Syntax Literate: Jurnal Ilmiah Indonesia p–ISSN: 2541-0849 e-ISSN: 2548-1398
Vol. 8, No. 6, Juni 2023

FRAUD DETECTION FOR ONLINE INTERBANK TRANSACTION USING DEEP LEARNING

Leshivan Savenjer Hasugian, Suharjito
Computer Science Department, BINUS Graduate Program–Master of Computer Science
Bina Nusantara University Jakarta, Indonesia
Email: leshivansav@gmail.com, suharjito@binus.ac.id

Abstract

The World Banking with its various financial services is an easy target for fraudsters to carry out their actions. Various kinds of fraud that occurred such as credit card fraud, online payment fraud, debit card fraud, online transaction fraud, e-commerce fraud and other services including interbank online transactions. Fast and reliable fraud detection is important because many financial losses have occurred due to fraud. The objective of this study is obtaining a more effective deep learning model for fraud detection in the interbank online transaction system compared to similar models. This study using CNN, LSTM and hybrid model CNN-LSTM models are used to build an interbank online transaction system. The proposed model CNN consist of three convolution layer, one maxpooling layer, one dropout layer and one fully connected layer. The proposed model LSTM built by double layer LSTM with each layer consist 32 cell LSTM, dropout layer and one fully connected layer. The proposed model CNN-LSTM built by combination three convolution layer, 1 maxpooling layer, dropout layer, 1 LSTM layer with 64 LSTM cell and one fully connected layer. The Dataset taken from an interbank online transaction in March 2021 from one of the switching company in Indonesia. SMOTE is use to overcome the imbalance Dataset in training and validation Dataset. The Dataset contains 279513 transactions with 2374 transactions categorized as fraud. The results showed that the CNN model scored an F1-score value at 93,09%, followed by the LSTM model at 86,25% and the CNN-LSTM hybrid model at 69,22%. Based on these results, the proposed CNN model can be accurate for fraud detection in interbank online transaction systems compared to similar models.

Keywords: *CNN; LSTM;SMOTE; Confusion Matrix; F1-score; Interbank transaction; fraud*

Introduction

Interbank online transactions consist of transaction balance inquiry, transaction cash withdrawal and electronic fund transfers (EFT) (Afaha, 2019). Electronic fund transfer has been used since late 1960s. People in that era using EFT for paying university fees through the banking automatic teller machine (ATM) network, Paying telephone bills and Interbank fund transfer with large value (Mamudu, 2021). Interbank online transaction

How to cite:	Leshivan Savenjer Hasugian, Suharjito (2023) Fraud Detection for Online Interbank Transaction Using Deep Learning, *(8) 6,* http://dx.doi.org/10.36418/syntax-literate.v6i6
E-ISSN:	2548-1398
Published by:	Ridwan Institute

comes to Indonesia in early 2000s which the foundation of interbank online transaction via switching in Indonesia. Interbank online transactions are currently spreading in Indonesia with the growth of e-commerce and financial technology in Indonesia (Trisnowati, Muditomo, Manalu, & Adriana, 2020). The growth of e-commerce comes from payment gateway, the catalyst of e-commerce growth with easier payment via debit card, credit card, online banking purchases and transfer of electronic funds (Kim & Kim, 2022). It leads interbank online transactions to increase significantly.

According to Bank Indonesia statistical data from 2009 to 2021 (Figure 1) there was a very significant increase in interbank transactions and interbank transactions using debit card or credit card especially between 2018 - 2021. Between 2017 – 2018 there is an increase in interbank transaction volume of 18,5% and interbank transaction value of 13.29%.

