ICIC Express Letters
Part B: Applications
Volume **14**, Number **7**, July **2023**

 ISSN 2185-2766
pp. 747–753

ARTIFICIAL INTELLIGENCE MODEL AS AN EARLY WARNING SYSTEM FOR FRAUDULENT TRANSACTIONS IN MOBILE BANKING

Merryta Djakaria and Tuga Mauritsius

Information Systems Management Department
BINUS Graduate Program – Master of Information Systems Management
Bina Nusantara University
Jl. Kebon Jeruk Raya No. 27, Kebon Jeruk, Jakarta 11530, Indonesia
merryta.djakaria@binus.ac.id; tmauritsus@binus.edu

Received November 2022; accepted January 2023

Abstract. *People nowadays can do various tasks more easily, thanks to the rapid development of technology. All current industries are undoubtedly impacted by this, including the banking sector. Many people are switching from making transactions via ATMs to mobile banking. In addition to convenience, security is one of the essential components that must be maintained and improved by every bank because patterns and methods of crime can change due to technological developments. This study aims to build an Artificial Intelligence (AI) model to detect fraudulent transactions through mobile banking. The data used to create the AI model is mobile banking transactions at XYZ Bank in 2021. Based on the research results, the XGBoost model has the best performance compared to other models and can be used as an early warning system to detect fraudulent transactions in mobile banking.*

Keywords: Artificial intelligence, Early warning system, Fraud detection, Machine learning, Mobile banking

1. **Introduction.** With the rapid pace of technological development during the Fourth Industrial Revolution, many tasks that needed a lot of time and human labor are now automated and simplified. Many people have started to adapt and utilize digital technology in their daily activities, especially since the COVID-19 pandemic [1]. Information and Communication Technology (ICT) in Indonesia continues to grow. According to data from Badan Pusat Statistik (BPS), in 2020, the use of technology grew by 10.10% compared to the previous year [2]. Banking is one of the industrial sectors that Indonesia's increasing usage of ICT has impacted. Mobile banking is one of the most popular cellular technology advancements in recent years. Notably, the widespread use of smartphones has increased the demand for mobile banking services and encouraged more banks or financial institutions to provide these cutting-edge services to broaden their customer base, increase customer retention, boost operational effectiveness, and create new job opportunities [3]. According to data from Bank Indonesia, transactions made through SMS/Mobile Banking have increased significantly between 2013 and 2021. Compared to the prior year, 2021 has the most significant growth rate, with increased transaction volume and value of 61.48% and 62.07%, respectively [4]. The significant growth in transactions through mobile banking has also changed people's behavior in transactions. Many people who once engaged in conventional transactions have shifted to digital ones; among them are XYZ bank customers. During the COVID-19 pandemic, there was a decrease in transactions through branches and ATMs. In bank XYZ's first quarter of 2021, branch-based transactions dropped by 22%, and ATM-based transactions decreased by 8% from the prior year.

DOI: 10.24507/icicelb.14.07.747

On the other hand, compared to other transaction channels, mobile banking transactions have had the most significant increase, with the most extensive transaction growth in 2021 reaching 70.65%.

The use of mobile banking is undoubtedly highly beneficial and makes it simpler for customers to complete transactions whenever and wherever they choose. In addition to ease, security is a crucial element that every bank must maintain and enhance as crime patterns and methods change in response to customer behavior shifting. According to Otoritas Jasa Keuangan (OJK), social engineering is the predominant form of cybercrime in the banking industry, with up to 2,000 private bank customers potentially falling victim to this scheme each month [5,6]. By using social engineering, the culprit manipulates the victim's psychological condition to obtain personal data that belongs to the victim so that the culprit can take control of the victim's account and spend the money in it [7].

Therefore, a quick and accurate early warning system is required to identify transactions suspected of being fraudulent. As technology advances, one possibility for identifying fraud in banking transactions is using Artificial Intelligence (AI). When compared to rule-based systems, which have static parameters, machine learning algorithm models on AI can be used to examine diverse fraud transaction patterns, predict transactions dynamically, and give early warnings to customers and banks [8].

