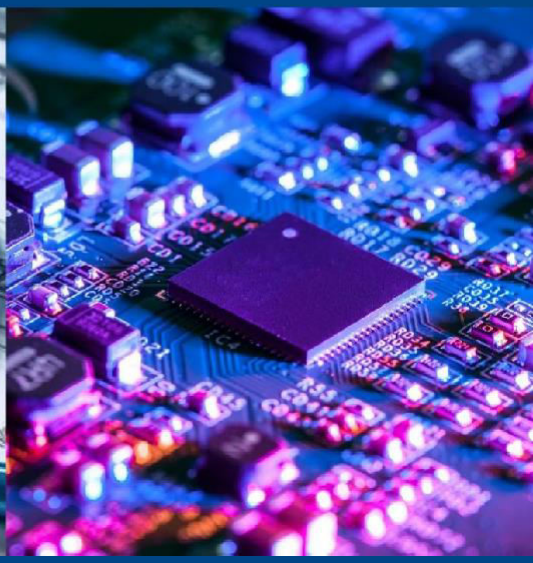
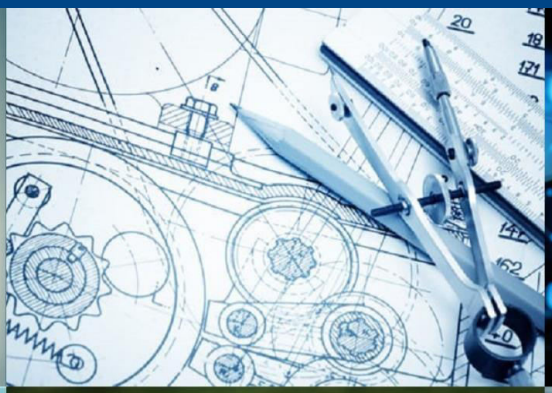
ISSN: 2582-7219

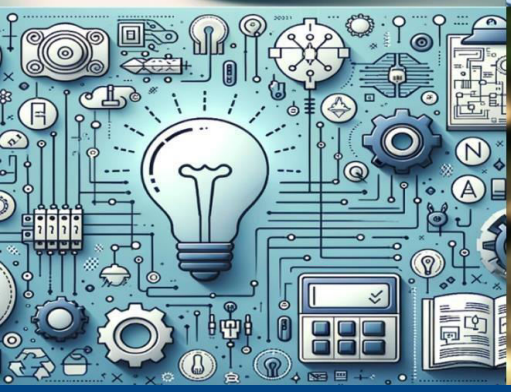




International Journal of Multidisciplinary Research in Science, Engineering and Technology

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.206 **Volume 8, Issue 7, July 2025**

© 2025 IJMRSET | Volume 8, Issue 7, July 2025| DOI:10.15680/IJMRSET.2025.0807049

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Intelligent Credit Card Fraud Detection System with Adaptive Response Mechanism

P. Shenbagam[1], A. Alex Pandi[2]

Assistant Professor, Department of MCA, RVS College of Engineering, Dindigul, Tamil Nadu, India[1]

MCA Student, RVS College of Engineering, Dindigul, Tamil Nadu, India[2]

ABSTRACT: In recent times, credit card fraud has emerged as a substantial financial challenge for both cardholders and the issuing authorities. To address this demanding issue, researchers have employed machine learning techniques to identify fraudulent activities within labeled transaction records. However, these techniques have primarily been evaluated on limited or specific datasets, which may not adequately represent the broader real-world scenario. These limitations motivated us to comprehensively assess the existing machine learning classifiers and propose an Optimized Deep Event-based Network (OptDevNet) framework capable of addressing these challenges. To evaluate the performance of the proposed model, we implemented and assessed five different machine learning classifiers using the well-known Credit Card Fraud Detection (CCFD) Dataset. Upon careful analysis, we found that our model surpasses these classifiers in terms of fraudulent transaction detection accuracy. Given these findings, we are confident that our proposed model has the potential for effective real-world deployment in detecting and preventing malicious transactions.