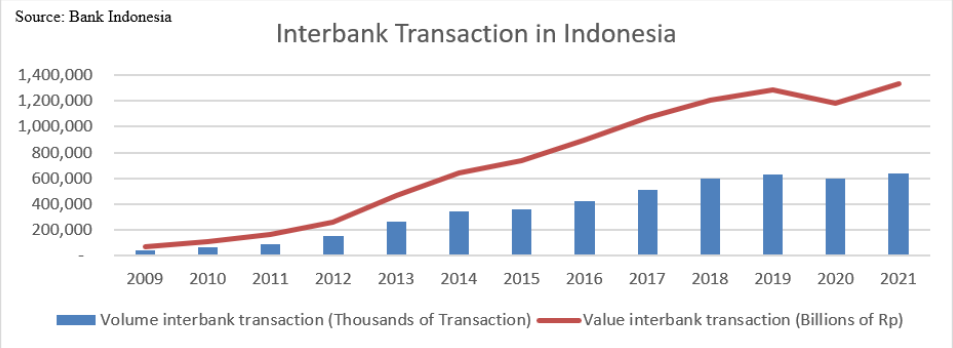


Figure 1
Trend of Interbank transaction in Indonesia

Behind the increase in interbank transactions, there is fraud lurking. Fraud is anything that can be thought of and attempted by a person to take advantage of another person in a dishonest way that causes the other person to be deceived (Consalvo, 2009). There are many modes that people use to commit fraud, ranging from skimming, phishing, keyloggers, password theft and card data theft (Malik, 2013). As a result, many victims suffered significant financial losses. Many companies in financial sector make fraud detection to overcome this. But, with advances in technology, fraud is predicted to increase in the future (West & Bhattacharya, 2016). Companies in financial sector must improve their fraud detection.

However, there are obstacles in building a fraud detection model, namely the amount of fraud data is very little, the availability of data due to privacy policies, features in transactions that are not standardized (Mittal & Tyagi, 2020). According to (Heryadi & Warnars, 2017), many studies in fraud transaction recognition to develop a robust classifier that maximize classification accuracy and minimize two aspects: (1) false positive where transaction genuine to fraud that make loss for customer, merchant and banks, and (2) false negative where transaction fraud to genuine that ruined the image of bank.

Machine learning techniques are applied for fraud detection in the past with various classification models and anomaly detection models (Alghofaili, Albattah, & Rassam, 2020). The Random Forest classification model Random-Tree and CART, OCSVM, Adaboost, Local outlier factor and isolation forest, and also k-NN, was used to build the fraud detection model. But nowadays with the advanced of deep learning techniques and many used in some area of research. Deep learning techniques also widely used nowadays for anomaly detection or intrusion detection include fraud detection with CNN and LSTM model (Elsayed, Le-Khac, Jahromi, & Jurcut, 2021).

Another model like hybrid CNN-LSTM, GAN, GNN and GRU also used to develop fraud detection. The high performance in Image Processing, Text Classification and also better learning and performance when there are many data input (Chen, Ubul, Xu, Aysa, & Muhammat, 2022). In this research, Deep learning was chosen to develop fraud detection in interbank online transaction.

The dataset used in this study uses a dataset of transaction data through switching in Indonesia in the period March 2021. The models that will be used are using Deep Learning model, likes CNN, LSTM, CNN-LSTM. The benchmark used to measure performance of model is the Confusion Matrix by focusing on the accuracy, precision, recall, F1-Score values and AUC. The paper is organized into following sections: related works include literature review, research method, results and conclusion.

Research Method

Fraud detection is one of the problems that using an outlier detection (Vanhoeyveld, Martens, & Peeters, 2020). Fraudulent transactions are also identified as outliers or anomalies because the transactions are of large value or the transactions are carried out many times or the transactions carried out are not like customers in general (Sharmila, Kumar, Sundaram, Samyuktha, & Harish, 2019). These transactions can be identified as outliers/anomalies. In this research, for outlier detection we using CNN, LSTM, CNN-LSTM because many researchers conduct using this and produce evaluation result with superior than some machine learning for outlier detection like Random Forest and SVM (Elmrabit, Zhou, Li, & Zhou, 2020).

1. Data Collection

The data taken using the guidelines of the ISO8583 Standard in 1987. Standard ISO 8583:1987 is a standard used in the banking and payment industry to communicate between financial institutions like banks, payment points, billers or card principals. The ISO8583:1987 standard is widely used for ATM (Automated Teller Machine) and POS (Point of Sale) transactions. The ISO8583 formatted message is an alphanumeric dataset arranged according to certain rules and read according to certain rules according to the rules of ISO8583.

In ISO8583:1987, there are data with various kinds of information such as information from the card (PAN, expiry date), the terminal (transaction number, merchant data) and transaction value(amount) to the destination account number. This research using data from private switching company in Indonesia. This data contains

sensitive customer information such as card numbers so it needs to be transformed to maintain customer confidentiality. The research data is divided into two class, namely non-fraud transaction and fraud transaction.

