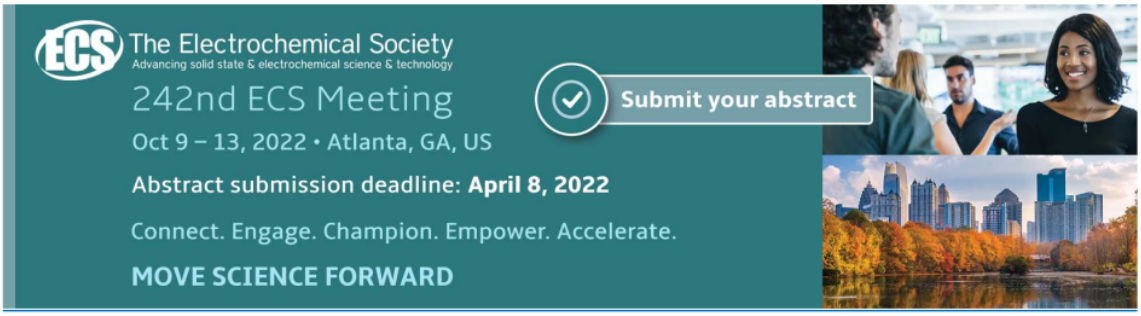
Detection of Frauds for Debit Card Transactions at Automated Teller Machine in Indonesia Using Neural Network

by Ermatita Ermatita

Submission date: 15-Oct-2022 09:36PM (UTC+0800)
Submission ID: 1925998109
File name: t_Automated_Teller_Machine_in_Indonesia_Using_Neural_Network.pdf (849.77K)
Word count: 3382
Character count: 18236

Detection of Frauds for Debit Card Transactions at Automated Teller Machine in Indonesia Using Neural Network



Detection of Frauds for Debit Card Transactions at Automated Teller Machine in Indonesia Using Neural Network

rmatita[1] , Indrajani Sutedja[2*]
[1] Informatics Department, Sriwijaya University, Inderalaya, Indonesia
[2*]Information Systems Department, School of Information Systems, Bina Nusantara University, Jakarta 11480, Indonesia
ermatitaz@yahoo.com, indrajani@binus.ac.id

Abstract. Fraud detection in an online banking transactions such as in Automated Teller Machine (ATM) is one of the important strategy implemented by banks to protect customer's account. Fraud detection requires a lot of investments, complex algorithms, training and testing. Fraud destroy the reputation of banks, loss of financials, and loss of the country's finances. This research is conducted in order to propose a model using neural network and data mining to detect fraud in debit card transaction. Neural network can be used as a benchmark to develop a logistic regression model in data mining. The evaluation of performance classifier (accuracy, sensitivity and specificity) in this research showed that the proposed model predicted class label tuple correct (76.3%). The result supports fraud analysis in debit card transaction in ATM. In conclusion the results show that the model has a good performance in detecting fraud in a debit card transaction.

1 Introduction

Debit Card is an electronic payment card issued by banks to replace cash payment, is widely used in many countries. Debit card payment can be used in several transactions such as cash withdrawal, tranfers, payments, purchases, balnce information, registration, change pin, top up[1, 2]. This card also functions as a replacement for cash payment. This card refers to the balance in the issuing bank. The functionn of debit card is to facilitate payment during shopping without having to bring cash. In several cases, the primary account number is given exclusively to be used in the internet and no requirement for the physical card. In Indonesia for example, the availability of ATM and the merchant receiving the ATM card contributed to the popularity of debit card such that ATM transactions becomethe main banking transactions [3]. Due to this condition, the number of fraud increases.

Fraud is an illegal act for the purpose of getting service, goods and money. In the last decade, fraud include several illegal practices and illegal acts. The main causes of information theft are skimming, card traps, PIN sharing, social engineering, fake call center and card informatino theft [4].The actor of fraud maybe imitating good customers and uses several bank transactions to perform illegal act.

Fraud has caused massive financial losses, loss of data, destroying the reputations of financial institutions [5]; Therefore as aneffort and initiatives, it is important to be able to identify fraud transactions. Several statistical model have been proposed to identify transaction frauds [7, 8, 9]. Studies include using actual data transactions, a combination of actual data set and syntetics [6],or the low level of communication packets from ATM to ATM Server [7].

