https://doi.org/10.62836/jcmea.v3i1.030102

Global Science Publishing

JCMEA

Journal of Computational Methods in Engineering Applications

https://ojs.sgsci.org/journals/jcmea

Article

Efficient Bank Fraud Detection with Machine Learning

Rong Zhang [1,*], Yu Cheng [2], Liyang Wang [3], Ningjing Sang [2] and Jinxin Xu [4]

[1] *Graduate School of Management, University of California, Davis, CA 95616, USA*

[2] *The Fu Foundation School of Engineering and Applied Science, Columbia University, New York, NY 10027, USA; yucheng576@gmail.com (Y.C); ns3319@columbia.edu (N.S.)*

[3] *Olin Business School, Washington University in St. Louis, St. Louis, MO 63130, USA; liyang.wang@wustl.edu*

[4] *Department of Cox Business School, Southern Methodist University, Dallas, TX 75205, USA; jensenjxx@gmail.com*

Abstract: The rapid expansion of IT technology has led to a significant increase in financial transactions, accompanied by a corresponding rise in fraudulent activities. This paper tackles the challenge of detecting fraud in various forms, such as credit card fraud, banker cheque fraud, and online funds transfer fraud, which have become increasingly sophisticated. Traditional methods struggle to keep pace with these evolving fraud techniques, necessitating advanced approaches. We propose the use of machine learning algorithms to enhance the detection of fraudulent transactions. Utilizing the BankSim dataset from Kaggle, which includes features like age, gender, payment domain, and transaction amount, we conducted a comprehensive analysis. The dataset was preprocessed to handle missing values and balance the instances of fraud. We then applied several machine learning algorithms, including K-Nearest Neighbors (KNN), Naive Bayes, and Support Vector Machine (SVM), training these models on a training set and evaluating them on a test set. The performance of these models was assessed using precision, recall, and F1-measure metrics. Our findings demonstrate that the SVM algorithm achieved the highest accuracy at 99.23%, significantly outperforming the other algorithms and previous studies. This study highlights the effectiveness of machine learning, particularly SVM, in developing robust fraud detection systems, offering a promising solution to improve financial security.

Keywords: machine learning; Bank Fraud Detection; SVM

1. Introduction

Financial deepening not only enhances capital liquidity and utilization efficiency but also promotes optimal resource allocation [1]. However, this expansion in financial activities also increases the complexity of the financial system, potentially leading to a higher incidence of fraudulent behavior. As fraudulent transactions become more sophisticated, advanced methods such as extreme value mixture modeling are essential for accurate risk estimation and fraud detection, helping banks and other financial institutes address the numerous problems caused by fraudulent transactions [2]. Consequently, detecting fraudulent transactions becomes increasingly tedious and challenging [3,4].

Fraud may occur in a few ways in financial transactions such as credit card fraud, banker cheque fraud, online funds transfer fraud and many more. To avoid credit card frauds, besides its latest developments, its

Received: 20 September 2023; Accepted: 16 October 2023.

* Corresponding: Rong Zhang (rzhang1118@gmail.com)

patterns are consistently changed but still fraudsters find methods to make fraudulent cards legitimate and causes frauds in transactions. These fraudulent acts make fraud detection more complicated and difficult to detect. Because of these rapid changes in frauds and scams, researchers are utilizing several methods to improve the performance of existing systems in financial transactions [5].