KEYWORDS: Credit card fraud detection, OptDevNet framework, automatic fraud detection, malicious transactions, credit card security.

I. INTRODUCTION

In the rapidly evolving financial sector, machine learning techniques have emerged as a game-changer, particularly in credit risk assessment and fraud detection. The rise of fintech and the availability of vast amounts of data have paved the way for leveraging advanced algorithms to tackle complex financial challenges that were once seen as too difficult to overcome . At the forefront of this revolution is credit risk assessment, where machine learning models can analyze intricate data patterns and extract valuable insights, enabling more accurate risk profiling and credit scoring. Techniques like extremely randomized trees (XRT)

support vector machines (SVM), and deep neural networks (DNN) have demonstrated superior performance compared to traditional statistical methods, ushering in a new era of precision and efficiency in lending decisions . Moreover, machine learning has

support vector machines (SVM), and deep neural networks (DNN) have demonstrated superior performance compared to traditional statistical methods, ushering in a new era of precision and efficiency in lending decisions. Moreover, machine learning has proven to be an invaluable ally in the battle against fraudulent credit card transactions. Convolutional neural proven to be an invaluable ally in the battle against fraudulent credit card transactions. Convolutional neural networks, for instance, can effectively learn and identify fraudulent patterns of transactions in large datasets. Therefore, these models often outperform traditional systems, which may struggle to keep pace with the ever-evolving strategies of cybercriminals . Their ability to continuously learn and adapt to changing situations gives them an advantage over traditional techniques, ensuring that financial institutions remain vigilant and proactive in protecting their customers' assets .

To address these challenges, we evaluate various machine learning algorithms using the well-known ''CCFD'' dataset to assess their performance. Furthermore, we propose an Optimized Deep Event- based Network (OptDevNet) to mitigate the issues of false negatives and false positives. networks, for instance, can effectively learn and identify fraudulent patterns of support vector machines (SVM), and deep neural networks (DNN) have demonstrated superior performance compared to traditional statistical methods, ushering in a new era of precision and efficiency in

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

However, using machine learning algorithms in finance sector creates many problems. Some of these concerns revolve around the interpretability of systems and applica- tions, which is followed by some additional challenges such as biases and regulatory standards, etc. Therefore, addressing these issues is imperative to guarantee the conscientious and ethical implementation of these algorithms in technological advancements . Nonetheless, the potential benefits of these algorithms—such as improved risk management, enhanced fraud detection, and optimized lending decision processes—make them an indispensable tool for the future financial sector. As fintech continues to disrupt traditional finance, the synergy between cutting-edge machine learn- ing techniques and traditional finance increases, helping to secure the financial sector. The deployment of new algorithms enables more secure, efficient, and reliable financial systems worldwide. This symbiotic relationship will not only strengthen the financial sector but also foster economic growth and stability, benefiting individuals and businesses

However, machine learning (ML), deep reinforcement learning (DRL), deep learning (DL), and transfer learning (TL) algorithms face challenges related to the occurrence of 'false negatives' (FN) and 'false positives' (FP) . False negatives occur when the algorithm fails to detect fraudulent transactions, which can negatively impact an organization's revenue. On the other hand, false positives happen when a legitimate customer or user transaction is mistakenly flagged as fraudulent or illegitimate, resulting in customer dissatisfaction, loss of trust, and financial losses. Notably, as indicated in , FRISS has pinpointed that false positives (FPs) represent one of the most formidable challenges in detecting fraud in online transactions. This challenge is particularly relevant in the financial sector, where the adoption of machine learning techniques for credit risk assessment and fraud detection is gaining traction. While machine learning models have demonstrated superior performance compared to traditional statistical methods in credit risk profiling and credit scoring, the issue of false positives remains a critical consideration. Inaccurately flag- ging legitimate transactions as fraudulent can erode customer trust and loyalty, ultimately undermining the legitimacy of financial institutions that aim to safeguard their clients' assets.