This research is conducted in order to propose a model using data mining and neural network to detect frauds on debit card transactions.The differencen of this research with previous reseaches is mainly: (1) the actual dataset of debit cardtransactions such that empirical results represent the actual condition.; and (2) classification model model do not require complex training phase thus this model is easier to adapt to the flow of debit card transaction with unbalance class distrbution.

2 Literatue Review

2.1 Debit Card

Debit card used generally consis of magnetic stripe. Magnetic stripe has a disadvantage, that is can be easily copied using skimmer card and then swiped and transfer information to a new card [10]. Developers need to finda way to increase the security of the cards.

Some researchers claimed that the above weakness has been resolved by not using magnetic stripe, however others thinks that with a large database ther is a way to detect and analyze to improve the weaknesses. A probable solution is using multitrack recording. This scheme encode two different data set in in one magnetic strip. Industries can develop theur own standards. Using three tracks is also possible [10].

Magnetic stripe is a tape at the back of a bank card. This stripe is composed of a thin magnetic particles embedded in the card [10].

Operation Process. During encoding process, the North and South end are filled with magnetic particles. All characters on the magnetic stripe is converted to binary numbers, a set of 1 and 0. The magnetic polarity is adjusted to represent each bit. Adjusting the magnetization of each particle on the stripe is a way to encode binary information where it will be decoded by appropriate reader [10].

Coersivity. Coersivity is the intensity of the magnetic field that is necessary to magnetize data into the magnetic stripe. There are two types of magnetic with different coersivity: Magnetic stripe HiCo (High Coersivity) provide a higher security towards damage and LoCo (Low Coersivity) which is more sensitive to third party magnetic field but more economical [10].

2.2 Methods of data thefts

First of all, criminals will identify the target and identify the information on PIN and name onthe debit card followed by duplicating the data and insertit into a new card that is designed to resemble the actual card. There are several ways to obtain the victims PIN [2, 3, 4]:

1. The subject peeks on the target victim who is performing a transation in ATM. This action occurs in the mall or bank lobbies, where the subject pretends to be in the queue behing the targeted victim where the ATM is in open space.
2. The subject places a small camera (spycamera) and a card reader on the ATM. The card reader is to record from the ATM's magnetic stripe while the camera records the PIN
3. The method to obtain data from ATM debirt card is
    1. By reading the last record on the ATM. This method is more difficult and more risky. The subject develop an electronic card formatted to read the last transation on the machine.
    2. Data obtained from skimming, recording the data electronically on the magnetic stripe. This can be performed using a small device of the size of a cigarette pack and the subject places this device in Restaurants, Hotels involving inside man such as the cashier. The cashier would swipe twice, one for the real transaction and one on the skimmer which is placedunder the desk.without the owners' knowledge.
    3. Another mehod is to add some kind of chip in an POS (**point of sale**) terminal which is a card swiper, The crime is committed by the cashier or the operator in the POS terminal. The chip is placed by the POS technician during maintenance.

2.3 Neural Network

It is called neural network because the design follows how the brain functions and sores information. The human brain comprises of thousands of neurons. Each neuron has a simple design. Neural network consist of nodes combined by inputs (variables from a database or output from other nodes). This node can be classified from three simple layer, the input layer, output layer and middle layer [11], [14], [16], [18,19, 20, 21, 22, 23, 24, 25].

First, a simple logistic model is created showing a simple neural model and in this case, it does not consume too much time to design a better model using logistic regression.In practice, neural network is to model a non linear statistical model. Neural network can be used to model a complex relationship between input and output in order to obtain a data pattern. Neural network essentially contains three parts: architecture and model, learning algorithm and activation function [13,14].

2.4 Comparison of algorithms used in data mining

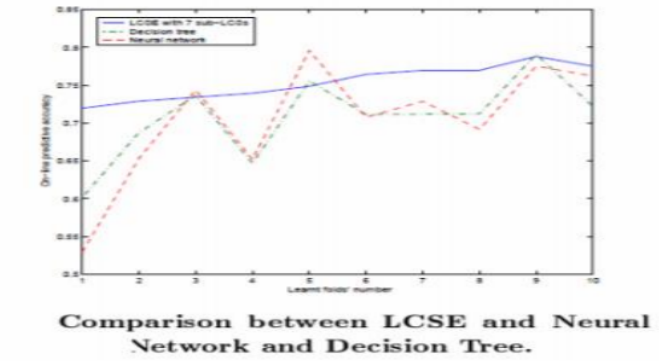


Fig. 1. LCSE, Neural Network and Decision Tree. (Source: Gao, Y.)[15]