Fraudsters typically exploit security, control, and monitoring weaknesses in commercial applications to achieve their goals. However, technology can also be leveraged to combat fraud effectively [6]. The application of neural networks for solving complex prediction problems, as studied in handling soil bearing capacity, can similarly be utilized to enhance the detection and prediction of fraud in large volumes of banking data, improving efficiency and reducing the reliance on manual transaction reviews [7]. Precision detection and imaging technologies enhance pattern recognition by improving the detection of fine structures and complex signals. Their application provides more sensitive fraud detection, addressing weaknesses in financial systems and enabling timely fraud prevention [8, 9]. Additionally, methods using large language models (LLMs) to extract key points from qualitative data can automatically generate key points of anomalous patterns in financial transactions, enhancing fraud detection systems' ability to capture suspicious activities. By analyzing transaction data with LLMs, the detection accuracy of complex fraud patterns can be improved, facilitating earlier identification and prevention of potential fraud [10]. Detecting fraud immediately after it occurs is crucial to prevent further incidents [11]. Fraud is defined as wrongful or criminal deception intended for financial or personal gain. Credit card fraud, specifically, involves the illegal use of credit card information for purchases, both in physical and digital forms. In digital transactions, fraud occurs when cardholders provide their card number, expiration date, and card verification number over the phone or online [12]. To mitigate fraud-related losses, two key mechanisms can be employed: fraud prevention and fraud detection. Fraud prevention is a proactive approach that aims to stop fraud before it happens. Conversely, fraud detection is essential when a fraudster attempts a fraudulent transaction [13].

Fraud detection in banking is treated as a binary classification problem, where data is categorized as either legitimate or fraudulent [14]. Given the large volume of banking data, manually reviewing transactions to identify patterns of fraud is impractical and time-consuming. Consequently, machine learning algorithms are crucial in detecting and predicting fraud [15]. For instance, semantic wireframe detection, which identifies complex structures in images to produce precise feature representations, can similarly be applied to financial data to recognize intricate transaction patterns, thereby improving fraud detection accuracy [16]. Machine learning and deep learning techniques provide swift and effective solutions to real-time fraud detection challenges [17]. In parallel, revised reinforcement learning based on anchor graph hashing optimizes data processing by simplifying it into efficient hash operations, enhancing analysis in large-scale data settings [18]. Machine learning models developed rapidly in the last decades, such as NLP that frequently used in texting analysis in transaction mono and notes analysis. Many existing backdoor attacks in NLP applications are mainly through various data poisoning manners with fixed/static triggers such as characters, words, and phrases [19]. Similarly, advancements in neural network-based solutions and techniques like extreme gradient boosting decision trees are increasingly applied to enhance the robustness and accuracy of machine learning models in various domains [20]. In addition to text analysis in machine learning, further developments such as Dynamic Graph Neural Networks (DGNNs) are benefiting the machine learning community [21].

This paper examines fraud occurring in financial transactions across various sectors, including hospitals, traffic systems, banks, and educational institutions. To conduct our study, we utilized the BankSim dataset from Kaggle, which includes seven features such as age, gender, payment domain, and amount paid. Transactions in the dataset have been labeled by experts, with '0' indicating no fraud and '1' indicating fraud.

We compared the performance of several machine learning algorithms such as K-Nearest Neighbors (KNN), Naive Bayes, and Support Vector Machine (SVM) to detect fraudulent activities. The models were trained using a training set and evaluated with a test set. Our results show that the SVM algorithm outperforms the others, achieving an accuracy of 99.23%. These findings demonstrate that SVM not only surpasses the other algorithms tested but also performs better than those reported in previous literature. These things are discussed in detail in the following sections.

The rest of the papers are organized in such a way that section 3 presents literature review, section 4 gives a problem statement while section 5 highlights a proposed solution. After the proposed solution section 6 presents results and discussion while section 7 discusses conclusion.

2. Related Work

2.1. Overview of Fraud Detection in Financial Transactions

Because of advancements in technology, financial transactions can be made in various ways such as credit card transfers and bank app transfers. As the use of these technologies increases, innovative approaches are essential to address the growing complexity of fraud detection. For instance, intelligent monitoring methods, such as those using distributed fiber optic sensors assisted by deep learning, enhance anomaly detection in transaction data [22]. Additionally, semi-supervised classification methods for detecting strip surface defects, as explored in recent studies, provide novel insights into handling partially labeled data, which can be applied to improve the detection of subtle and emerging patterns in financial fraud [23]. Moreover, advancements in surface plasmon polariton graphene mid-infrared photodetectors highlight how cutting-edge technologies can improve sensitivity and precision, principles applicable to financial fraud detection systems [24, 25]. A huge literature exists on fraud detection in financial transactions, and we present some here in this section.

