them were conducted on a single platform. Therefore, it is obtained research opportunity of **detecting fraud accounts on multi-platform e-commerce**. The results of data collection and interviews with stakeholders also support this opportunity, which stated that e-commerce fraud in Indonesia occurred on various platforms [7]. The Green Platform and Red Platform are used to focus the research since they were the top most visited platforms in Indonesia [3]. The Naïve Bayes classification, Decision Tree, and K-NN algorithms applied in this research for modeling since they were the basic classification algorithm. The algorithms expected to construct a model capable of detecting fraud with the highest accuracy value.

The dataset used in this research was obtained from the public report submitted online to the Cyber Patrol website (https://patrolisiber.id). After that, according to the scope of this research, the report data filtered by the Green and Red Platform. The remaining entities of the account then scrapped using the URL from each platform's data. The data scrapping result is then stored into DBMS to build the platform dataset and analyse it later on, as displayed in figure 1 below

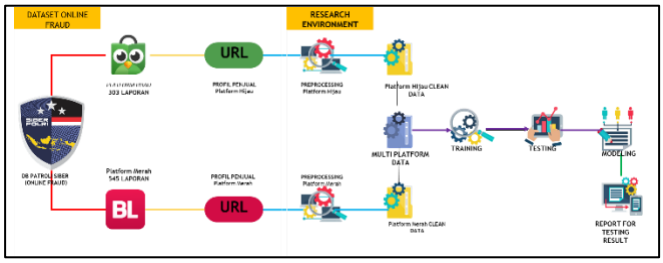

Figure 1 Scheme of Research Methodology

I. FINDINGS AND ANALYSIS

A. *Data Exploration*

There were 303 Green Platform accounts and 545 Red Platform accounts that successfully exported from the Cyber Patrol website (https://patrolisiber.id). The data later compared and validated to check there is no cross-matching entity between the Green and Red Platform. From the data exploration, the perpetrators' most widely used modus operandi is to offer goods to buyers at a lower price that is about 20%-40% cheaper than the market price [8]. Once the buyer is attracted, the perpetrators would persuade the buyer not to use the escrow account and transfer the money directly to the perpetrators' account, as shown in the scheme portrayed in figure 2 [9] [10].

Figure 2 Scheme of Fraud Transactions.

B. *Understanding of Data*

After taking an inventory of accounts in the form of a list of URLs and usernames, then

understanding the data is carried out by designing a Data Dictionary, which contains a list of features used in model building. From the Green Platform, a 23 feature scheme will be prepared, which will be scrapped, as shown in table 2.

Table 2. Attribute Preparation from Green Platform

No	Features	Description
1	Scrapped Time	A feature that shows the time when an account is scrapped for research.
2	Fraud	Account label on dataset which generated from the cyber patrol database.
3	Status	Status feature in shops' account
4	Establish	A feature which records time when the online shop registering to the platform.
5	URL	URL of the online shops.
6	Username	A feature which records the username
7	Address	A feature which records address
8	Description	A feature which description address
9	Location	A feature which records location
10	Review	A feature to display product review number
11	Followers	A feature to display number of follower
12	Seller Type	A feature to display online shop type
13	Rating Negative_1	A feature to display number of star 1 rates of
14	Rating Negative_2	A feature to display number of star 2 rates of
15	Rating_netral_3	A feature to display number of star 3 rates of
16	Rating Positive_4	A feature to display number of star 4 rates of
17	Rating Positive_5	A feature to display number of star 5 rates of an online shop.
18	Delivery Options	A feature which records delivery service
19	Badge	A feature which records badge
20	Point	A feature which records number of points
21	Rank	A feature which records ranks
22	Product Sold	A feature to display number of sold products
23	Reply Time	A feature to display respond time of a discussion/DM of an online shop.

From the Red Platform, a scheme of 13 features will be prepared, which will be scrapped as shown in table 3.