This dataset was created by the author with combine from transaction table and fraud table. The dataset contains online interbank transactions that occurred in March 2013. A total of 279.513 data transactions with 0.869% or 2409 transactions were identified as fraudulent transactions. There 9 features in this dataset which describe in Table 2. In this dataset, feature retrieval_ref_nbr and switch_trml_id have value with alphanumeric. This feature must be convert to numeric with help String to bytes converter before it become the input data for the model.

Table 1
Feature Description

Feature	Description
PAN	Number of Card when transaction is held
AMOUNT	Amount of Transaction
PROC_CODE	Code of Transaction for withdrawal, balance inquiry, transfer inquiry and transfer
TRAN_TIME	Time of Transaction
ORIG_TRAN_DATE	Date of Transaction
MERCHANT_TYPE	Channel / Terminal where customer held transaction
ABA_ACQUIRER	Bank code of Terminal
RETRIEVAL_REF_NBR	Unique code for transaction
SWITCH_TRML_ID	Terminal Code

2. Oversampling Data

The dataset used for training and testing in this study is very unbalanced between non-fraud and fraudulent transactions. Figure 6 illustrated how imbalance between class fraud and non-fraud. The imbalanced dataset will make the deep learning model to be trained less accurate and less perform. This problem can be avoided by using oversampling data. SMOTE (Synthetic Minority Oversampling Technique) is one of the most popular oversampling techniques. SMOTE interpolates sample to generate new instances. Saputra using SMOTE to overcame the imbalanced dataset problem. The experiment showed increasing in value of recall, F1-score and G-mean. SMOTE make data fraud and non-fraud is balanced like showed in Figure 7. Hopefully, the model we proposed can identify fraudulent and non-fraud transactions more precisely.

3. Proposed Model

Three different model were conducted to train and testing model. The proposed model are CNN, LSTM, and CNN-LSTM which based on literature review is the best model to make fraud detection. Model CNN and LSTM comes from research by (Nguyen, Tran, Thomassey, & Hamad, 2021). Nguyen use double convolution layer with dropout and maxpooling layer. The result are spectacular with accuracy score 99% and F1-score 78%. Nguyen et al also using LSTM to make fraud detection which perform well than CNN. In his model, the LSTM using single layer with 50 LSTM

cell. The result comes with 99.5% in accuracy and 84.85 in F1-score. In his research, the dataset using ULB dataset credit card fraud detection. which is commonly used to build fraud detection model.

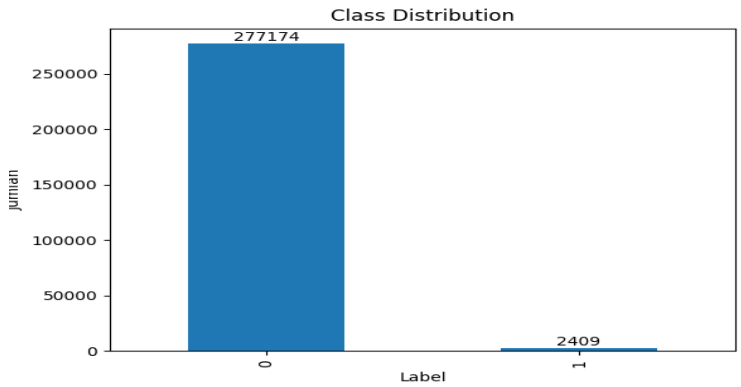


Figure 2
Fraud and non-fraud before SMOTE

Figure 3
Fraud And Non-Fraud After SMOTE

Another research for fraud detection using model CNN-LSTM to detect fraud detection. (Heryadi & Warnars, 2017) et al using data historical debit card transaction from local bank in Indonesia from 2016-2017. The model consists of 2 convolution layer with each layer have maxpooling, LSTM with 100 layer and Dropout with Batch Normalization layer between CNN and LSTM layer and LSTM layer with output. The research scored AUC with 77.5 % using CNN – LSTM outperform CNN and SLTSM with each model score 72%.

Based on research above, The Model CNN we proposed using triple convolution layers to aim make model better to classify fraud and non-fraud transaction. The model also using dropout layer to prevent the model overfitting. In model LSTM using double stacked layer to make difference approach for LSTM model. For model combination CNN-LSTM, 3 convolution layer and 1 LSTM layer. For this research using fixed hyperparameter to ensure the model can perform well to detect fraud transaction. Table

3 show hyperparameter that this research using and Table 4 illustrated the architecture model we proposed.