Aisha et al. explores the application of advanced technologies to combat financial fraud in the rapidly evolving FinTech sector [26]. It highlights the increasing sophistication of fraudulent activities, which challenge both consumer trust and economic stability. The study evaluates several machine learning models—Decision Trees, SVM, Random Forests, Neural Networks, and a customized anomaly detection model—assessing their effectiveness in identifying fraudulent transactions. These models are evaluated using metrics such as ROC/AUC scores, True Positives, and False Positives. The customized anomaly detection model achieved the highest ROC/AUC score of 0.98, outperforming the other models despite variations in their performance regarding true and false positive rates. The paper underscores the significance of big data in enhancing fraud detection capabilities. By processing and analyzing large transactional datasets, machine learning models can uncover fraudulent patterns more effectively. However, the study identifies several challenges, including the lack of universally effective models and the scarcity of comprehensive, publicly available datasets. To address these issues, the authors advocate for greater data sharing and collaboration between financial entities and researchers to improve fraud detection systems.

2.2. Machine Learning in Fraud

The paper titled "A survey of machine-learning and nature-inspired based credit card fraud detection technique [27]" highlights the significance of credit cards in facilitating electronic transactions globally, noting their convenience and ease of use. However, it also addresses the increasing threat of credit card fraud, which has led to substantial financial losses for companies and individuals worldwide. The paper emphasizes the urgency of developing advanced and adaptable fraud detection techniques due to the continuously evolving methods used by cybercriminals. The review focuses on recent advancements in credit card fraud detection, specifically highlighting machine learning and nature-inspired techniques. It provides a comprehensive overview of the current trends, contributions, and limitations of existing methods, offering essential background information for researchers. Additionally, the paper serves as a valuable resource for financial institutions and individuals seeking effective solutions for credit card fraud detection.

Various machine learning algorithms are used in the fraud detection to detect fraudulent activities within financial transactions [28]. The study employs a dataset from the Kaggle repository, which includes over 6.3 million transaction records with ten different features. The researchers evaluated multiple machine learning models including MLP Regressor, Random Forest Classifier, Complement NB, Gaussian NB, Bernoulli NB, LGBM Classifier, AdaBoost Classifier, K Neighbors Classifier, Logistic Regression, Bagging Classifier, Decision Tree Classifier, and Deep Learning algorithms. The findings show that algorithms have obtained about 99% of accuracy. These results underscore the importance of dataset balancing in improving the performance of

fraud detection models. In addition, the paper highlights the significant potential of machine learning algorithms in enhancing the detection of fraudulent financial transactions, emphasizing the need for continuous improvement and adaptation of these models to handle the dynamic nature of fraudulent activities.

Chen et al. explores the application of the CatBoost algorithm to improve the accuracy and efficiency of fraud detection in financial transactions [29]. Utilizing a dataset from the Kaggle competition platform, the researchers implemented feature engineering to enhance model performance and employed memory compression techniques to speed up the detection process. The results demonstrated that the CatBoost-based model achieved an optimal accuracy of 98.3%, highlighting its potential for real-time fraud detection in dynamic financial environments.

The paper "Attention-Enhancing Backdoor Attacks Against BERT-based Models" explores the application of machine learning techniques widely used in the United States and the large amount of EHR data generated provides an opportunity for machine learning based predictive modeling to improve decision support [19]. Machine learning models influence financial modelling everywhere such as learn the pattern in the time series data [30]. Fraud also is threating the virtual financial market such as transactions on dark web including Bitcoin blockchain [31].

As mentioned above, huge similar literature can be found on various frauds detections in financial transaction using machine learning, however, we can conclude from above that the issue is of high importance and has not been tackled by the way we are going to handle.