Table 3 Preparation Attribute from Red Platform

No	Features	Description
1	Scrapped Time	A feature that shows the time when an account is scrapped for research.
2	Fraud	Account label on dataset which generated from the cyber patrol database.
3	Establish	A feature which records time when the online shop registering to the platform.
4	URL	URL from online shops.
5	Username	A feature which records the username
6	Location	A feature which records location
7	Review	A feature to display product review number
8	Followers	A feature to display number of follower
9	Seller Type	A feature to display online shop type

10	Rating Positive	A feature to display number of positive rates of an online shop.
11	Rating Negative	A feature to display number of negative rates of an online shop.
12	Delivery Service	A feature which records delivery service of the online shops on the platform.
13	Delivery Time	A feature to display average time of sending package to the expedition service.

As for the prepared features, the data scrapping is done using the Jupyter-Notebook 6.0 tool based on Python 3.7.6. The results of scrapping data are then stored into MySQL
7.4.3 DBMS for later analysis of the features of the seller's accounts as displayed in figure 3 below.

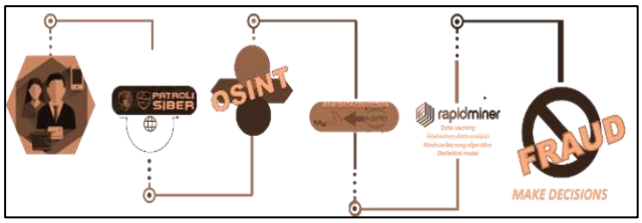

Figure 3 Real World Data Collection

C. Preprocessing Data

1) Green Platform

A total of 1127 accounts were scrapped from on the Green Platform dataset, consisting of 303 fraud accounts and 824 non-fraud accounts originating from the cyber patrol database. From the scrapped data, there were several missing values

known in several features, such as Status (760), Description (434), Location (6), Type Seller (591). Then, replacement fills in features with Nominal data types, such as No Status Alert value on the Status feature, No Description value in the Description feature, No Location value in the Location feature, and Special value in the Type Seller feature. Thus the output of this stage is the absence of Missing Values on all Green Platform data features.

For transformation data, the scrapped and establish features indicate the time since they do not correlate with the Fraud / Not Fraud classification, so these two features are not used (exclude). In addition, the review feature on this platform is provided together with a rating containing the opinions of buyers who need text mining analysis to determine whether the review is negative or positive, so this feature is also not used (excluded) from the Fraud / Not Fraud classification. It is derived to be a new feature for several other features by using the strata sampling method to form 21 derived features as shown in table 4.

Table 4. Data Transformation on the Green Platform

No	Features	Description
1	Fraud	Account label on dataset which generated from the cyber patrol database.
2	Alert	Derivative feature of status
3	URL	URL from online shops.
4	Username Prefix Number	Derivative feature of username to check wether username contains number in prefix
5	Username Infix Number	Derivative feature of username to check wether username contains number in infix

6	Username Suffix Number	Derivative feature of username to check wether username contains number in sufix
7	Username Number Only	Derivative feature of username to check wether username contains number only
8	Username Text Only	Derivative feature of username to check wether username contains text only
9	Address	Derivative feature of address become binominal value (True / False)
10	Description	Derivative feature of description become binominal value (True / False)
11	Location	Derivative feature of location become binominal value (True / False)
12	Followers	A feature to display number of follower reviews of an online shop (no changes)
13	Special Seller	Derivative feature of seller type become binominal value (True / False)
14	Ratio Negative	Derivative feature of negative rating
15	Ratio Positive	Derivative feature of positive rating
16	Instant Delivery	Derivative feature of delivery service become binominal value (True / False)
17	Badge	A feature which records badge of an online shop (no changes)
18	Point Reputation	A feature which records number of points of an online shop (no changes)
19	Rank	A feature which records ranks given by the platform to the online shops based on received rates (no changes)
20	Sold Item	A feature to display number of sold products of an online shop (no changes)
21	Category Reply	Derivative feature of reply

After that, data reduction was performed by detecting outliers using the turkey test method. A total of 143 accounts were reduced based on the average value of outliers from the Turkey Test, leaving 984 accounts consisting of 686 accounts labelled as NOT_FRAUD and 298 accounts labelled as FRAUD.