Table 2
Hyperparemeter Value

Parameter	Value
Epochs	100
Optimizer	Adam
Batch_size	32
Loss Function	Binary_crossentropy
Learning Rate	10 e-3
Validation Split	0.3

4. Evaluation Model

This is the final stage to find out how far the model we have made. The Testing dataset that has been shared in the data sharing process is used here. The evaluation of the model is carried out using the Confusion Matrix method which is commonly used for the evaluation of machine learning classification. The table confusion matrix is show in Table 3.

Table 3
Confusion Matrix

Class	Actual Positive	Actual Negative
Predictive Positive	True Positive (TP)	False Positive(FP)
Predictive Negative	False Negative (FN)	True Negative (TN)

After obtaining the values in the Confusion Matrix Table, the next step is to find the accuracy value. Evaluation with accuracy value is generally carried out to measure the accuracy of the model being trained when using the training dataset. Accuracy meaning ratio between the number of correctly classified samples and the overall number of samples. In addition, the F1-Score also measured to measure the recall and precision values. F1-score defined as the harmonic mean of precision and recall. The formula to compute accuracy and F1-score as follows:

$$\boldsymbol{Accuracy} = \frac{\boldsymbol{TP+TN}}{\boldsymbol{TP+TN+FP+FN}} \quad (1)$$

$$\boldsymbol{Recall} = \frac{\boldsymbol{TP}}{\boldsymbol{TN+FP}} \quad (2)$$

$$\boldsymbol{Precision} = \frac{\boldsymbol{TP}}{\boldsymbol{TP+FP}} \quad (3)$$

$$\boldsymbol{F1-score} = \frac{\boldsymbol{2\ x\ Recall\ x\ Precision}}{\boldsymbol{Precision+Recall}} \quad (4)$$

Last to evaluate the model, using AUC score. ROC is a two-dimensional curve that plots the false positive rate (FPR) as horizontal axis against the true positive rate (TPR) as vertical axis. TPR and FPR formula to compute as follows:

$$\boldsymbol{TPR} = \frac{\boldsymbol{FP}}{\boldsymbol{FP+TN}} \quad (5)$$

$$\boldsymbol{FPR} = \frac{\boldsymbol{TP}}{\boldsymbol{TP+FN}} \quad (6)$$

Area under the ROC curve (AUC) is a scalar value whose value between 0 and 1 which to score perfomance of classifier. The statistical property of AUC is equivalent to probability that the classifier will rank a randomly selected positive sample higher than a randomly selected negative sample. The higher AUC value, the higher performance of the model.

Table 4
Proposed Model Architecture

CNN	**LSTM**	**CNN-LSTM**
Conv1D Layer Number of Channels = 64 Kernel Size = 1 Activation Function = ReLU	**LSTM Layer** Number of LSTM blocks = 32 Activation Function = Tanh	**Conv1D Layer** Number of Channels = 32 Kernel Size = 1 Activation Function = ReLU
Conv1D Layer Number of Channels = 64 Kernel Size = 1 Activation Function = ReLU	**LSTM Layer** Number of LSTM blocks = 32 Activation Function = Tanh	**Conv1D Layer** Number of Channels = 64 Kernel Size = 1 Activation Function = ReLU
Conv1D Layer Number of Channels = 64 Kernel Size = 1 Activation Function = ReLU	**Dropout** Threshold = 0.5	**Conv1D Layer** Number of Channels = 96 Kernel Size = 1 Activation Function = ReLU
Dropout Threshold = 0.5	**Dense** Number of Nodes = 64 Activation Function = ReLU	**MaxPooling** Pool Size = 1
MaxPooling1D Pool Size = 1		**LSTM Layer** Number of LSTM blocks = 64
Flatten Number of Nodes = 64		**Dropout** Threshold = 0.5
Dense Number of Nodes = 64 Activation Function = ReLU		**Dense** Number of Nodes = 32 Activation Function = ReLU
Output Number of Nodes = 1 Activation Function = Sigmoid	**Output** Number of Nodes = 1 Activation Function = Sigmoid	**Output** Number of Nodes = 1 Activation Function = Sigmoid

Result and Discussion

1. Hardware Specifications

In this experiment, the hardware to computing model Deep learning must have high-end specifications. Deep learning need more compute to train and test which need some high-end hardware to compensate that. If the experiment using low-end hardware, it will make the computation really show and effect to performance of model (Sankhe et al., 2019). Some option like using GPU is approach if the CPU is not enough

to do computation, like very slow CPU or not enough memory. In this study used computing devices with the following specifications like Table 5.

