Modern machine learning and deep learning algorithms for preventing credit card frauds

Indurthi Ravindra Kumar[1], Shaik Abdul Hameed[1], Bala Annapurna[2], Rama Krishna Paladugu[3], Veeramreddy Surya Narayana Reddy[4], Kiran Kumar Kaveti[5]

[1]Department of Computer Science and Engineering, VNR Vignana Jyothi Institute of Engineering and Technology, Hyderabad, India
[2]Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, India
[3]Department of Computer Science and Engineering, R.V.R and J.C College of Engineering, Guntur, India
[4]Department of Computer Science and Engineering, BVRIT Hyderabad College of Engineering for Women, Hyderabad, India
[5]Department of Computer Science and Engineering, Vignan's Foundation for Science Technology and Research, Guntur, India

Article Info

Article history:

Received Apr 18, 2024
Revised Nov 15, 2024
Accepted Nov 24, 2024

Keywords:

Credit card frauds
Deep learning
Fraud detection
Machine learning
Online fraud
Transaction data analysis

ABSTRACT

Credit card fraud poses a significant threat to financial institutions and consumers, particularly in the context of online transactions. Conventional rule-based systems often struggle to keep pace with the evolving tactics of fraudsters. This research paper investigates the application of advanced machine learning and deep learning algorithms for credit card fraud detection. By reviewing existing methodologies and addressing the challenges associated with fraud detection, we explore the potential of state-of-the-art techniques in enhancing detection accuracy and efficiency. Key aspects such as transaction data analysis, feature engineering, model evaluation metrics, and practical implementations are discussed. The findings underscore the importance of leveraging advanced algorithms to combat fraudulent activities effectively, thereby safeguarding the integrity of online transactions.

Corresponding Author:

Veeramreddy Surya Narayana Reddy
Department of Computer Science and Engineering, BVRIT Hyderabad College of Engineering for Women
Hyderabad, India
Email: veeramreddysurya@gmail.com

1. INTRODUCTION

The advent of digital commerce has revolutionized the way financial transactions are conducted, with credit cards serving as a ubiquitous tool for online payments. While this advancement has brought unprecedented convenience, it has also opened avenues for fraudulent activities. Credit card fraud remains a pressing concern for financial institutions and consumers alike, imposing substantial financial losses and undermining trust in online transactions [1]. Traditional methods of fraud detection, relying on predefined rules and thresholds, often fall short in detecting sophisticated fraudulent schemes. As fraudsters continuously adapt their tactics to evade detection, there arises a critical need for more advanced and adaptive solutions. In recent years, machine learning and deep learning algorithms have emerged as powerful tools for addressing complex and dynamic fraud patterns [2]. The primary objective of this research paper is to explore the application of state-of-the-art machine learning and deep learning techniques in credit card fraud detection. By synthesizing existing literature, analyzing methodologies, and discussing practical implementations, we aim to provide insights into the efficacy and challenges of utilizing advanced algorithms in combating credit card fraud [3], [4]. Through this comprehensive exploration, we aim to contribute to the advancement of credit card fraud detection methodologies and facilitate the development of more effective and resilient fraud detection systems in the digital age [5].

The rise of online transactions and the sophistication of fraud methods have made credit card fraud detection difficult in the financial industry. Conventional fraud detection systems use rule-based algorithms to alert transactions based on thresholds or patterns. These systems can detect established fraud types, but they struggle to adapt to new patterns and small anomalies [6]. Traditional rule-based systems are restricted; thus, researchers and practitioners are using machine and deep learning. Machine learning provides more accurate and adaptable fraud detection by discovering patterns and links in past transaction data. Deep learning, a subset of machine learning, is popular for complex and unstructured data like transaction records because it automatically learns hierarchical data representations [7]. Many research has found encouraging results using machine learning and deep learning algorithms to detect credit card fraud. Random forests and gradient boosting machines can detect fraudulent transactions. Convolutional neural networks (CNNs) and recurrent neural networks (RNNs) can also capture complicated fraud patterns [8], [9]. Though fraud detection systems have improved, hurdles remain. Imbalanced datasets with more genuine than fraudulent transactions make model training and evaluation harder. Real-time fraud detection requires algorithms that adapt and learn from streaming data. Algorithm development and implementation should include fraud detection systems' ethical implications, including privacy and biases [10]. Research suggests machine learning and deep learning can detect credit card theft. By addressing past approaches' flaws and applying new algorithms, researchers and practitioners might create more resilient and adaptable fraud detection systems to prevent credit card fraud [11].