Botchey et al. compared the performance of three classification algorithms in supervised learning: Support Vector Machines, Gradient Boosted Decision Trees, and Naïve Bayes to predict fraud in Mobile Money Transactions (MMT). Based on the evaluation results, the Gradient Boosted Decision Tree model has the best performance and can be used to detect fraud in MMTs [9]. Research done by Ileberi et al. aims to develop a machine learning model for detecting fraud in credit card transactions. This study used five different models: Decision Tree, Random Forest, Logistic Regression, Artificial Neural Network, and Naïve Bayes. According to the evaluation results, the Random Forest model has the best accuracy performance by 99.98% [10]. Liu et al. also researched to create a machine learning-based system for detecting online transaction fraud. Two algorithms have been proposed, Fully Connected Neural Network and Extreme Gradient Boosting (XGBoost). This study uses AUC to measure model performance, and XGBoost has the best AUC value of 0.969 [11]. Chang et al. conducted research to identify fraud detection models for digital payments using credit card transactions. Five alternative learning models are proposed and compared: K-Nearest Neighbours, Logistic Regression, Autoencoder, Decision Tree, and Random Forest. The results of this research show that the Logistic Regression and Random Forest models perform better than other algorithms. The performance of the suggested model can also be enhanced by using the undersampling technique and principal component analysis to reduce the number of features [12].

In the past, many studies have explored machine learning models for identifying fraudulent transactions. However, most of this research focuses on finding online fraud in general or fraud in credit card transactions. Therefore, this research aims to create and compare various AI models that could be used as early warning systems to detect and prevent fraudulent transactions, specifically in mobile banking.

This paper is divided into four sections: the introduction, the methodology section that describes the method and data used in this research, the result section that explains the result and evaluation of the models that have been developed, and the conclusion section.

2. **Methodology.** This research was conducted by creating an AI model with stages based on the CRISP-DM framework. The first stage in this research is to assess the business requirements. This stage is where the project objectives and the demands of business objectives are recognized [13]. Based on the background previously described, it was found that there is a need for an early warning system to detect fraudulent transactions in mobile banking. The second stage is data understanding. Data gathering and data interpretation

are included in this stage [14]. The data used in this study are 605,869 samples of XYZ Bank mobile banking transactions in 2021, including data from both before and after the consumer is exposed to fraud, with 7.97% representing fraudulent and the rest are genuine. Besides, 6,653 customer data are used to identify the customers' profiles.

The third stage is data preparation. After the required data has been collected, data cleansing is done to adjust the data format and handle inconsistent field contents and missing values. This stage also involves feature engineering, resulting in the creation of 16 features that can be utilized to build AI models, including customer segmentation, such as the period of use of mobile banking, the age of the customer, and the type of card used. Additionally, there are transaction-based predictor variables for successful and unsuccessful mobile banking transactions, including average, accumulation, and increase.

After the dataset is ready to use, it is divided with a proportion of 70 : 30 for train and test data. The class ratio plays a crucial part in the performance model when it comes to supervised learning classification. It can be discovered that there is a class imbalance in the dataset utilized when creating an AI model to detect fraudulent transactions [15]. Because the dataset used in this research has a reasonably significant class imbalance, the SMOTE method is used, so the data has a balanced class.

Based on several studies mentioned in the introduction section, some of the models with the best performance are Decision Tree, Random Forest, XGBoost, Naïve Bayes, and Logistic Regression. Therefore, those algorithms will also be used to build AI models in this research.

Decision Tree is a supervised learning algorithm that can be applied to regression and classification problems. It is used to choose the best course of action and has a prediction model with hierarchies or tree structures [9]. The Random Forest algorithm uses an ensemble of decision trees to make predictions, and the decision is made by a majority vote [10]. XGBoost is a decision tree ensemble that uses gradient boosting and is built to be very scalable by expanding the objective function additively by minimizing a loss function [16]. Naïve Bayes classifiers are built on the Bayes theorem for conditional probabilities. It is known as one of the extremely quick classification algorithms and a suitable technique for processing massive amounts of data [9]. The Logistic Regression classifier is a supervised machine learning algorithm typically used for binary classification tasks involving a particular sort of linear regression in which a linear function is added to the logit function [10].