In the domain of fraud detection, the prowess of machine learning techniques like CNN has shown valuable results in the identification of frauds. However, their usefulness diminishes if they generate too many false alerts, leading to unnecessary investigations and potentially alienating cus- tomers. Tackling the issue of false positives is paramount for the conscientious and ethical application of these innovations in the financial sector. Credit card fraud happens when someone uses a credit card without permission of the owner to make an unauthorized transaction. It is a common form of financial deception where individuals misuse someone else's card without their knowledge/consent . Financial organizations continually seek novel strategies to combat fraud by considering the potential risks of fraudulent transactions. However, fraudsters are also working to exploit newly adopted technologies using innovative techniques. This ongoing challenge necessitates the development of highly efficient and effective algorithms . In this scenario, the utilization of machine learning algorithms play a vital role to identifying fraudulent transactions. However, as discussed earlier, the occurrence of false negatives and false positives poses a significant challenges to these algorithms.

To address these challenges, we evaluate various machine learning algorithms using the well-known ''CCFD'' dataset to assess their performance. Furthermore, we propose an Optimized Deep Event-based Network (OptDevNet) to mitigate the issues of false negatives and false positives. The main highlights of this work are summarized as follows:

1. We start by conducting a comprehensive performance evaluation of various machine learning algorithms on the well-known Credit Card Fraud Detection (CCFD) dataset. This rigorous evaluation helps and provides valuable insights about the efficiency of these algo- rithms in detecting fraudulent credit card transactions.
2. Subsequently, we propose an Optimized Deep Event-based Network (OptDevNet) framework designed to address the limitations of existing algorithms in online credit card fraud detection. Fur- thermore, the proposed model enhances the accuracy and efficiency of fraudulent transaction identification by harnessing the capabilities of optimized event-based deep neural network architectures.
3. We also assess how well the proposed model can reduce false positives and false negatives. This evaluation helps determine how effectively the model identifies fraud, which is important for increasing customer satisfaction and revenue.
4. Through rigorous evaluation, OptDevNet demonstrates significant improvements in fraud detection accu- racy, ultimately benefiting financial organizations by mitigating financial losses and enhancing customer satisfaction.
5. Finally, we comprehensively assess the effectiveness of our proposed model against existing machine learning models using various comparative metrics, demonstrating its superior performance and robustness in CCFD.

© 2025 IJMRSET | Volume 8, Issue 7, July 2025| DOI:10.15680/IJMRSET.2025.0807049

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

II. EXISTING SYSTEM

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Credit card fraud has become a persistent and complex issue in the financial industry, leading to substantial monetary losses, reputational damage, and a lack of customer trust. Fraudsters employ increasingly sophisticated tactics, making it challenging for traditional fraud detection systems to identify fraudulent transactions accurately. Conventional methods often rely on rule- based approaches and static models that struggle to detect evolving and dynamic fraud patterns, resulting in high false positive rates, delayed detection, and undetected fraudulent activities. These limitations compromise transaction security, increase operational costs, and create friction for legitimate customers through unnecessary transaction denials. Additionally, existing fraud detection systems face challenges in processing large-scale, high-dimensional transactional data. They often fail to capture intricate temporal patterns and sequential dependencies that are essential for accurate fraud detection. The inability to adapt to new fraud techniques and analyze real-time data exacerbates the vulnerability of financial institutions, making them susceptible to emerging threats. The lack of a proactive, risk-based response mechanism further limits the effectiveness of traditional systems in preventing fraudulent transactions. To address these challenges, there is a pressing need for an advanced, intelligent fraud detection system that can accurately analyze sequential transaction data, adapt to evolving fraud strategies, and minimize false positives while ensuring a smooth experience for genuine users. Leveraging LSTM-based deep learning techniques combined with an adaptive response mechanism can significantly enhance the detection and prevention of credit card fraud.