Credit card fraud detection presents a myriad of challenges stemming from the dynamic nature of fraudulent activities, the characteristics of transaction data, and the need for real-time detection. Addressing these challenges is crucial for developing effective fraud detection systems capable of accurately identifying fraudulent transactions while minimizing false positives and ensuring the smooth operation of legitimate transactions [12]. One of the primary challenges in credit card fraud detection is the imbalance between legitimate and fraudulent transactions in the dataset. Fraudulent transactions are typically rare compared to legitimate ones, resulting in imbalanced class distributions. This imbalance can lead to biased models that favour the majority class (i.e., legitimate transactions) and struggle to accurately detect fraudulent instances. Mitigating the effects of class imbalance requires specialized techniques such as oversampling of minority classes, under sampling of majority classes, or the use of cost-sensitive learning algorithms to assign higher penalties to misclassifying fraudulent transactions [13]. Fraudulent activities are constantly evolving as fraudsters develop new tactics to circumvent detection measures. Traditional rule-based systems may fail to adapt to emerging fraud patterns, as they rely on predefined rules and thresholds. Machine learning and deep learning algorithms offer a more adaptive approach by automatically learning patterns and relationships from historical transaction data. However, continuously monitoring and updating fraud detection models to keep pace with evolving fraud patterns remains a significant challenge for financial institutions [14], [15]. Timely detection of fraudulent transactions is essential for mitigating financial losses and preventing further fraudulent activities. Real-time detection requires algorithms capable of processing streaming transaction data with low latency while maintaining high accuracy. Traditional batch processing approaches may not be suitable for real-time detection, necessitating the development of specialized algorithms and infrastructure capable of handling high-volume, high-velocity data streams in real time [16]. Transaction data can have noise, missing values, and inconsistencies that might hurt fraud detection methods. Data cleansing, normalization, and feature engineering improve data quality and form. Domain expertise and rigorous research are needed to discover significant elements and extract valuable insights from transaction data [17]. Fraud detection methods create privacy, fairness, and openness issues. Accessing sensitive financial transaction data to detect fraud raises data privacy and confidentiality risks. Fairness and justice in fraud detection algorithms are also important due to algorithmic biases and demographic discrimination [18]. Advanced algorithms, data pre-processing, domain expertise, and ethics are needed to solve these problems. Financial institutions can improve fraud detection systems by using machine learning and deep learning algorithms to address credit card transaction data's unique characteristics [19].

2. METHOD

Machine learning algorithms can discover patterns and associations from historical transaction data, making them popular for credit card fraud detection. These algorithms are better at identifying complicated and changing fraud than rule-based systems because they are more adaptable and data-driven. We describe many machine learning algorithms used in credit card fraud detection, their merits, weaknesses, and applications [20]. Logistic regression is a popular classification approach that predicts the probability of a binary result (fraudulent or genuine transaction) based on one or more independent variables. Logistic regression may find linear correlations between input features and fraud likelihood despite its simplicity. However, it may struggle to capture nonlinear relationships and complicated feature interactions, limiting its ability to detect sophisticated fraud patterns [21]. Decision trees and random forests can encapsulate nonlinear data linkages and interactions under ensemble learning. Random forests use numerous decision trees to improve forecast accuracy and robustness, whereas decision trees divide the feature space into hierarchical decision nodes based on input attributes. These algorithms excel at imbalanced datasets and nonlinear fraud patterns. They may overfit, especially with big, high-dimensional datasets [22]. SVMs classify data points by determining the best hyperplane to divide them. SVMs capture complex feature space decision boundaries and work effectively with high-dimensional data. They excel at binary classification jobs like fraud detection. SVMs can be computationally expensive and require careful hyper parameter tweaking, especially with large datasets [23]. Gradient boosting machines (GBMs) successively integrate weak learners like decision trees to increase predicting performance. GBMs iteratively fit new models to previous model residuals, minimizing prediction error. GBMs are adaptable and can capture complex nonlinear data correlations. These methods excel at skewed datasets and have been used to detect credit card fraud [24]. Isolation forests and one-class SVMs discover data anomalies by recognizing unusual outliers. These methods are ideal for detecting fraudulent transactions, which often have unusual patterns. In rare cases of fraud with unclear patterns, anomaly detection systems work well. They may struggle with severely imbalanced datasets and need careful detection threshold calibration [25]. Each credit card fraud detection technology using machine learning algorithms has pros and cons. Financial institutions can create resilient and adaptable fraud detection systems that reduce fraud risks by using these algorithms with effective feature engineering and model evaluation methods [26].