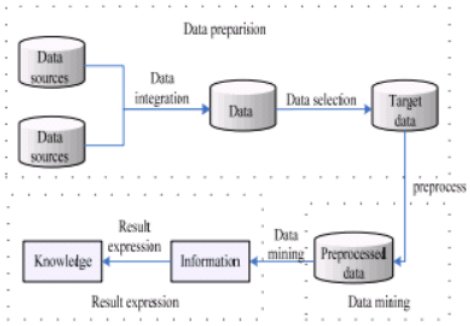


Fig. 2. General data mining process (Source : Ni, Xianjun) [17]

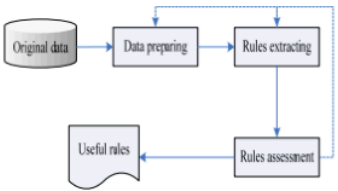


Fig. 3. Data mining process based neural network (Source : Ni, Xianjun) [17]

There are several algorithms for data mining. In this paper, a comparison of learning classifier system, neural networks and decision tree is performed. The Learnning Classifier system used is the LCSE algorithm, also known as Learning Classifier System Ensemble, which combines learning classifier with ensemble learning. The figure below shows the learning comparison of LCSE, decision tree, and neural network. Represented by solid blue line is LCSE, dashed blue line is the decision tree and the red dashed line shows neural network [15].

There are hundeds of data mining based on neural network. However, only two are most widely used. This is based on self-organizing neural network and fuzzy neural network. [17]

2.5 Neural Networks in Data Mining

Neural network are not linear. They are used to develop a model which is non-linear and complex. It can also be used to identify patterns from a set of data. Firms dealing with data warehouse extracts information via neural network tools. This process is knwn as data mining.
Information obtained by data mining helps user to make decisions. Neural network is composed of three parts: the architecture, the learning algorithm and the activation functions. Using Neural Network datasets are "trained" in a way to finally able to retrieve patterns used to solve complext combinatorial problems. Through the process, able to filter noise and recognize patterns. Dataset grows in time, in fact nowadays data sets are humungous in size, making it a necessity to automate the process. Using neural network, it provide data mining with functions in an uncountable ways [18,19, 20, 21].

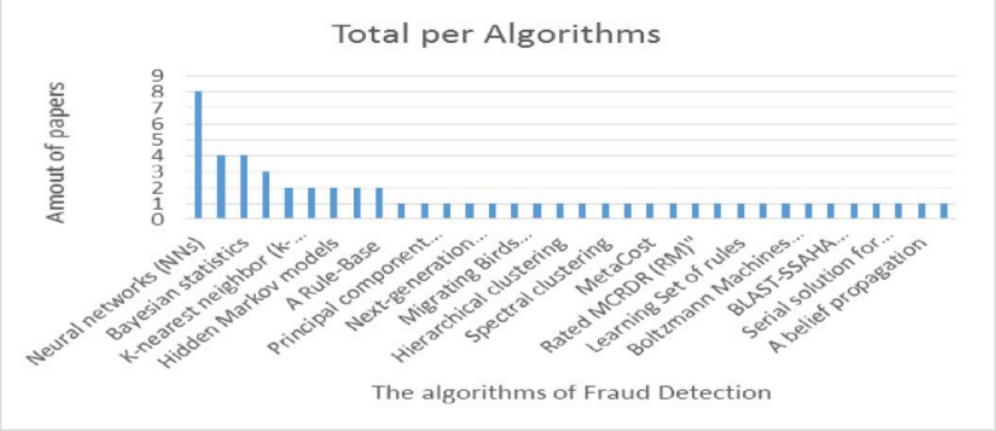


Fig. 4. Algorithms of Fraud Detection from Big Data based on analyzed literature frequency (Source: Indrajani, Prabowo, H.,Meyliana)[12]

3 Method

3.1 Dataset

Dataset for this research consists of a sample set representing debit card transaction from a number of ATM. Data is obtaied from the data warehouse from a commercial bank in Indoesian with permission. Unfortunately it is mot permissibile to release the bank's name. The dataset contains 6.820 transactions, from 60 samples of debit cards, consisting of 4.881 non-fraud transactional data and 1.939 fraud data from March, April, and May 2016. The debit card samples are selected at random from the database. The relationship among entities in the transactions can be seen in Diagram 2. For simplicity, the transaction is limited to the transactions executed in ATM with no relation payment transactions. It contains 51 variable with the following descriptions:

- Card Holder' Profile e.g. gender, age, etc.
- Transaksi entities e.g: amount, date, time.
- ATM entitas e.g.i: ATM location, machine, barand, type, etc.