The model will use a data train with balancing and without balancing method, so ten models are developed. The confusion matrix and AUC are used to evaluate the developed model. The confusion matrix is a simple method to determine the performance of the developed classification model by estimating both correct and incorrect classification rates [17]. The illustration of the confusion matrix is shown in Table 1. Four matrices can be used to determine the goodness of the model, including accuracy, recall, precision, and F1 Score, as shown in Equations (1)-(4) [18]. In addition, AUC can also be used to measure the performance of the classification model. If the AUC value is close to 1, the better the model predicts positive and negative classes [19].

$$Accuracy = \frac{TP + TN}{TP + FP + TN + FN} \tag{1}$$

$$Recall = \frac{TP}{TP + FN} \tag{2}$$

$$Precision = \frac{TP}{TP + FP} \tag{3}$$

$$F1\ Score = \frac{2 \times Precision \times Recall}{Precision + Recall} \tag{4}$$

TABLE 1. Confusion matrix

	Actual Genuine	**Actual Fraud**
Predicted Genuine	True Negative (TN)	False Negative (FN)
Predicted Fraud	False Positive (FP)	True Positive (TP)

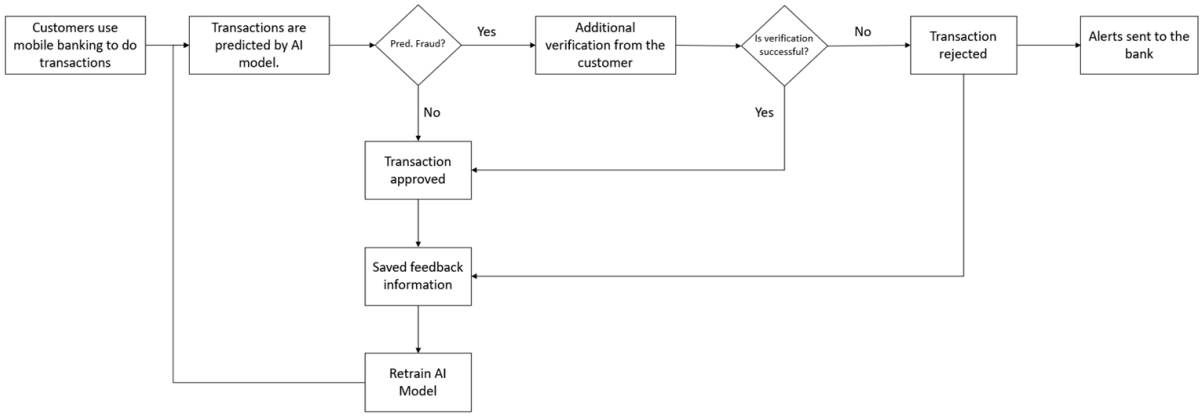

FIGURE 1. AI model as an early warning system

If the AI model used has been determined, then the model can be implemented to make predictions on transactions through mobile banking, as illustrated in Figure 1. Transactions predicted as fraud by the AI model need additional verification by the customer; If the verification process is unsuccessful, it can be assumed that the transaction is legitimate as fraud, and a warning will be sent to the bank for additional investigation and mitigation. To keep the AI model up to date when the pattern of fraudulent transactions changes, feedback from each transaction will be held in the database and utilized for retraining.