Deep learning can detect credit card fraud by automatically learning complex patterns and representations from massive transaction data. Unlike standard machine learning approaches, deep learning algorithms can represent complicated nonlinear interactions and detect fraud. This section discusses the uses, strengths, and considerations of many deep learning architectures for credit card fraud detection. CNNs are used for picture recognition and sequential data analysis, including transaction sequences. Credit card fraud can be detected using CNNs extracting timestamps, amounts, and merchant IDs from transaction data. CNNs learn hierarchical representations of fraudulent patterns using convolutional operations on transaction sequences to detect fraud. CNNs detect local patterns and transaction sequence inconsistencies well. RNNs can represent sequential data with temporal relationships, making them excellent for credit card fraud detection. RNNs process input sequences one element at a time and store temporal information. Because they capture long-range relationships and alleviate the vanishing gradient problem, LSTM and GRU RNNs are used in fraud detection. Encoding transaction sequences into latent representations and learning fraud patterns helps RNNs detect fraud. Autoencoders recover input data by encoding it in a lower-dimensional latent space. To detect credit card fraud anomalies, autoencoders learn to recreate authentic transaction data and identify deviations from the learned distribution as fraudulent. Variational and Sparse Autoencoders can identify fraud by learning compact transaction data representations and detecting abnormal patterns. Autoencoders can detect anomalous and non-trendy fraud [27]. Hybrid designs optimize performance using CNNs, RNNs, and autoencoders. CNNs may extract spatial features from transaction data and pass them to an RNN for temporal modeling in a hybrid architecture. Hybrid architectures with many deep learning components can capture complex transaction sequence patterns and temporal correlations, improving fraud detection systems. Deep learning techniques detect credit card fraud, however data pretreatment, model interpretability, and computational complexity are concerns. Preprocessing transaction data to identify critical features and normalize input values is crucial for deep learning model development. As black boxes, deep learning models' conclusions and fraud detection factors are hard to explain. Deep learning models may need plenty of computer power for training and inference on large datasets. Deep learning can detect credit card fraud using complex transaction patterns and temporal correlations. CNNs, RNNs, autoencoders, and hybrid architectures can help financial institutions build resilient and adaptive fraud detection systems. Deep learning-based fraud detection systems require data preparation, model interpretability, and computational complexity [28], [29]. Feature engineering is needed to create robust credit card fraud detection systems. Transaction data can reveal fraud. Common fraud detection approaches include transaction data analysis and feature extraction [30].

3. RESULTS AND DISCUSSION

This section showcases case studies and real implementations of credit card fraud detection with machine learning and deep learning methods. These examples demonstrate how fraud detection systems are used in real-world scenarios, illustrating the efficacy of advanced techniques in preventing fraudulent activity. The utilization of powerful machine learning and deep learning algorithms for credit card fraud detection has become an essential instrument in guaranteeing the security and reliability of online transactions. By utilizing these technologies, firms can identify and thwart fraudulent activity, safeguard their clients from monetary losses, and maintain trust and assurance in digital payment systems.

A model of classification visualisation shows the projected model fit to the findings previously linked to the earlier ones using a confusion measure. A common practice is to store the expected outcomes in a variable before transforming it into an association table. It is possible to plot the confusion metrics using the association table as a heatmap. We can build and show confusion measures based on the score to allow for better correlation, even if there are multiple built-in techniques to do so. The metrics for machine learning algorithms' perplexity are shown in Figure 1.