Assumtion is made that fraudand non-fraud transaction.can be executed using either the same or different ATM.

3.2 Data Preprocessing

The objective of data preprocessing is to prepare debit card transaction standardsso thatit can be analyzed quantitatively. The data processing involves thefollowing:1). Data computation aggregate: frquency and accumulated amount of transaction from each debit card sample and category of the tendency of executing transactions fromthe last 3 months.

2). Quantization of non-numerical data: converting non-numerical data into numeric. For example binary varaible "yes" and "no" is converted to "1" and "0" respectively.

3.3 Feature Selection

Finding feature in order to reduce datadata dimension (variable) by selecting thekey vaiable from the debit card transactions that is relevant for analysis. In this research, 23 key variables are selected, such as deit cardor not, age category, transanction category, custoer category, account category, kiosk category, trend category. All variables are quantized.

3.4 Cross-Validation

Cross-validation used is cut-out technique so that 80% of the dataset is used for training and 20% of the dataset for testing. The classifier performance is tested using accuracy test.

4 Results

There are some important factors in the implementation of neural network in data mining:

a. The effective combination between Neural Network and Data Mining generally obtained using a neural network software or transforming to an existing neural network. Data model and other interfaces are developed using standardized form such that the two technologies are integrated effectively.

b. The combination between knowledge process and neural computation is used to evaluate whether a data mining algorithm works well or not. The following are the indicators and caharacteristics: (1) high quality with noise condition and data is not processes completely, (2) the model must be accepted by the user and is utilized for managerial decision; (3) the model is able to gain knowledge and therefore improve the model.

c. Based on the consideration that the method using neural netwrok is complex, a software is required having relational database, multi-dimenisonal database and data warehouse must synergize with the requirement of data miming. A neural network with data mining is developed by preparing data, appropriate extraction rules and assessment rules.

From the flat file, debit card is filtered to identiy the fraud and non-fraud data. It is then merged with a flat file profile of the card holder. Process is executed from non-nominal into categories such as age_bin, vintage_bin, frek_bln and nom_bin. Then the data includes training and testing data, 80% for the training data, 20% testing data. This data is fed into the neural network (fig. 5.)