3. **Result.**

3.1. **Exploratory data analysis.** According to the findings of the data exploration, customers who have recently used mobile banking applications are typically more vulnerable to fraud than customers who have been using them for a long time. Data shows that 70.87% of customers exposed to fraud have only used mobile banking for less than two years. It also shows that 64.57% of customers affected by fraud are between 17-30 years old. This is in line with the mobile banking users at XYZ Bank, who are young adult customers. The fraudulent mode carried out by fraudsters under the guise of gifts or online investments makes many young adult customers easy to trust and provide confidential data to the fraudster compared to other age categories. It was also discovered that fraud mainly occurred between noon and night, with the evening having the highest percentage (30.30%). This shows how fraudsters steal information about victims during office hours so that people can easily assume that the person contacting them about a lottery or investment opportunity is a legitimate company representative.

3.2. **Model evaluation.** Once the AI model has been developed, it is evaluated using the previously prepared test data. Each model's accuracy, precision, recall, and AUC values are compared during evaluation to find the best model to implement as an early warning system. Figure 2 shows that compared to other models, the XGboost model created without data balancing has the best level of accuracy, which is 95.45%.

If the performance model is seen from the precision matrix, the Random Forest model created without data balancing has the highest precision value of 96.30%. While in general, as illustrated in Figure 3, the model created with data balancing using SMOTE performs