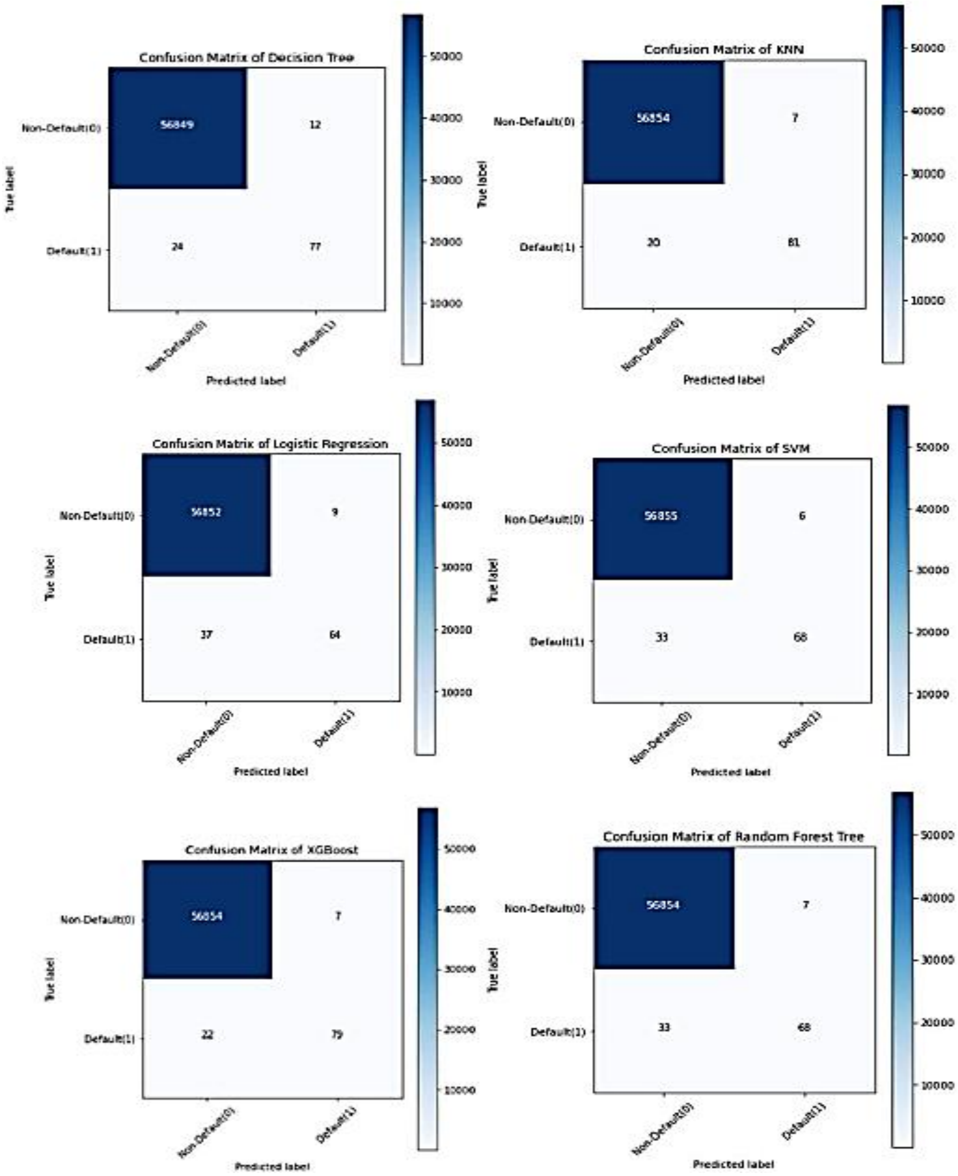

Figure 1. Metrics for measuring algorithmic confusion in machine learning

Figure 2, which displays the case count statistics, shows that the 'Amount' variable's' values change significantly once they are linked to the variables' respites. We may standardize it using Python's 'Standard-Scaler' technique to reduce the broad range of values. Figure 3 displays a comparative comparison of machine learning techniques applied to CCF, employing accuracy and F1 measure metrics. To facilitate the comparison of the losses, we train the model for either thirty or forty epochs, with or without rigorous initialization, depending on our preference. From the perspective of validation loss, the graphic makes it very evident that cautious initialization provides a distinct advantage. Figure 4 illustrates the validation loss that occurs when both zero bias and cautious bias principles are applied. Figure 5 offers an illustration of the training and validation accuracy of the proposed model over a period of 20 and 50 epochs, respectively, over a period of 30 and 60 epochs.