3. Methodology

Traditionally, financial market simulations have focused on prediction problems like economic growth, market trends, and consumption patterns. Besides, there has been significant research on fraud detection, but these normally focus a specific area such as ATM fraud detection, fraud detection from CCTV images and fraud detection in online payments. However, there is currently a lack of research on fraud detection in banks transactions for various purposes. Some literature exists but there is space to improve accuracy.

3.1. Selection of Machine Learning Algorithm

The proposed system model is illustrated in Figure 1. The foundation of this system is the BankSim dataset, sourced from Kaggle, which encompasses information on financial transactions across various domains. The dataset, initially in raw form, necessitated several preprocessing steps to normalize the data effectively. One critical preprocessing task was handling missing values, ensuring the dataset's completeness. Moreover, a significant challenge was the imbalance in the dataset, where instances of fraudulent transactions were substantially lower in number compared to non-fraudulent ones. To address this, techniques were applied to balance the number of instances, thereby preventing bias in the model's training process. Additionally, regularization was introduced using the lambda function to further refine the data quality.

Following the preprocessing phase, feature selection was performed to identify the most relevant attributes from the dataset, which were then used as inputs for the classifier. The dataset was subsequently divided into training and testing sets, adhering to a split ratio of 30% for training and 70% for testing. This stratified split ensures that the model is exposed to a diverse range of transaction patterns during training, enhancing its generalization capabilities.

3.2. Model Training

The model was trained using the training set and subsequently evaluated on the test set. A comparative analysis of various machine learning models for fraud detection was conducted. The machine learning algorithms employed in this study included Naive Bayes, KNN, Random Forest and SVM. Each model was rigorously trained on the training set and evaluated on the test set to ascertain its performance.

To evaluate the efficacy of the models, several performance metrics were incorporated. These included accuracy, precision, recall, F1 measure, and the Receiver Operating Characteristic (ROC) curve. Accuracy

provides a general measure of the model's correct predictions, while precision and recall offer insights into the model's performance in identifying fraudulent transactions specifically. The F1 measure, a harmonic mean of precision and recall, provides a balanced evaluation of the model's capability. The ROC curve further illustrates the trade-off between the true positive rate and false positive rate, offering a comprehensive view of the model's diagnostic ability.

The entire system was implemented using Python, leveraging various machine learning libraries for data preprocessing, visualization, and model implementation. Libraries such as Pandas and NumPy were utilized for data manipulation and preprocessing, while Matplotlib and Seaborn were employed for visualization purposes. For implementing the machine learning models, libraries such as Scikit-learn, and others were used.

To conclude, the proposed system model demonstrates a robust approach to financial fraud detection by integrating advanced machine learning techniques with meticulous data preprocessing and feature selection. The comparative analysis of multiple algorithms provides valuable insights into their respective strengths and weaknesses, ultimately contributing to a more secure and reliable financial transaction environment.

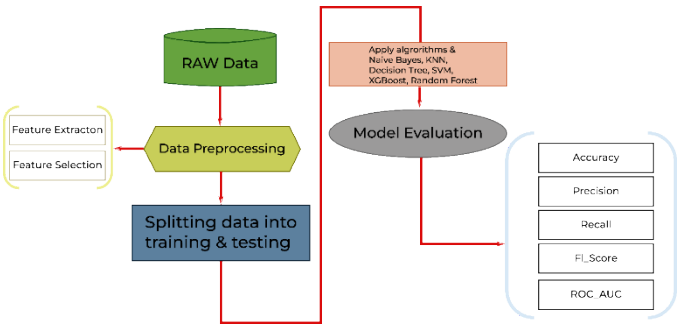

Figure 1. Proposed System Model.

4. Experiment And Result

4.1. Data Collection

The BankSim dataset, sourced from Kaggle, is a dataset that simulates financial transactions, providing a robust framework for developing and testing fraud detection models. This dataset is particularly useful for academic and practical purposes because it replicates realistic transaction patterns and behaviors, enabling researchers and practitioners to explore various fraud detection methodologies. The dataset consists of 8 columns and 594,643 instances. Following are the different features of the dataset.