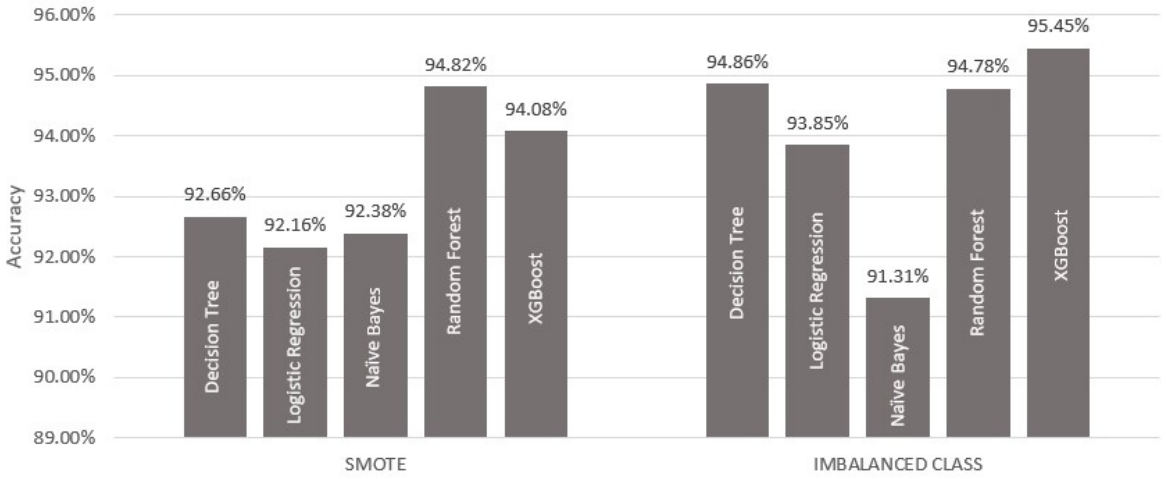

FIGURE 2. Performance comparison by accuracy

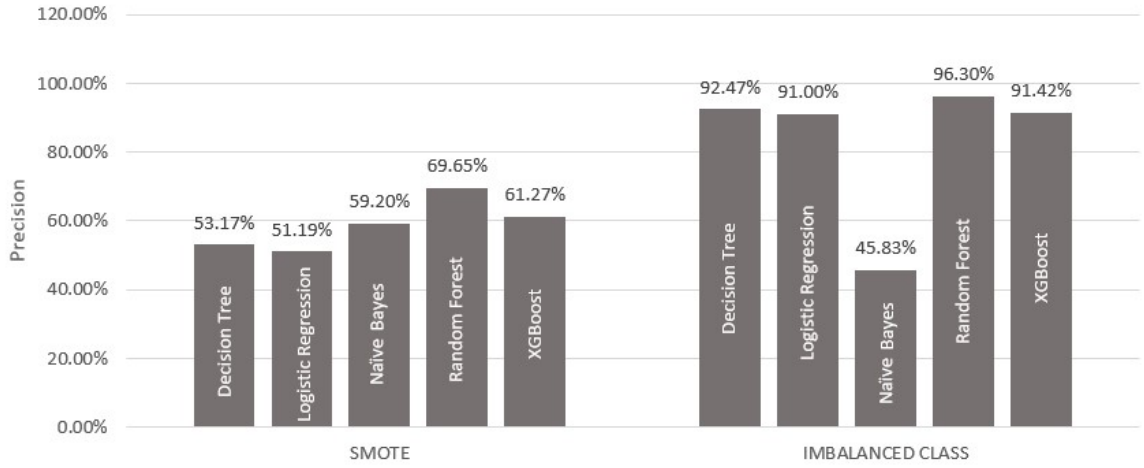

FIGURE 3. Performance comparison by precision

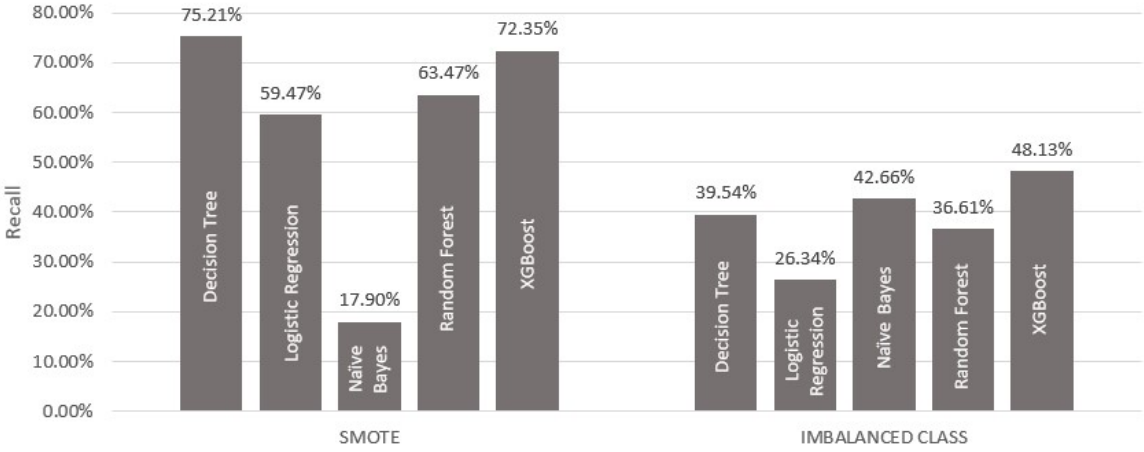

FIGURE 4. Performance comparison by recall

significantly below the model without data balancing. However, when viewed from the recall matrix, the model developed using SMOTE performs better than the model made with an imbalanced class, where the Decision Tree-SMOTE model has the highest recall value of 75.21% when compared to other models.

Based on the evaluation of the performance model using AUC, it was found that there was no noticeable difference between the models created with and without data balancing. Figure 5 shows that both Random Forest and XGBoost models have the best AUC performance compared to other models.