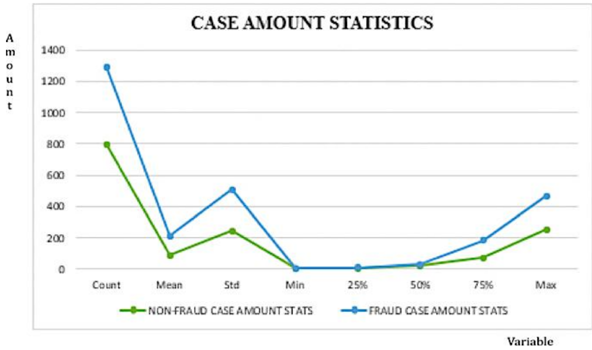

Figure 2. The numbers of cases involving both fraudulent and legitimate transactions

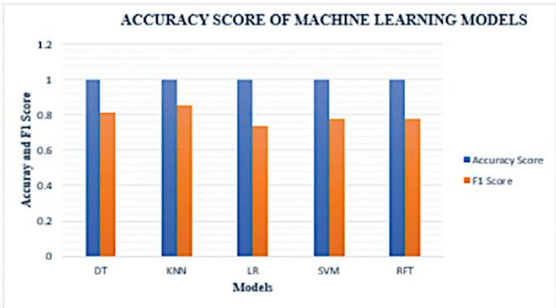

Figure 3. The evaluation of various machine learning methods for CCF based on their accuracy

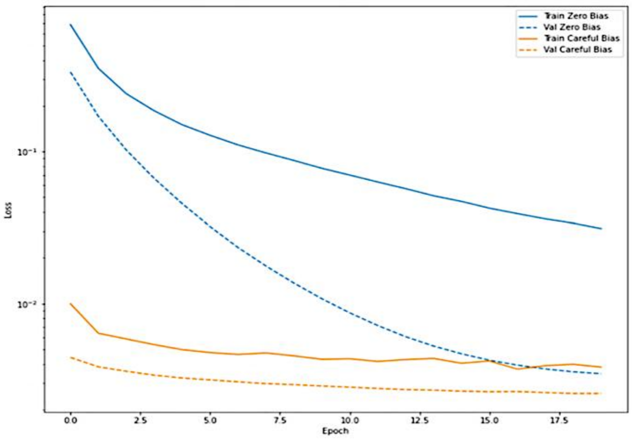

Figure 4. The reduction in validity when employing mindful bias and zero bias

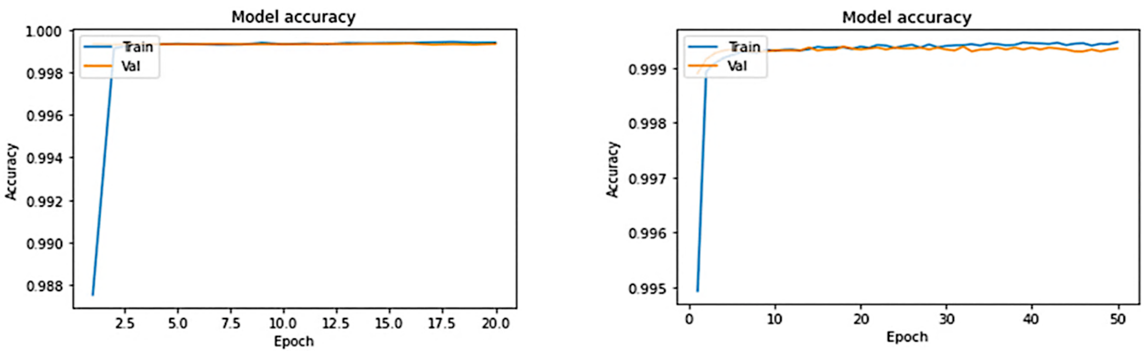

Figure 5. Precision of the model at 30 and 60 epochs

4. CONCLUSION

Credit card fraud detection is a critical challenge facing financial institutions and consumers in the digital age. Traditional rule-based systems have limitations in effectively detecting sophisticated fraudulent activities, necessitating the adoption of advanced machine learning and deep learning algorithms. In this research paper, we have explored the application of state-of-the-art techniques for credit card fraud detection, including machine learning algorithms such as random forests and gradient boosting machines, as well as deep learning architectures such as CNNs and RNNs. We have shown that these methods may detect fraudulent transactions and reduce financial losses through case studies and actual applications. Organizations can create powerful fraud detection systems that identify fraudulent patterns and anomalies by using transaction data and extracting significant information. Additionally, model evaluation metrics and approaches allow enterprises to evaluate their fraud detection models' performance and dependability and make educated model selection and optimization decisions.