2) Red Platform

From the scrapping result on the Red platform, 1320 accounts were obtained, which consisted of 545 fraud accounts and 775 non-fraud accounts originating from the cyber patrol database. From the scrapped data, there were several missing values known in several features, such as Establish (425), Location (6), Followers (425), Type Seller (632), and Delivery Time (425). The replacement fill-in was implemented on establishing, followers, type seller, and delivery time feature on the Red platform dataset. The value of the established attribute must be of type date time to support data processing using machine learning; therefore, replacement fill in data was given in dates with values outside the available data as a replacement value. Whereas for an empty value on the delivery time feature, a 0 hours value was assigned.

Some of the features that were not correlated with the classification will be excluded, such as scrapped, establish, review, and location features from the Fraud / Not Fraud classification. The strata sampling method is used for several features to form derived features with 13 features as shown in table 5.

Table 5. Data Transformation on the Red Platform

No	Features	Description
1	Fraud	Account label on dataset which generated from the cyber patrol database.
2	URL	URL from online shops.

3	User Prefix Number	Derivative feature of username to check wether username contains number in prefix
4	User Infix Number	Derivative feature of username to check wether username contains number in prefix
5	User Suffix Number	Derivative feature of username to check wether username contains number in infix
6	User Number Only	Derivative feature of username to check wether username contains number in sufix
7	User Text Only	Derivative feature of username to check wether username contains number only
8	Followers	A feature to display number of follower reviews of an online shop (no changes)
9	Special Seller	Derivative feature of seller type become binominal value (True / False)
10	Ratio Negative	Derivative feature of negative rating
11	Ratio Positive	Derivative feature of positive rating
12	Instant Delivery	Derivative feature of delivery service become binominal value (True / False)
13	Category Delivery Time	Derivative feature of delivery time

Post-data reduction, outliers detection is carried out using the turkey test method on the Review, Followers, Negative Ratio, Positive Ratio, and Sold Item features. Due to a single value of the location feature (LOC entirely), excluded in the next stage. Based on the average outlier value from Turkey Test's, data reduction was carried out by 196 accounts, so that the remaining 1124 accounts consisted of 580 accounts labelled as NOT_FRAUD and 544 accounts labelled as FRAUD.

3) Multi Platform

Multi-platform accounts, data cleansing, data reduction, and data transformation are no longer carried out; data integration remains. At this stage, data integration was carried out from the Green Platform and Red Platforms; a union table

was carried out on the corresponding attributes according to table 6.

Table 6. The Multi-Platform Attributes

No	Features	Description
1	Fraud	Account label on dataset which generated from the cyber patrol database.
2	URL	URL from online shops.
3	User Prefix Number	Derivative feature of username to check whether username contains number in prefix
4	User Infix Number	Derivative feature of username to check whether username contains number in prefix
5	User Suffix Number	Derivative feature of username to check whether username contains number in infix
6	User Number Only	Derivative feature of username to check whether username contains number in suffix
7	User Text Only	Derivative feature of username to check whether username contains number only
8	Followers	A feature to display number of follower reviews of an online shop (no changes)
9	Special Seller	Derivative feature of seller type become binominal value (True / False)
10	Negative Ratio	Derivative feature of negative rating
11	Positive Ratio	Derivative feature of positive rating
12	Instant Delivery	Derivative feature of delivery service become binominal value (True / False)

The total data resulting from the Green Platform and Red Platform dataset integration is 2,108

accounts consisting of 842 data labelled as fraud and 1,266 data labelled as NOT_FRAUD.