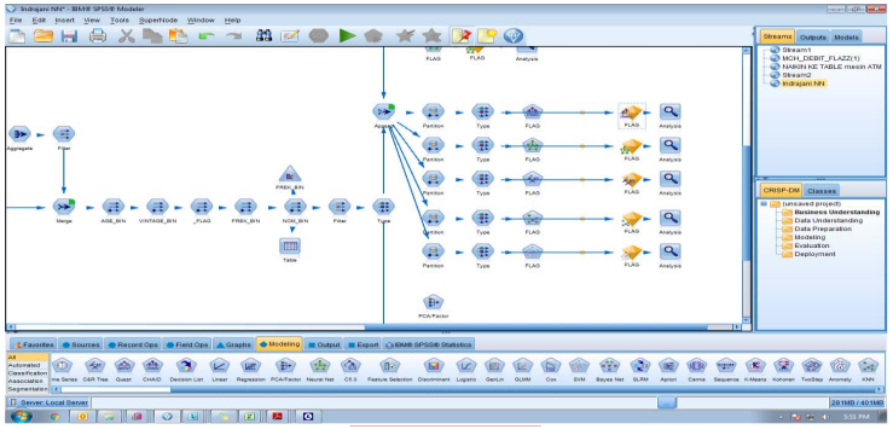


Fig. 5. Categorizing data

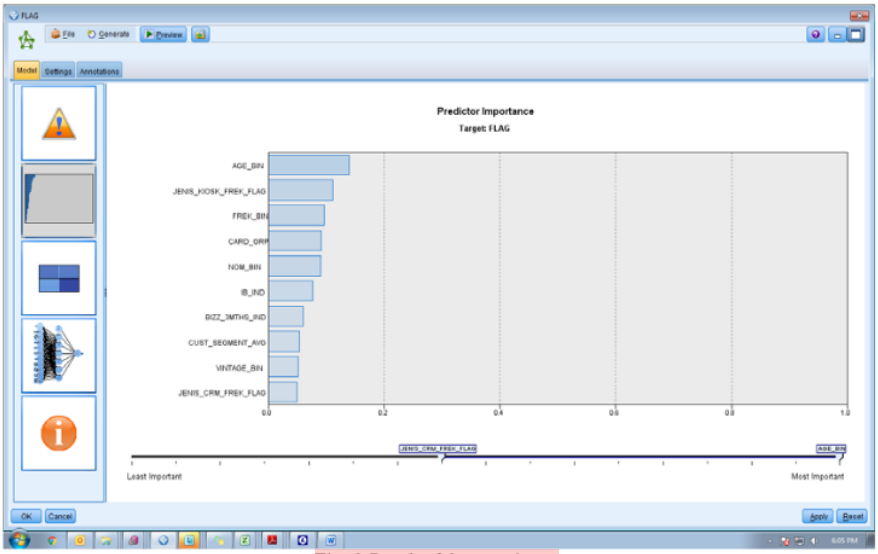


Fig. 6. Result of the experiment.

The result of the experiment is shown in figure 6. The predictor to identify fraud and non-fraud are age_bin, jenis_kios_frek_flag, frek_bin, card_grp, nom_bin, ib_ind, bizz_3mths_ind, cust_segment_avg, vintage_bin, and jenis_crm_frek_flag.

Figure 7 and 8 shows the neural network. Figure 9 shows the final result, where data is categorized by fraud and non-fraud, and the accuracy percentage.