ACKNOWLEDGMENTS

The authors would like to express their sincere gratitude to Organizations for their support and assistance throughout this research. We also extend our appreciation to our colleagues and peers for their valuable insights and constructive feedback, which contributed to the improvement of this study. Finally, we thank our families and friends for their encouragement and support during this research journey.

FUNDING INFORMATION

The authors declare that no funding was received for this research.

AUTHOR CONTRIBUTIONS STATEMENT

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Indurthi Ravindra Kumar	✓	✓	✓	✓				✓	✓	✓			✓	
Shaik Abdul Hameed	✓	✓			✓	✓	✓	✓	✓	✓	✓	✓		
Bala Annapurna	✓		✓			✓			✓		✓		✓	
Rama Krishna Paladugu	✓	✓	✓	✓					✓		✓			
Veeramreddy Surya Narayana Reddy	✓	✓	✓	✓	✓		✓			✓		✓		
Kiran Kumar Kaveti	✓		✓			✓			✓		✓		✓	

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal analysis
I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting
Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject administration
Fu : **Fu**nding acquisition

CONFLICT OF INTEREST STATEMENT

The authors declare that they have no conflicts of interest related to this research.

ETHICAL APPROVAL

This research does not involve human participants, animals, or sensitive data requiring ethical approval.

DATA AVAILABILITY

The data supporting the findings of this study are available from the corresponding author upon reasonable request.

REFERENCES

[1] K. Patel, "Credit card analytics: a review of fraud detection and risk assessment techniques," *International Journal of Computer Trends and Technology*, vol. 71, no. 10, pp. 69–79, Oct. 2023, doi: 10.14445/22312803/ijctt-v71i10p109.

[2] W. Hilal, S. A. Gadsden, and J. Yawney, "Financial fraud: a review of anomaly detection techniques and recent advances," *Expert Systems with Applications*, vol. 193, p. 116429, May 2022, doi: 10.1016/j.eswa.2021.116429.

[3] A. Cherif, A. Badhib, H. Ammar, S. Alshehri, M. Kalkatawi, and A. Imine, "Credit card fraud detection in the era of disruptive technologies: A systematic review," *Journal of King Saud University - Computer and Information Sciences*, vol. 35, no. 1, pp. 145–174, Jan. 2023, doi: 10.1016/j.jksuci.2022.11.008.

[4] A. R. Khalid, N. Owoh, O. Uthmani, M. Ashawa, J. Osamor, and J. Adejoh, "Enhancing credit card fraud detection: an ensemble machine learning approach," *Big Data and Cognitive Computing*, vol. 8, no. 1, p. 6, Jan. 2024, doi: 10.3390/bdcc8010006.

[5] E. Ileberi, Y. Sun, and Z. Wang, "A machine learning based credit card fraud detection using the GA algorithm for feature selection," *Journal of Big Data*, vol. 9, no. 1, p. 24, Dec. 2022, doi: 10.1186/s40537-022-00573-8.

[6] S. Gbadebo-Ogunmefun, A. G. Oketola, T. Gbadebo-Ogunmefun, and A. Agbeja., "A review of credit card fraud detection using machine learning algorithms," 2023.

[7] A. Aldoseri, K. N. Al-Khalifa, and A. M. Hamouda, "Re-thinking data strategy and integration for artificial intelligence: concepts, opportunities, and challenges," *Applied Sciences (Switzerland)*, vol. 13, no. 12, p. 7082, Jun. 2023, doi: 10.3390/app13127082.

[8] I. D. Mienye and Y. Sun, "A deep learning ensemble with data resampling for credit card fraud detection," *IEEE Access*, vol. 11, pp. 30628–30638, 2023, doi: 10.1109/ACCESS.2023.3262020.

[9] M. A. Islam, M. A. Uddin, S. Aryal, and G. Stea, "An ensemble learning approach for anomaly detection in credit card data with imbalanced and overlapped classes," *Journal of Information Security and Applications*, vol. 78, p. 103618, Nov. 2023, doi: 10.1016/j.jisa.2023.103618.

[10] B. Borketey, "Real-time fraud detection using machine learning," *Journal of Data Analysis and Information Processing*, vol. 12, no. 02, pp. 189–209, Jan. 2024, doi: 10.4236/jdaip.2024.122011.