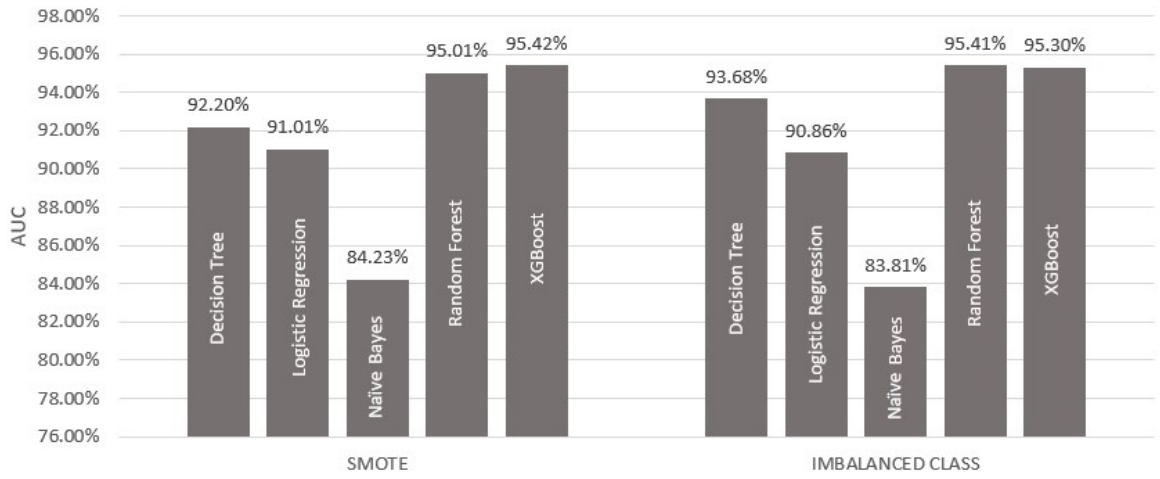

FIGURE 5. Performance comparison by AUC

Overall, it is clear that each model performs better in some matrices, but whether a model was created using the SMOTE approach or not, the Random Forest and XGBoost models perform the best than others.

4. **Conclusions.** This study was conducted by creating 10 AI models that may be used to identify fraudulent transactions in mobile banking. Based on the comparative analysis, it was found that the model developed with datasets that had unbalanced classes tended to provide more accurate predictions of fraudulent transactions. It can be seen from each model's superior precision and accuracy values. However, the model developed with a balanced class has a better performance in detecting transactions that are indeed fraudulent. It is shown by the recall value, which is better than the model with an unbalanced class. All developed models have AUC values above 0.8 which means the model can predict positive and negative classes well. Because this AI model development aims to prevent losses due to fraudulent transactions, it is recommended that the model developed using the SMOTE method can be chosen. Based on recall and AUC value, the XGBoost model has the best performance compared to other models.

The models developed in this study still have some limitations that can be explored in future research by creating new models using more advanced methods like deep learning and neural networks, as well as hyperparameter tuning that can be used to improve the model performance. Hopefully, this research can help XYZ Bank to detect and mitigate fraudulent transactions that occurred in mobile banking earlier.

Acknowledgment. Bina Nusantara University supports this work. The authors also gratefully acknowledge the helpful comments and suggestions of the reviewers, which have improved the presentation.

REFERENCES

[1] Yusuf, *The COVID-19 Pandemic Stimulates Adaptation to Using Digital Technology*, Kementerian Komunikasi Dan Informatika Republik Indonesia (Ministry of Communication and Information Technology, Indonesia), https://www.kominfo.go.id/content/detail/32602/pandemi-covid-19-pacu-adaptasi-gunakan-teknologi-digital/0/berita_satker, Accessed on May 10, 2022.

[2] Badan Pusat Statistik, *The 2020 Indonesia Information and Communication Technology Development Index Is 5.59 on a Scale of 0-10*, Badan Pusat Statistik Indonesia (Indonesian Central Bureau of Statistics), https://www.bps.go.id/pressrelease/2021/08/18/1848/indeks-pembangunan-teknologi-informasi-dan-komunikasi--ip-tik--indonesia-2020-sebesar-5-59-pada-skala-0----10.html, Accessed on May 10, 2022.

[3] A. A. Shaikh, Mobile banking adoption issues in Pakistan and challenges ahead, *J. Inst. Bankers Pak.*, vol.80, no.3, pp.12-15, https://www.scopus.com/inward/record.urieid=2-s2.0-84922337800&partnerID=40&md5=9ab827ee71f53f68ffa85276815ed380, 2013.

[4] Bank Indonesia, *Payment Statistics System and Financial Market Infrastructure March 2022*, https://www.bi.go.id/id/statistik/ekonomi-keuangan/spip/Pages/SPIP-Maret-2022.aspx, Accessed on Jun. 03, 2022.

[5] Herman, *Social Engineering Is the Most Mode that Attacks Bank Customers*, https://www.beritasatu.com/ekonomi/846591/modus-social-engineering-paling-banyak-serang-nasabah-bank, Accessed on Nov. 11, 2022.