Table 5
Hardware specifications

Part	Specifications
CPU	Intel Core i7-11800H 2.3 GHz
RAM	16 GB DDR4
GPU	NVIDIA GeForce RTX 3060
GPU Memory	6GB VRAM GDDR6
Cuda Core	3840
OS	Windows 10

On the software side, this research uses python programming language supported by keras libraries and tensorflow to create deep learning models. The IDE used is PyCharm 2021.3.2 with a student license for research.

2. Dataset

This dataset is then analyzed using the correlation matrix method. The result is that ORIG_TRAN_DATE and MERCHANT_TYPE features have a close relationship with class features with positive correlation values. It can be assumed that there is data in the feature that affects transactions including the category of fraud or not. Like many fraudulent transactions carried out on the same day and the same transaction channel. The correlation matrix image can be seen in Figure 8.

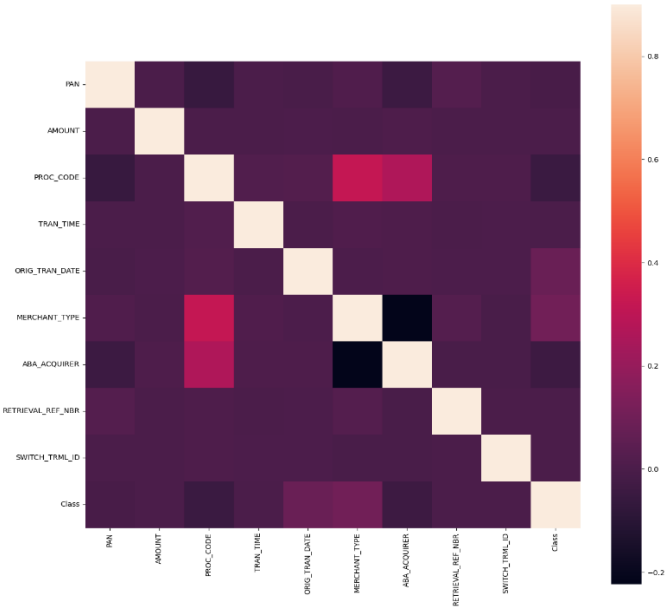


Figure 4
Correlation Matrix of Dataset

From the training results, the proposed CNN model produces an average training accuracy 99.14% with a range of testing accuracy values between 93% and 99.85%. The average training loss value is 0.0267 with a range from 0.0056 – 0.2004 in 100

epochs. When entered into the validation data, the average validation accuracy value is 99.36% with a range of validation accuracy values between 94.47% and 99.93%. The average loss validation value is 0.0198 with a range from 0.0029 to 0.1683 out of 100 epochs. The graph of the loss accuracy of training and validation for the CNN model can be seen in the figure 9.