[11] M. Elahi, S. O. Afolaranmi, J. L. M. Lastra, and J. A. P. Garcia, "A comprehensive literature review of the applications of AI techniques through the lifecycle of industrial equipment," *Discover Artificial Intelligence*, vol. 3, no. 1, Dec. 2023, doi: 10.1007/s44163-023-00089-x.

[12] M. Zareapoor, S. K. Seeja, and M. A.Alam, "Analysis on credit card fraud detection techniques: based on certain design criteria," *International Journal of Computer Applications*, vol. 52, no. 3, pp. 35–42, Aug. 2012, doi: 10.5120/8184-1538.

[13] A. Singh, R. K. Ranjan, and A. Tiwari, "Credit card fraud detection under extreme imbalanced data: a comparative study of data-level algorithms," *Journal of Experimental and Theoretical Artificial Intelligence*, vol. 34, no. 4, pp. 571–598, Apr. 2022, doi: 10.1080/0952813X.2021.1907795.

[14] L. Shaikh, B. Patil, S. Ramteke, R. Sudan, and M. Khajuria, "Credit card fraud detection using machine learning algorithms," 2023.

[15] P. Hajek, M. Z. Abedin, and U. Sivarajah, "Fraud detection in mobile payment systems using an XGBoost-based framework," *Information Systems Frontiers*, vol. 25, no. 5, pp. 1985–2003, Oct. 2023, doi: 10.1007/s10796-022-10346-6.

[16] A. Diro, S. Kaisar, A. V. Vasilakos, A. Anwar, A. Nasirian, and G. Olani, "Anomaly detection for space information networks: a survey of challenges, techniques, and future directions," *Computers and Security*, vol. 139, Jul. 2024, doi: 10.1016/j.cose.2024.103705.

[17] B. N. Bhukya *et al.*, "Integrating the internet of things to protect electric vehicle control systems from cyber attacks," *IAENG International Journal of Applied Mathematics*, vol. 54, no. 3, 2024.

[18] A. Ali *et al.*, "Financial fraud detection based on machine learning: a systematic literature review," *Applied Sciences (Switzerland)*, vol. 12, no. 19, p. 9637, Sep. 2022, doi: 10.3390/app12199637.

[19] M. A. Ahmed and S. Alnatheer, "A novel approach for detecting sensor-based semiconductor fault yield classification using convolutional neural networks," *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS)*, vol. 33, no. 3, pp. 1448–1464, Mar. 2024, doi: 10.11591/ijeecs.v33.i3.pp1448-1464.

[20] T. S. Anagha, A. Fathima, A. D. Naik, C. Goenka, S. B. Devamane, and A. R. Thimmapurmath, "Credit card fraud detection using machine learning algorithms," *Proceedings - 2023 International Conference on Computational Intelligence for Information, Security and Communication Applications, CIISCA 2023*, vol. 12, no. 11, pp. 419–424, Nov. 2023, doi: 10.1109/CIISCA59740.2023.00085.

[21] S. Masrom, R. A. Rahman, N. H. M. Shukri, N. A. Yahya, M. Z. A. Rashid, and N. B. Zakaria, "The nexus of corruption and non-performing loan: machine learning approach," *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS)*, vol. 32, no. 2, pp. 838–844, Nov. 2023, doi: 10.11591/ijeecs.v32.i2.pp838-844.

[22] Q. Dong, X. Chen, and B. Huang, "Decision trees and ensemble learning," in *Data Analysis in Pavement Engineering*, Elsevier, 2024, pp. 211–222.

[23] M. Awad and R. Khanna, "Support vector machines for classification," in *Efficient Learning Machines*, Apress, 2015, pp. 39–66.

[24] A. Natekin and A. Knoll, "Gradient boosting machines, a tutorial," *Frontiers in Neurorobotics*, vol. 7, no. DEC, 2013, doi: 10.3389/fnbot.2013.00021.

[25] M. Almansoori and M. Telek, "Anomaly detection using combination of autoencoder and isolation forest," in *1st Workshop on Intelligent Infocommunication Networks, Systems and Services*, 2023, pp. 25–30, doi: 10.3311/wins2023-005.

[26] A. A. Almazroi and N. Ayub, "Online payment fraud detection model using machine learning techniques," *IEEE Access*, vol. 11, pp. 137188–137203, 2023, doi: 10.1109/ACCESS.2023.3339226.