D. Data Testing

Towards dataset of Green Platform, Red Platform, and Multi-Platform (data from the integration results between the Green Platform and Red Platforms) are then carried out by training and testing separately. Data Training and Testing were divided using 90:10, 80:20, 70:30, and 60:40 variables, where it will use the stratified sampling method, which divides the data proportionally based on the class/label they have.

After that, every dataset was trained by using the NB, DT, and K-NN algorithm. For DT algorithm is given an additional parameter, namely maximum depth from the tree, which is valued from 5 until 10, to examine how far accuracy value from classification will have the best performance and tends to consistent the value (mature). The same goes for modeling using the K-NN algorithm, which is given an additional parameter, namely K value from 1 – 15 (odd numbers only), to select Neighbor in the data surroundings that will be classified. Each platform testing result is shown in table 7, 8 and 9 respectively.

Table 7. Testing Results on Green Platform

No	Testing Result	NB	DT	K-NN
1	Highest Accuracy	82.74%	88.81%	90.51%
2	Data Ratio	80:20	70:30	70:30
3	Additional Parameter	-	MaxDepth=8	k=11
4	Precision	99.05%	90.14%	88.36%
5	Recall	75.91%	92.75%	94.16%
6	F1 Score	85.95%	91.43%	91.17%

Table 8. Testing Results on Red Platform

No	Testing Result	NB	DT	K-NN
1	Highest Accuracy	95.54%	96.89%	96.22%
2	Data Ratio	90:10	80:20	60:40
3	Additional Parameter	-	MaxDepth=5	k=11
4	Precision	96.43%	100.00%	97.78%
5	Recall	93.10%	93.10%	94.83%
6	F1 Score	94.74%	96.43%	96.28%

Table 9. Testing Results on Multi-Platform

No	Testing Result	NB	DT	K-NN
1	Highest Accuracy	90.02%	88.47%	88.31%
2	Data Ratio	80:20	70:30	70:30
3	Additional Parameter	-	MaxDepth=8	k=7
4	Precision	98.17%	95.43%	83.77%
5	Recall	84.98%	82.61%	87.75%
6	F1 Score	91.10%	88.56%	85.71%

E. Models Construction

From the results of the analysis of the test results, a model with the best level of performance is

obtained from each platform with the following details:

1) *Fraud Account Classification on the Green Platform*

The classification model on the green platform uses 21 features[13]. For the Green platform dataset, the best performance on classification reached with the K-NN algorithm using a data ratio of 70% data for training and 30% data for testing with an accuracy of 90.51% and the number of K was 11. The highest information gain this algorithm is in the **sold item** feature with a score **0.36106**.

2) *Fraud Account Classification on Red Platform*

The classification model on the red platform uses 13 features[14]. The best performance on classification reached with the DT algorithm using a data ratio of 80% data for training and 20% data for testing with an accuracy of 96.89%, and the number of max depth was 5. The highest information gain this algorithm is in the **Special seller** feature with a score **0.79534.**

3) *Fraud Account Classification on Multi Platforms*

The multi-platform classification model uses 12 features (table 2) that came from unifying the corresponding green and red platforms dataset. The best performance on classification reached with the NB algorithm using a data ratio of 80% data for training and 20% data for testing with an accuracy of 90.02%. The highest information gain from this algorithm is in the **positive ratio** feature with a score **0.59535.**

II.

III. FINAL REMARKS

The research has built three datasets from online fraud reports extracted from The Cyber Patrol website (https://patrolisiber.id). The first dataset is from the Green platform in 984 accounts, which consists of 686 data labeled as not fraud accounts and 298 data labeled as fraud accounts. The second is the Red platform in 1124 accounts, consisting of 580 data labeled as not fraud accounts and 544 data labeled as fraud accounts. Meanwhile, the third dataset is the multi- platform dataset constructed from the union between the Green and Red datasets. The multi-platform dataset in of 2108 accounts, which consists of 1266 data labeled as not fraud accounts and 842 data labeled as fraud accounts.