Step: A unit of time representing the elapsed time since the first transaction. This feature is useful for understanding temporal patterns and trends in transactions.

Customer: An identifier for the customer conducting the transaction. This helps in tracking transaction behaviors of individual customers.

Age: The age category of the customer. Age can be a critical factor in understanding spending patterns and detecting anomalies.

Gender: The gender of the customer. Gender-related spending habits might help in identifying unusual transaction behaviors.

Merchant: An identifier for the merchant where the transaction took place. This feature is vital for detecting fraudulent merchants or unusual transaction locations.

Category: The category of the transaction, such as groceries, entertainment, etc. Different categories might have different fraud risk profiles.

Amount: The amount of money involved in the transaction. Unusually high or low amounts can be indicative of fraud.

Fraud: A binary indicator of whether the transaction is fraudulent (1) or not (0). This is the target variable for the fraud detection model.

The BankSim dataset was generated using a simulation based on real-world transaction patterns and

behaviors. This synthetic data aims to mimic genuine financial transactions, incorporating randomness and variability that reflect actual usage scenarios. The advantage of using a synthetic dataset like BankSim is that it avoids privacy issues while providing realistic data for model training and evaluation. A sample of data is show in Table No.1.

Table 1. BankSim dataset Used for Our Experiments.

Step	Customer	Age	Gender	Zip Code	Merchant
0	'C1093826151'	'4'	'M'	'28007'	'M348934600'
0	'C352968107'	'2'	'M'	'28007'	'M348934600'
0	'C2054744914'	'4'	'F'	'28007'	'M1823072687'
0	'C1760612790'	'3'	'M'	'28007'	'M348934600'
0	'C757503768'	'5'	'M'	'28007'	'M348934600'
0	'C1315400589'	'3'	'F'	'28007'	'M348934600'
0	'C1865204568'	'5'	'M'	'28007'	'M1823072687'

Zip Merchant	Category	Amount	Fraud
'28007'	'es_transportation'	4.55	0
'28007'	'es_transportation'	39.68	0
'28007'	'es_transportation'	26.89	0
'28007'	'es_transportation'	17.25	0
'28007'	'es_transportation'	35.72	0
'28007'	'es_transportation'	25.81	1

4.2. Model Performance Metrics

As discussed above, we present a comparative analysis of machine learning models for frauds detections in banks using BankSim dataset. We have recycled various machine learning algorithms which are KNN, Naïve Bayes, Random Forest and SVM in our experiments. As illustrated by Figure No.2 the lowest accuracy is that of Random Forest, which is 96%, Naïve Bayes stands second with an accuracy of 98.39% while KNN possess and accuracy of 98.51. The highest accuracy is that of SVM which outperforms all other classifiers and has achieved 99.2% accuracy.

Figure 2 summarizes the performance of the SVM model on the testing dataset. Metrics include accuracy, precision, recall, F1-score, and area under the ROC curve (AUC).

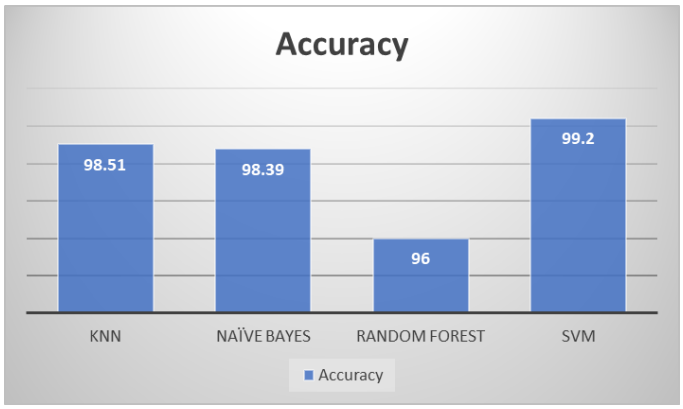

Figure 2. Performance Metrics of The SVM on the German Credit Data Test Set.