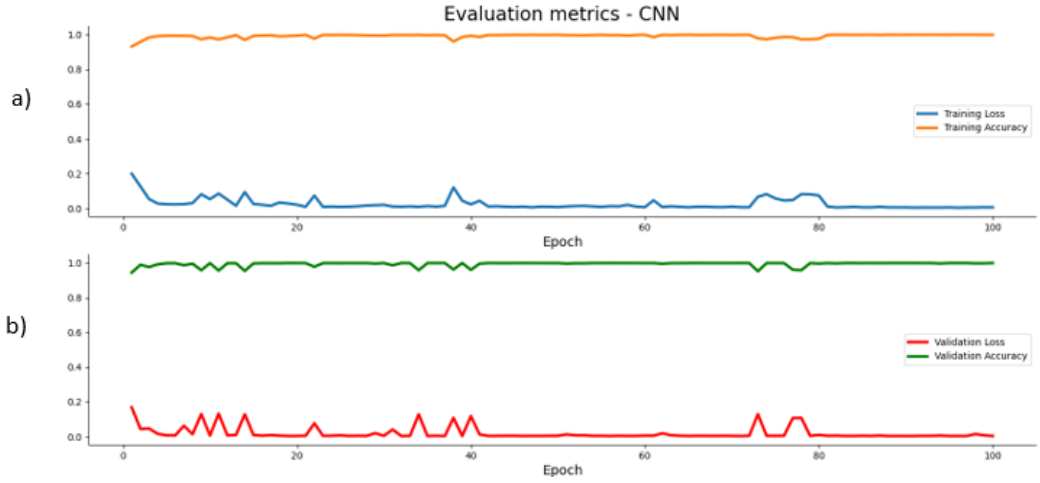
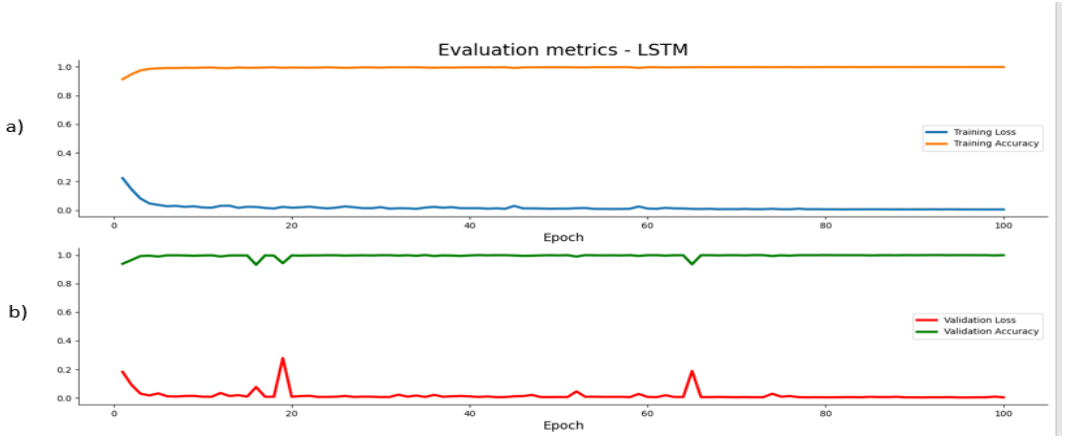


Figure 5

a) Graph loss accuracy CNN in training, b) Graph loss accuracy CNN in testing

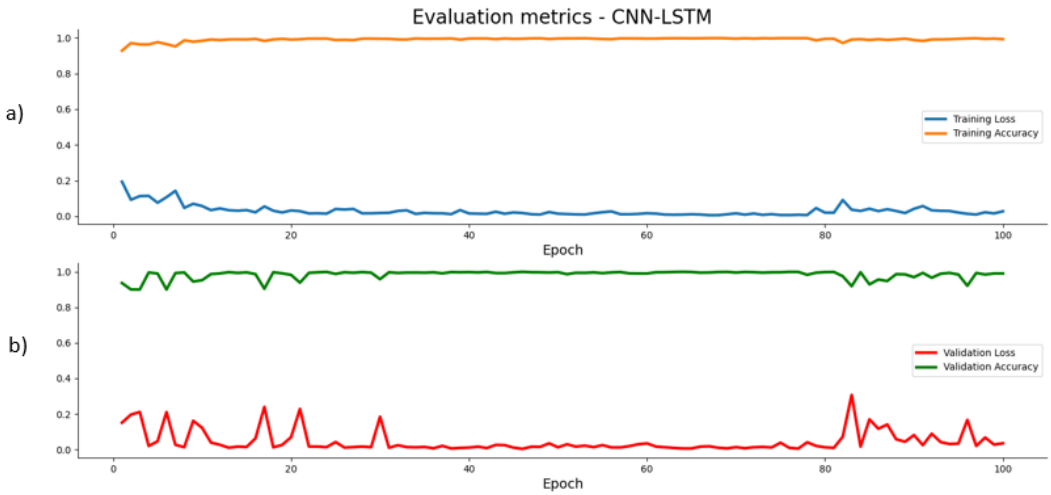
The proposed LSTM model produces an average training accuracy 99.44% with a range of training accuracy values between 91.33% and 99.83%. The average training loss value was 0.0177 with a range from 0.0053 – 0.2232 in 100 epochs. When entered into validation data, the average validation accuracy value is 99.41% with the validation accuracy value range between 88.63% and 99.92%. The average loss validation value is 0.0175 with a range from 0.0033 to 0.2789 out of 100 epochs. The graph of loss accuracy from training and validation for the LSTM model can be seen in the figure 10.