The dataset, later on, was used to model the fraud classification using the NB, DT, and K-NN algorithms. The green platform reaches the highest accuracy using **the K-NN algorithm (90.51%)** with **sold item** as the highest information gain, the red platform went to the optimal performance using **the DT algorithm (96.89%)** with **Special seller** as the highest information gain, and the multi-platform reached the optimal performance using the **NB algorithm (90.02%)** with **positive ratio** as the highest information gain.

For further research, the common detection model's performance expects to enhance the model performance using the cross-fold validation and feature reduction technique. It is also an interesting topic to develop the detection model across social media platforms since many people also used social media to sell products.

REFERENCES

[1] P. Bagian Operasional Dittipidsiber, “Database kejahatan siber 2015 - 2018.” Bareskrim Polri, Agustus 2019.

[2] C. Teoh dan A. K. Mahmood, “National cyber security strategies for digital economy,” *Journal of Theoretical and Applied Information Technology*, vol. 95, hlm. 6510–6522, 2017, doi: 10.1109/ICRIIS.2017.8002519.

[3] I. iPrice, "Daftar 50 Website & Aplikasi E-Commerce di Indonesia 2019," *Peta E-Commerce Indonesia*, Nov 07, 2019. https://iprice.co.id/insights/mapofecommerce/ (diakses Nov 07, 2019).
[4] G. T. Sahid, R. Mahendra, dan I. Budi, "E-Commerce Merchant Classification using Website Information," dalam *Proceedings of the 9th International Conference on Web Intelligence, Mining and Semantics - WIMS2019*, Seoul, Republic of Korea, 2019, hlm. 1–10. doi: 10.1145/3326467.3326486.
[5] H. Zhou, G. Sun, S. Fu, W. Jiang, dan J. Xue, "A Scalable Approach for Fraud Detection in Online E-Commerce Transactions with Big Data Analytics," *Computers, Materials & Continua*, vol. 60, no. 1, hlm. 179–192, 2019, doi: 10.32604/cmc.2019.05214.
[6] S. Luo dan S. Wan, "Leveraging Product Characteristics for Online Collusive Detection in Big Data Transactions," *IEEE Access*, vol. 7, hlm. 40154–40164, 2019, doi: 10.1109/ACCESS.2019.2891907.
[7] A. Saprudin, "Wawancara strategi penanggulangan kejahatan siber terutama pada online fraud," Oktober 2019.
[8] Tokopedia, "Rekening Bersama | Tokopedia Kamus," Nov 12, 2020. https://kamus.tokopedia.com/r/rekening-bersama/ (diakses Nov 12, 2020).
[9] Tokopedia, "Penyebab Toko Dimoderasi - Pusat Seller Tokopedia," *Pusat Seller*, Agu 26, 2019. https://seller.tokopedia.com/edu/penyebab-toko-dimoderasi/ (diakses Nov 12, 2020).
[10] Bukalapak, "Tanya Jawab - Cara Melaporkan Akun yang Melanggar," *Bukalapak*, Nov 12, 2020. https://www.bukalapak.com/bantuan/pelanggaran/pelanggaran- akun%20/cara-melaporkan-pelanggaran-akun (diakses Nov 12, 2020).
[11] G. Sugiharto, "Dataset Green Platform Before Preprocessing," *Penelitian Machine Learning*, Mei 18, 2021. http://bit.ly/green_raw2021 (diakses Mei 18, 2021).
[12] G. Sugiharto, "Dataset Red Platform Before Preprocessing," *Penelitian Machine Learning*, Mei 18, 2021. http://bit.ly/red_raw2021 (diakses Mei 18, 2021).
[13] G. Sugiharto, "Dataset Green Platform After Preprocessing," *Penelitian Machine Learning*, Mei 18, 2021. http://bit.ly/green_pre2021 (diakses Mei 18, 2021).
[14] G. Sugiharto, "Dataset Red Platform After Preprocess," *Penelitian Machine Learning*, Mei 18, 2021. http://bit.ly/red_pre2021 (diakses Mei 18, 2021).