4.3. Comparative Analysis of SVM and Logistic Regression

Beside accuracy metric we have also used other metrics such ass Precision, Recall F1-Measure and ROC

curve which shows further insight into results. The Precision, Recall and F1-Measuer on weighted average basis for fraud and no-fraud instances are shown in Table No.2 Bellow.

Table 2. Precision, Recall and F1-Measure Obtained from Experiments.

Algorithm	Precision	Recall	F1-Measure
KNN	0.98	0.98	0.98
Naïve Bayes	0.98	0.98	0.99
Random Forest	0.99	0.96	0.97
SVM	0.99	0.99	0.99

KNN has a high precision, recall, and F1 measure, indicating that it is very effective at correctly identifying fraudulent transactions with minimal false positives and false negatives. Naïve Bayes also performs well, with precision and recall like KNN. The slightly higher F1 measure suggests a slightly better balance between precision and recall. Furthermore, Random Forest shows the highest precision, meaning it is very accurate when it predicts a transaction as fraudulent. However, its recall is slightly lower, indicating it misses some fraudulent transactions. The F1 measure reflects a slight trade-off between precision and recall. Last but not the least but even better, SVM achieves the highest precision, recall, and F1 measure among the models, indicating it is exceptionally effective at identifying fraudulent transactions with the least number of errors in both false positives and false negatives.

4.4. ROC Analysis

In addition to the above-mentioned metrics, I have ROC (Receiver Operating Characteristic) curve which illustrates the trade-off between the true positive rate (sensitivity) and the false positive rate across different threshold settings. It helps in evaluating the performance of a classification model by showing its ability to distinguish between classes. A higher area under the ROC curve (AUC) indicates better model performance. ROC curves all the models are shown in Figure 3.

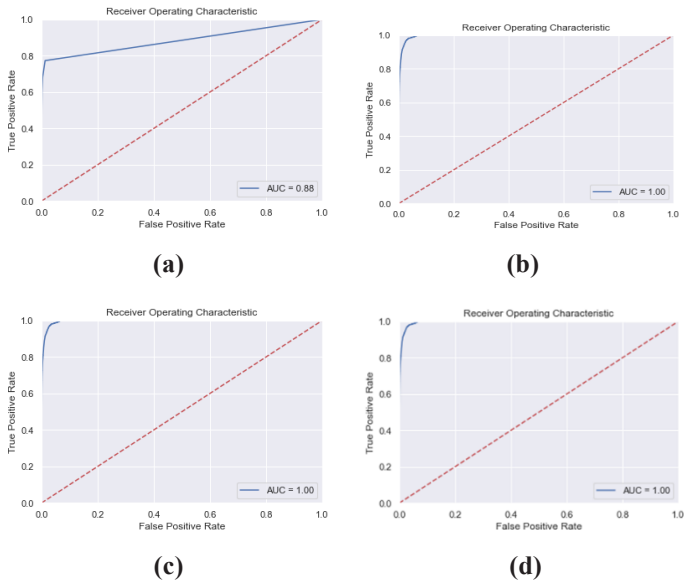

Figure 3. Figures a, b, c, and represents the ROC Curve of KNN, Naïve Bayes, Random Forest and SVM respectively.

5. Conclusions

The widespread adoption of IT technology has led to a significant increase in the volume of financial transactions, presenting both opportunities and challenges for financial institutions. Among the most pressing

challenges is the rise in fraudulent activities, which pose substantial threats to financial security and necessitate the development of advanced detection methods. This paper has explored the application of several machine learning algorithms to enhance the detection of fraudulent transactions, using the BankSim dataset from Kaggle.

The comparative analysis of K-Nearest Neighbors (KNN), Naive Bayes, Random Forest, and Support Vector Machine (SVM) algorithms revealed that SVM outperforms the other models, achieving an impressive accuracy of 99.23%. This high level of performance underscores the potential of machine learning techniques, particularly SVM, in mitigating fraud in financial transactions. The superior results of SVM are attributed to its ability to handle high-dimensional data and identify complex patterns associated with fraudulent behavior.