The CNN-LSTM model produces an average training accuracy value 98.58% with a training accuracy value range from 92.91% to 99.83%. The average training loss value is 0.0453 with a range of 0.0071–0.2212 in 100 epochs. When entered into



validation data, the average validation accuracy value is 97.59% with a validation accuracy value range from 87.61% to 99.93%. The average validation loss value is 0.0651 with a range from 0.0029 to 0.3972 out of 100 epochs. The loss accuracy graph of training and validation for the CNN-LSTM model can be seen in the figure 11.

Figure 6
a) Graph loss accuracy LSTM in training, b) Graph loss accuracy LSTM in testing
Figure 11



a) Graph loss accuracy CNN-LSTM in training, b) Graph loss accuracy b) CNN-LSTM in testing

After that, the model is carried out to tested using testing data. The purpose is to evaluate the model after training model. In this experiment, the model use confusion matrix to know how well the model we proposed perform. The confusion matrix will produce performance values in form of accuracy, F1-score and AUC which show in table 6.

Table 6
Performance Of Model

Model	Accuracy	Precision	Recall	F1-score	AUC
CNN (proposed)	99.88%	87.07%	100%	93.09%	99.94%
LSTM (proposed)	99.74%	75.83%	100%	86.25%	99.87%
CNN-LSTM (proposed)	99.28%	53.33%	98.69%	69.22%	98.99%

The results of the tests show that the CNN model produces the best performance value where the accuracy value is 99.88%, precision 87.07% recall 100%, F1-score is 93.09% and AUC is 99.94%. The second model developed using LSTM model obtained results under the CNN model where the accuracy value was 99.74%, precision 75.83%, recall 100%, F1-score 86.25% and AUC 99.87%. The last CNN-LSTM model has a lower value than CNN and LSTM where the accuracy value is 99.28%, precision 53.33% recall 98.69%, F1-score is 69.22% and AUC is 98.99%.

Another experiment is using architecture model from other research with dataset fraud online interbank transaction. Architecture CNN and LSTM take from experiment

by Nguyen et al and for model hybrid CNN-LSTM using architecture from Heryadi et al. From the test results, the Nguyen LSTM Model produces bad performance value with accuracy value is 99.67%, F1-score is 83.42% and AUC is 99.84%. However, the model CNN that only produces an accuracy value is 99.48%, F1-score is 57.97% and AUC is 71.81%. The interesting thing about this test is that the model CNN model produces low performance values when it is above epoch 46. After epoch 46, the model's performance value for accuracy is around 84%. When the epoch is below 46, the accuracy value is around 98%.

The CNN – LSTM model from Heryadi et al is testing using dataset fraud online interbank transaction. The results achievement is very poort with accuracy at 86.33%, F1-score at 10.7% and AUC at 93.11%. From the trial, it is concluded that Nguyen's LSTM model was still capable of building fraud detection for interbank online transactions.

This model can identify fraudulent transactions and genuine transactions well as evidenced by the excellent performance value, especially the F1-score performance value of 83.42%. The CNN model from Nguyen and the CNN-LSTM model from Heryadi resulted in poor performance from learning the fraud dataset of interbank online transactions. The comparison of model we proposed with Nguyen's CNN and LSTM and Heryadi's hybrid model CNN-LSTM can be seen in Table 7.

Table 7
Comparison Another Model with Dataset Fraud Online Interbank Transaction

Model	Accuracy	F1-score	AUC
CNN (proposed)	99.88%	93.09%	99.94%
CNN [11]	99.48 %	57.97%	71.81%
LSTM (proposed)	99.74%	86.25%	99.87%
LSTM [11]	99.67%	83.42%	99.84%
CNN-LSTM (proposed)	99.28%	69.22%	98.99%
CNN-LSTM [5]	86.33%	10.7%	93.11%

Conclusion

Based on the results of the above experiment, the CNN and LSTM proposed models tend to be stable in learning compared to the CNN-LSTM proposed model. The proposed CNN-LSTM model in several epochs spiked for low value loss and accuracy. These spikes indicate that there are times when the model produces low performance due to the less optimal model for learning with datasets of fraudulent online transactions between banks. The proposed model of CNN and LSTM which tends to be stable with more epochs carried out indicates that the proposed model of CNN and LSTM is optimal in studying the fraud dataset of interbank online transactions. But in the future research, the model can use optimization method to increase the performance model.