[6] CNN Indonesia, *Per Month, 2 Thousand Bank Customers Become Victims of Cyber Crime*, https://www.cnnindonesia.com/teknologi/20220826193538-185-839667/per-bulan-2-ribu-nasabah-bank-jadi-korban-kejahatan-siber, Accessed on Nov. 11, 2022.

[7] D. Prastya, *Social Engineering Is the Most Dominant Cyber Crime in Indonesia*, https://www.suara.com/tekno/2021/11/16/233155/social-engineering-adalah-kejahatan-siber-paling-dominan-di-indonesia, Accessed on Nov. 11, 2022.

[8] Y. Han, S. Yao, T. Wen, Z. Tian, C. Wang and Z. Gu, Detection and analysis of credit card application fraud using machine learning algorithms, *J. Phys. Conf. Ser.*, vol.1693, no.1, DOI: 10.1088/1742-6596/1693/1/012064, 2020.

[9] F. E. Botchey, Z. Qin and K. Hughes-Lartey, Mobile money fraud prediction – A cross-case analysis on the efficiency of support vector machines, gradient boosted decision trees, and Naïve Bayes algorithms, *Inf.*, vol.11, no.8, DOI: 10.3390/INFO11080383, 2020.

[10] E. Ileberi, Y. Sun and Z. Wang, A machine learning based credit card fraud detection using the GA algorithm for feature selection, *J. Big Data*, vol.9, no.1, DOI: 10.1186/s40537-022-00573-8, 2022.

[11] B. Liu, X. Chen and K. Yu, Online transaction fraud detection system based on machine learning, *J. Phys. Conf. Ser.*, vol.2023, no.1, DOI: 10.1088/1742-6596/2023/1/012054, 2021.

[12] V. Chang, L. M. T. Doan, A. Di Stefano, Z. Sun and G. Fortino, Digital payment fraud detection methods in digital ages and Industry 4.0, *Comput. Electr. Eng.*, vol.100, no.8, 107734, DOI: 10.1016/j.compeleceng.2022.107734, 2022.

[13] A. F. Siregar and T. Mauritsius, Ulos fabric classification using Android-based convolutional neural network, *International Journal of Innovative Computing, Information and Control*, vol.17, no.3, pp.753-766, DOI: 10.24507/ijicic.17.03.753, 2021.

[14] I. Dewantoro and T. Mauritsius, Implementation of data mining on customs false declaration detection, *J. Theor. Appl. Inf. Technol.*, vol.100, no.7, pp.1664-1674, 2022.

[15] A. Mishra and C. Ghorpade, Credit card fraud detection on the skewed data using various classification and ensemble techniques, *2018 IEEE Int. Students' Conf. Electr. Electron. Comput. Sci. (SCEECS2018)*, pp.1-5, DOI: 10.1109/SCEECS.2018.8546939, 2018.

[16] C. Bentéjac, A. Csörgő and G. Martínez-Muñoz, A comparative analysis of gradient boosting algorithms, *Artif. Intell. Rev.*, vol.54, no.11, pp.1937-1967, DOI: 10.1007/s10462-020-09896-5, 2019.

[17] H. Kang, *Fraud Detection in Mobile Money Transactions Using Machine Learning*, https://lib.dr.iastate.edu/cgi/viewcontent.cgiarticle=1449&context=creativecomponents, 2019.

[18] S. K. Arjaria, A. S. Rathore and J. S. Cherian, Kidney disease prediction using a machine learning approach: A comparative and comprehensive analysis, in *Demystifying Big Data, Machine Learning, and Deep Learning for Healthcare Analytics*, N. Pradeep, S. Kautish and S.-L. Peng (eds.), Academic Press, 2021.

[19] C. Marzban, The ROC curve and the area under it as performance measures, *Weather Forecast.*, vol.19, no.6, pp.1106-1114, DOI: 10.1175/825.1, 2004.