In conclusion, this study demonstrates the critical role of machine learning, particularly SVM, in enhancing financial security by effectively detecting fraudulent transactions. The findings contribute to the ongoing efforts to develop robust and reliable fraud detection systems, ultimately enhancing the security and integrity of financial operations. By continuing to refine these models and integrating them with real-time systems, financial institutions can better protect themselves and their customers from the ever-evolving threat of fraud.

Funding

Not applicable.

Author Contributions

Conceptualization, writing—original draft preparation and writing—review and editing, R.Z., Y.C., L.W., N.S. and J.X.; All of the authors read and agreed to the published the final manuscript.

Institutional Review Board Statement

Not applicable.

Informed Consent Statement

Not applicable.

Data Availability Statement

Not applicable.

Conflicts of Interest

The authors declare no conflict of interest.

References

1 Qiu Y. Financial Deepening and Economic Growth in Select Emerging Markets with Currency Board Systems: Theory and Evidence. 2024. arXiv: 2406.00472.

2 Qiu Y. *Estimation of Tail Risk Measures in Finance: Approaches to Extreme Value Mixture Modeling*; Johns Hopkins University, 2019.

3 Hashemi SK, Mirtaheri SL, Greco S. Fraud Detection in Banking Data by Machine Learning Techniques. *IEEE Access* 2022; **11**: 3034–3043.

4 Matloob I, Khan SA, Rukaiya R, Khattak MAK, Munir A. A Sequence Mining–Based Novel Architecture for Detecting Fraudulent Transactions in Healthcare Systems. *IEEE Access* 2022; **10**: 48447–48463.

5 Feng H. Ensemble Learning in Credit Card Fraud Detection Using Boosting Methods. In Proceedings of the 2021 2nd International Conference on Computing and Data Science (CDS), 28–29 January 2021, Stanford, CA, USA.

6 Soltani Delgosha M, Hajiheydari N, Fahimi SM. Elucidation of Big Data Analytics in Banking: a Four–Stage Delphi Study. *Journal of Enterprise Information Management*, 2021; **34**(**6**): 1577–1596.

7 Wenjun D, Fatahizadeh M, Touchaei HG, Moayedi H, Foong LK. Application of Six Neural Network–

Based Solutions on Bearing Capacity of Shallow Footing on Double–Layer Soils. *Steel and Composite Structures* 2023; **49**(**2**): 231–244.

8 Deng X, *et al*. Five–Beam Interference Pattern Model for Laser Interference Lithography. In Proceedings of the The 2010 IEEE International Conference on Information and Automation, 20–23 June 2010, Harbin, China.

9 Deng X, Kawano Y. Terahertz Plasmonics and Nano–Carbon Electronics for Nano–Micro Sensing and Imaging. *International Journal of Automation Technology* 2018; **12**(**1**): 87–96.

10 Zhao F, Yu F, Trull T, Shang Y. A New Method Using LLMs for Keypoints Generation in Qualitative Data Analysis. In Proceedings of the 2023 IEEE Conference on Artificial Intelligence (CAI), Santa Clara, CA, USA, 5–6 June 2023.

11 Puh M, Brkić L. Detecting Credit Card Fraud Using Selected Machine Learning Algorithms. In Proceedings of the 2019 42nd International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, Croatia, 20–24 May 2019.

12 Randhawa K, Loo CK, Seera M, Lim CP, Nandi KA. Credit Card Fraud Detection Using AdaBoost and Majority Voting. *IEEE Access* 2018; **6**: 14277–14284.

13 Kumaraswamy N, Markey MK, Ekin T, Barner JC, Rascati K. Healthcare Fraud Data Mining Methods: A Look Back and Look Ahead. *Perspectives in Health Information Management* 2022; **19**(**1**): 1i.

14 Malik EF, Khaw KW, Belaton B, Wong WP, Chew X. Credit Card Fraud Detection Using a New Hybrid Machine Learning Architecture. *Mathematics* 2022; **10**(**9**): 1480.