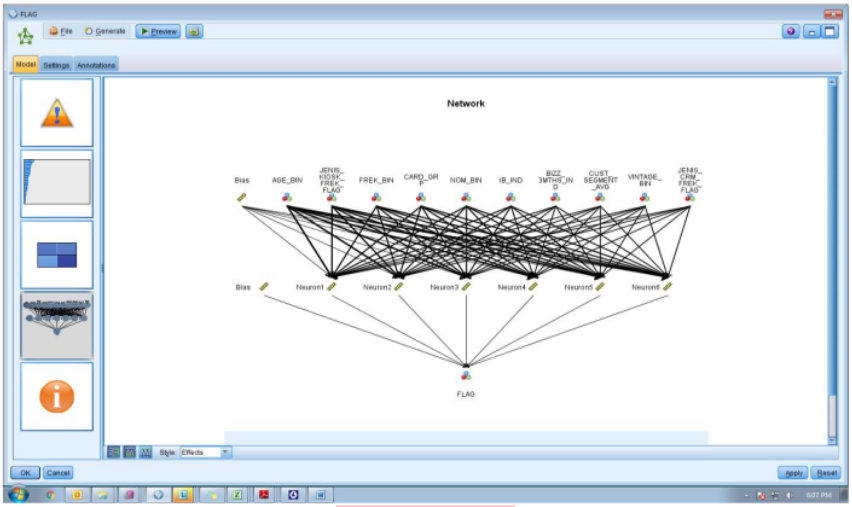


Fig. 7. Neural Network

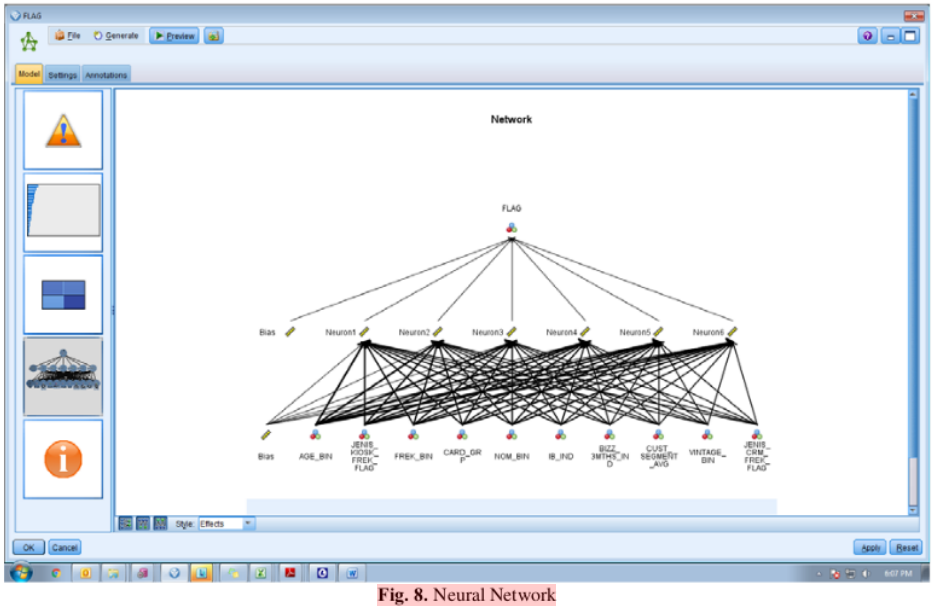


Fig. 8. Neural Network

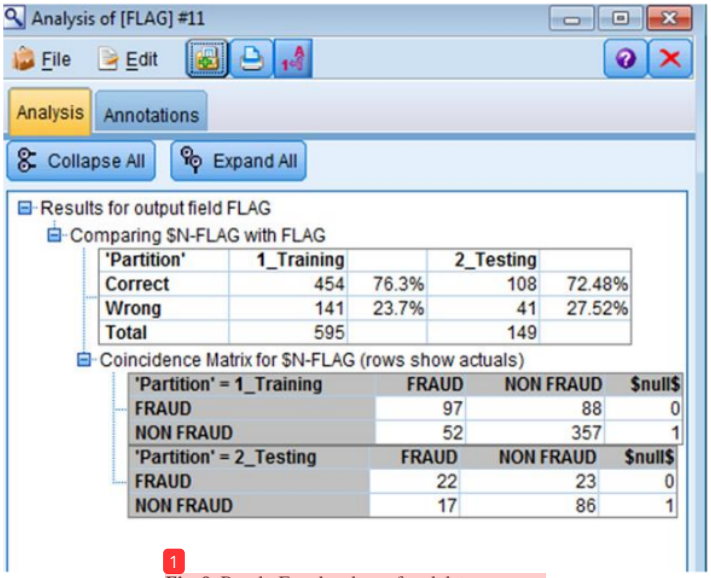


Fig. 9. Result: Fraud and non-fraud data accuracy

From figure 8 above, the training accuracy is 76.3 % and testing accuracy is 72,48%.

5 Conclusion

From some of the fraud cases occuring during debit card transactions, there are more factors and weaknesses in the existing system. The weakness of magetic stripe enabling it to be copied easily and easy for criminals to steal and duplicate cards. Security is improved by using chip. This chip is embedded into the card having more security because the chip uses many layered security.However, there are still methods that can be used by criminals to compromize the security of debit cards.

Data mining is appropriate to solve fraud problems because of the high accuracy, high tolerance to noise, independent to prior assumpsions and easy to process. Neural network can be trained using a large dataset and performed iteratively. Data mining becomes more useful by combining the strength of neural network and statistical tools. This combination is believed to provide a synergy and a good result. The Neural network provides a benchmark model. Since the result shows an accuracy of 76.3%, for future work a hybrid neural network with fuzzy or genetic algorithm might be a consideration to increase the accuracy percentage to above 98%.

References

[1] Case, P. and S. N. Sisat, "Secured Automatic Teller Machine (ATM) and Cash Deposit Machine (CDM)," vol. 7782, pp. 118–121, (2014)

[2] Bank Indonesia, "Mengenal Kartu Debit & ATM," pp. 1–2, (2009).

[3] Departemen Kebijakan Makroprudensial, "*Kajian Stabilitas Keuangan*," *Igarss 2014*, no. 1, pp. 1–5, (2014).

[4] Otoritas Jasa Keuangan, "*Bijak Ber-eBanking*," Bank Indonesia, (2015).

[5] Auditor General Western Australian, "Fraud Prevention and Detection in the Public Sector," pp. 1–24, (2013).

[6] Jog, Vivek V., and Nilesh R. Pardeshi. "Advanced Security Model for Detecting Frauds in ATM Transaction," *International Journal of Computer Applications 95*, no. 15, pp. 47-50, (2014).

[7] Anderka, M., T. Klerx, S. Priesterjahn, and H. K. Büning, "Automatic ATM Fraud Detection as a Sequence-based Anomaly Detection Problem," *Proc. 3rd Int. Conf. Pattern Recognit. Appl. Methods (ICPRAM 2014)*, (2014).