It was concluded that the application of SMOTE on CNN was able to handle the imbalance of credit card fraud detection dataset by producing higher F-1 scores and AUC using testing data. This proves that the SMOTE method is effective in increasing the performance of unbalanced data classification. The proposed model, CNN, gives very good results which can detect genuine and fraudulent transactions and can be used as

fraud detection for credit card transactions. Followed by model LSTM which the performance below CNN. On the other hand, the CNN-LSTM model has not given good results and needs to make layer adjustments to get optimal results in the next research.

BIBLIOGRAFI

Afaha, John Sylvester. (2019). Electronic payment systems (E-payments) and Nigeria economic growth. *European Business and Management*, *5*(6), 77–87.

Alghofaili, Yara, Albattah, Albatul, & Rassam, Murad A. (2020). A financial fraud detection model based on LSTM deep learning technique. *Journal of Applied Security Research*, *15*(4), 498–516.

Chen, Meikang, Ubul, Kurban, Xu, Xuebin, Aysa, Alimjan, & Muhammat, Mahpirat. (2022). Connecting text classification with image classification: a new preprocessing method for implicit sentiment text classification. *Sensors*, *22*(5), 1899.

Consalvo, Mia. (2009). *Cheating: Gaining advantage in videogames*. mit press.

Elmrabit, Nebrase, Zhou, Feixiang, Li, Fengyin, & Zhou, Huiyu. (2020). Evaluation of machine learning algorithms for anomaly detection. *2020 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*, 1–8. IEEE.

Elsayed, Mahmoud Said, Le-Khac, Nhien An, Jahromi, Hamed Z., & Jurcut, Anca Delia. (2021). A hybrid CNN-LSTM based approach for anomaly detection systems in SDNs. *Proceedings of the 16th International Conference on Availability, Reliability and Security, Vienna, Austria*, 17–20.

Heryadi, Yaya, & Warnars, Harco Leslie Hendric Spits. (2017). Learning temporal representation of transaction amount for fraudulent transaction recognition using CNN, Stacked LSTM, and CNN-LSTM. *2017 IEEE International Conference on Cybernetics and Computational Intelligence (CyberneticsCom)*, 84–89. IEEE.

Kim, Shee Ihn, & Kim, Seung Hee. (2022). E-commerce payment model using blockchain. *Journal of Ambient Intelligence and Humanized Computing*, *13*(3), 1673–1685.

Malik, Vanita. (2013). E-Threats And Internet Banking. *REVELATION*, 28.

Mamudu, Zebedee Udo. (2021). Electronic banking payment system and its impact on the Nigerian economy. *Journal of Emerging Trends in Economics and Management Sciences*, *12*(1), 8–26.

Mittal, Sangeeta, & Tyagi, Shivani. (2020). Computational techniques for real-time credit card fraud detection. *Handbook of Computer Networks and Cyber Security: Principles and Paradigms*, 653–681.

Nguyen, H. Du, Tran, Kim Phuc, Thomassey, Sébastien, & Hamad, Moez. (2021).

Forecasting and Anomaly Detection approaches using LSTM and LSTM Autoencoder techniques with the applications in supply chain management. *International Journal of Information Management*, *57*, 102282.

Sankhe, Kunal, Belgiovine, Mauro, Zhou, Fan, Angioloni, Luca, Restuccia, Frank, D'Oro, Salvatore, Melodia, Tommaso, Ioannidis, Stratis, & Chowdhury, Kaushik. (2019). No radio left behind: Radio fingerprinting through deep learning of physical-layer hardware impairments. *IEEE Transactions on Cognitive Communications and Networking*, *6*(1), 165–178.

Sharmila, V. Ceronmani, Kumar, Kiran, Sundaram, R., Samyuktha, D., & Harish, R. (2019). Credit card fraud detection using anomaly techniques. *2019 1st International Conference on Innovations in Information and Communication Technology (ICIICT)*, 1–6. IEEE.

Trisnowati, Yanuar, Muditomo, Arianto, Manalu, Erwin P. S., & Adriana, Dadi. (2020). The COVID-19 Pandemic's Impact on Indonesia's Electronic Retail Payment Transactions. *2020 International Conference on Information Management and Technology (ICIMTech)*, 504–509. IEEE.

Vanhoeyveld, Jellis, Martens, David, & Peeters, Bruno. (2020). Value-added tax fraud detection with scalable anomaly detection techniques. *Applied Soft Computing*, *86*, 105895.

West, Jarrod, & Bhattacharya, Maumita. (2016). Intelligent financial fraud detection: a comprehensive review. *Computers & Security*, *57*, 47–66.