15 Gupta K, Singh K, Singh GV, Hassan M, Sharma U. Machine Learning Based Credit Card Fraud Detection–A Review. In Proceedings of the 2022 International Conference on Applied Artificial Intelligence and Computing (ICAAIC), Salem, India, 9–11 May 2022.

16 Zhou Y, *et al*. Semantic Wireframe Detection. Available online: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www. ndt. net/article/dgzfp2023/papers/P17. pdf (accessed on 15 June 2023).

17 Almutairi R, Godavarthi A, Kotha AR, Ceesay E. Analyzing Credit Card Fraud Detection Based on Machine Learning Models. In Proceedings of the 2022 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS), Toronto, ON, Canada, 1–4 June 2022.

18 Sun G, Zhan T, Owusu BG, Daniel A–M, Liu G, Jiang W. Revised Reinforcement Learning Based on Anchor Graph Hashing for Autonomous Cell Activation in Cloud–RANs. *Future Generation Computer Systems* 2020; **104**: 60–73.

19 Lyu W, Zheng S, Pang L, Ling H, Chen C. Attention–Enhancing Backdoor Attacks Against BERT–based Models. 2023. arXiv:2310.14480.

20 Liu Y, Liu L, Yang L, Hao L, Bao Y. Measuring Distance Using Ultra–Wideband Radio Technology Enhanced by Extreme Gradient Boosting Decision Tree (XGBoost). *Automation in Construction* 2021; **126**: 103678.

21 Xie J, Liu Y, Shen Y. Explaining Dynamic Graph Neural Networks via Relevance Back–Propagation. 2022. arXiv: 2207.11175.

22 Liu Y, Bao Y. Intelligent Monitoring of Spatially–Distributed Cracks Using Distributed Fiber Optic Sensors Assisted by Deep Learning. *Measurement* 2023; **220**: 113418.

23 Liu Y, Yang H, Wu C. Unveiling Patterns: A Study on Semi–Supervised Classification of Strip Surface Defects. *IEEE Access* 2023; **11**: 119933–119946.

24 Deng X, Kawano Y. Surface Plasmon Polariton Graphene Midinfrared Photodetector with Multifrequency Resonance. *Journal of Nanophotonics* 2018; **12**(**2**): 026017–026017.

25 Deng X, Oda S, Kawano Y. Graphene–Based Midinfrared Photodetector with Bull's Eye Plasmonic Antenna. *Optical Engineering* 2023; **62**(**9**): 097102–097102.

26 Saxena AK, Vafin A. Machine Learning and Big Data Analytics for Fraud Detection Systems in the United States Fintech Industry. *Emerging Trends in Machine Intelligence and Big Data* 2019; **11**(**12**): 1–11.

27 Adewumi AO, Akinyelu AA. A Survey of Machine–Learning and Nature–Inspired Based Credit Card Fraud

Detection Techniques. *International Journal of System Assurance Engineering and Management* 2017; (**8**): 937–953.

28 Amarasinghe T, Aponso A, Krishnarajah N. Critical Analysis of Machine Learning Based Approaches for Fraud Detection in Financial Transactions. In Proceedings of the 2018 International Conference on Machine Learning Technologies, Jinan, China, 19–21 May 2018.

29 Chen Y, Han X. CatBoost for Fraud Detection in Financial Transactions. In Proceedings of the 2021 IEEE International Conference on Consumer Electronics and Computer Engineering (ICCECE), Guangzhou, China, 15–17 January 2021.

30 Li Z, Yu H, Xu J, Liu J, Mo Y. Stock Market Analysis and Prediction Using LSTM: A Case Study on Technology Stocks. *Innovations in Applied Engineering and Technology* 2023; **2**(**1**): 1–6.

31 Carr T, *et al*. Into the Reverie: Exploration of the Dream Market. In Proceedings of the 2019 IEEE International Conference on Big Data (Big Data), Los Angeles, CA, USA, 9–12 December 2019.