[27] J. Chaquet-Ulldemolins, F. J. Gimeno-Blanes, S. Moral-Rubio, S. Muñoz-Romero, and J. L. Rojo-álvarez, "On the black-box challenge for fraud detection using machine learning (ii): nonlinear analysis through interpretable autoencoders," *Applied Sciences (Switzerland)*, vol. 12, no. 8, p. 3856, Apr. 2022, doi: 10.3390/app12083856.

[28] A. Roy, J. Sun, R. Mahoney, L. Alonzi, S. Adams, and P. Beling, "Deep learning detecting fraud in credit card transactions," *2018 Systems and Information Engineering Design Symposium, SIEDS 2018*, pp. 129–134, 2018, doi: 10.1109/SIEDS.2018.8374722.

[29] A. C. Bahnsen, D. Aouada, A. Stojanovic, and B. Ottersten, "Feature engineering strategies for credit card fraud detection," *Expert Systems with Applications*, vol. 51, pp. 134–142, Jun. 2016, doi: 10.1016/j.eswa.2015.12.030.

[30] S. K. Hashemi, S. L. Mirtaheri, and S. Greco, "Fraud detection in banking data by machine learning techniques," *IEEE Access*, vol. 11, pp. 3034–3043, 2023, doi: 10.1109/ACCESS.2022.3232287.

BIOGRAPHIES OF AUTHORS

Mr. Indurthi Ravindra Kumar is working as assistant professor in the Department of Computer Science and Engineering at VNR Vignan Jyothi Institute of Engineering and Technology, Hyderabad. He registered Ph.D. in Andhra University and Completed his M.Tech. from Andhra University, Visakhapatnam from C R Reddy college of engineering in the year 2014. He has more than 8+Years of Teaching Experience. He has published more than 7 research articles published in international journals, conferences. His research interest includes machine learning, pattern recognition, computer vision, image processing, deep learning. He can be contacted at email: indurthiravindrakumar@gmail.com.

Mr. Shaik Abdul Hameed is working as assistant professor in the Department of Computer Science and Engineering at VNR Vignan Jyothi Institute of Engineering and Technology, Hyderabad. He Completed his M.Tech. from JNTUH in the year of 2019. He has 4+Years of Teaching Experience. He has published 2 research articles published in international journals. His research interest includes network security, pattern recognition, data mining, data analysis, deep learning. He can be contacted at email: hameeduser4@gmail.com.

Dr. Bala Annapurna associate professor, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vijayawada, Andhra Pradesh. I have been actively engaged in academic and research endeavors for more than twenty-five years, making substantial contributions to the scholarly community during this time. My research interests encompass a wide range of topics in computer science and engineering, with a specific focus on data mining. I am deeply engaged in research areas such as clustering and regression analysis and have a strong commitment to pushing the boundaries of knowledge in these fields. She can be contacted at email: annapurnagandrety@gmail.com.

Rama Krishna Paladugu is an assistant professor in Computer Science and Engineering department at R.V.R. and J.C. College of Engineering, Chowdavaram, Guntur, Andhra pradesh, India and is a research scholar at Acharya Nagarjuna University, Guntur, Andhra Pradesh, India. His research interests are data mining, information retrieval systems, software engineering. He can be contacted at email: mails4prk@gmail.com.

Dr. Veeramreddy Surya Narayana Reddy obtained his B. Tech from JNTU, Ananthapur in 2012. He received his Master of Technology from JNTU, Ananthapur in 2014. He received his Ph.D. in 2023 from Visvesvaraya Technological University, Belagavi, Karnataka. Currently, he is working as an assistant professor in the Department of CSE at BVRIT, Hyderabad College of Engineering for Women, Hyderabad, India. His areas of interest are data mining, deep learning, machine learning, and network security. He has published more than 10 papers in National and International Journals. He can be contacted at email: veeramreddysurya@gmail.com.

Mr. Kiran Kumar Kaveti is assistant professor in the Department of Computer Science and Engineering, Vignan’s Foundation for Science Technology and Research Vadlamudi, Guntur, India. Pursuing Ph.D. from Pondicherry University, India. His primary research areas are image segmentation using deep learning-based transfer learning techniques. He can be contacted at email: kirankumar.institute@gmail.com.