[8] Lepoivre, M. R., C. O. Avanzini, and G. Bignon, "Credit Card Fraud Detection with Unsupervised Algorithms," vol. 7, no. 1, (2016).

[9] Kass, G. V., "An Exploratory Technique for Investigating Large Quantities of Categorical Data," *Applied Statistics*, Vol. 29, No. 2, pp. 119–127, (1980).

[10] Svigals, J.;"The Long Life and Immenent Death of the Mag-Stripe Card"; *IEEE Spectrum*; (June 2012); 73-76

[11] M. Paliwal and U. A. Kumar: *Neural networks and statistical techniques* : A review of applications. Expert Syst. Appl., vol. 36, no. 1. (2009) 2–17

[12] Indrajani, Prabowo, Harjanto, Meyliana, "Learning Fraud Detection from Big Data in Online Banking Transactions: A Systematic Literature Review." *Journal of Telecommunication, Electronic and Computer Engineering (JTEC)* 8.3 (2016): 127-131.**ISSN 2180-1843 e***ISSN 2289-8131*

[13] Ainslie, A., and X. Dreze. "Data Mining: Using Neural Networks as a Benchmark for Model Building." *Decisions Marketing* (1996).

[14] Cheng, Jianlin, Zheng Wang, and Gianluca Pollastri. "A neural network approach to ordinal regression." *2008 IEEE International Joint Conference on Neural Networks (IEEE World Congress on Computational Intelligence)*. IEEE, (2008).

[15] Gao, Yang, et al. "Learning classifier system ensemble for data mining." *Proceedings of the 7th annual workshop on Genetic and evolutionary computation*. ACM, (2005).

[16] Singh, Yashpal, and Alok Singh Chauhan. "Neural networks in data mining." *Journal of Theoretical and Applied Information Technology* 5.6 (2009): 36-42.

[17] Ni, Xianjun. "Research of data mining based on neural networks." *World Academy of Science, Engineering and Technology* 39 (2008): 381-384.

[18]. Zhang, G. Peter. "Neural networks for data mining." *Data mining and knowledge discovery handbook*. Springer US, (2009). 419-444.

[19] Craven, Mark W., and Jude W. Shavlik. "Using neural networks for data mining." *Future generation computer systems* 13.2 (1997): 211-229.

[20] Gaur, Priyanka. "Neural Networks in Data Mining." *International Journal of Electronics and Computer Science Engineering* 1.3 (2013).

[21] V]enkateswarku, Vuggam, B. Chinna Subbana and M. Kalyana Chakravarthy. "Neural Networks for Data Mining." (2014).

[22]. Mukkamala, Srinivas, Guadalupe Janoski, and Andrew Sung. "Intrusion detection using neural networks and support vector machines." *Neural Networks, 2002. IJCNN'02. Proceedings of the 2002 International Joint Conference on*. Vol. 2. IEEE, (2002).

[23]. Patidar, Raghavendra, and Lokesh Sharma. "Credit card fraud detection using neural network." *International Journal of Soft Computing and Engineering (IJSCE)* 1.32-38 (2011).

[24]. Lee, Walter W., et al. "Identification and management of fraudulent credit/debit card purchases at merchant ecommerce sites." U.S. Patent No. 8,065,233. (22 Nov. 2011).

[25]. Barraclough, P. A., et al. "Intelligent phishing detection and protection scheme for online transactions." *Expert Systems with Applications* 40.11 (2013): 4697-4706.

Detection of Frauds for Debit Card Transactions at Automated Teller Machine in Indonesia Using Neural Network

ORIGINALITY REPORT

97%	18%	97%	12%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Ermatita, Indrajani Sutedja. "Detection of Frauds for Debit Card Transactions at Automated Teller Machine in Indonesia Using Neural Network", Journal of Physics: Conference Series, 2019 Publication	89%
2	Submitted to President University Student Paper	6%
3	Hui Xia, Hui Ma. "A Novel Structure-based Feature Extraction Approach for Financial Fraud Detection", Journal of Physics: Conference Series, 2021 Publication	1%
4	iopscience.iop.org Internet Source	1%
5	Indarti, Inova Fitri Siregara. "Accountant's Perception on Fraud Detection in Financial Statement Reporting Using Fraud Triangle Analysis", IOP Conference Series: Earth and Environmental Science, 2018	1%

Publication

Exclude quotes	On	Exclude matches	< 1%
Exclude bibliography	On		