III. PROPOSED SYSTEM

The proposed system introduces an advanced fraud detection mechanism using Long Short-Term Memory (LSTM) networks to enhance the security of e-commerce transactions. It intelligently detects fraudulent activities by analyzing transaction patterns and implements a risk-based response system to prevent unauthorized transactions.

The system employs Long Short-Term Memory (LSTM) networks to detect fraudulent transactions with high accuracy. It analyzes past transaction patterns, extracts hidden state and cell state features, and classifies transactions as legitimate or fraudulent. By learning sequential dependencies, LSTM effectively identifies anomalies in user behavior.

The system continuously monitors transactions in real time, assessing risk factors such as IP address, geolocation, device information, BIN data, and user behavior. This allows for immediate fraud detection, minimizing financial losses.

Instead of generating an OTP for transactions suspected of fraud, the system prevents unauthorized payments by displaying a "Server Down" or "Server Busy" message. This approach reduces the chances of fraudsters bypassing authentication and improves security.

If a fraudulent transaction is detected, the system triggers automated alerts to notify the admin and customer. It also generates detailed fraud reports, enabling further analysis and manual review of high- risk transactions.

The fraud detection model is deployed within the E- Commerce Web Application, ensuring smooth transaction processing without disrupting the user experience. It integrates with existing

payment gateways and backend systems for enhanced security. These limitations compromise transaction security, increase operational costs, and create friction for legitimate customers through unnecessary transaction denials. Additionally, existing fraud detection systems face challenges in processing large-scale, high-dimensional transactional data. They often fail to capture intricate temporal patterns and sequential dependencies that are essential for accurate fraud detection. The inability to adapt to new fraud techniques and analyze real-time data exacerbates the vulnerability of financial institutions, making them susceptible to emerging threats. The lack of a proactive, risk-based response mechanism further limits the effectiveness of traditional systems in preventing fraudulent transactions. To address these challenges, there is a pressing need for an advanced, intelligent fraud detection system that can accurately analyze sequential transaction data, adapt to evolving fraud strategies, and minimize false positives while ensuring a smooth experience for genuine users. Leveraging LSTM-based deep learning techniques combined with an adaptive response mechanism can significantly enhance the detection and prevention of credit card fraud.

However, using machine learning algorithms in finance sector creates many problems. Some of these concerns revolve around the interpretability of systems and applica- tions, which is followed by some additional challenges such as

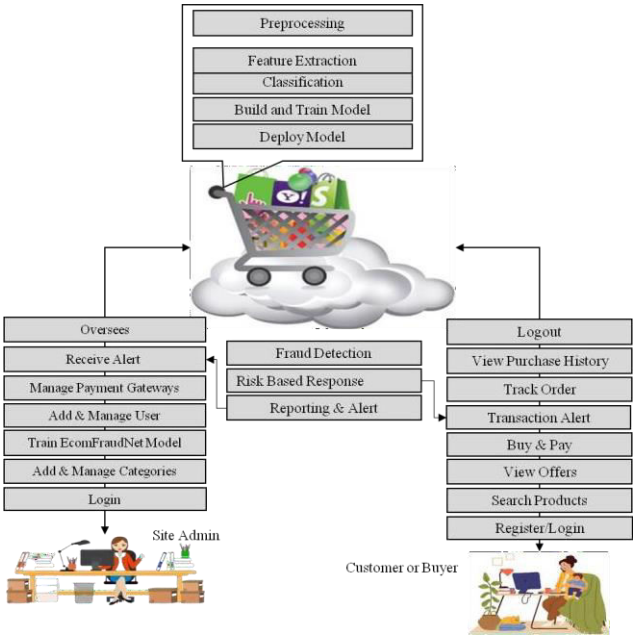
ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

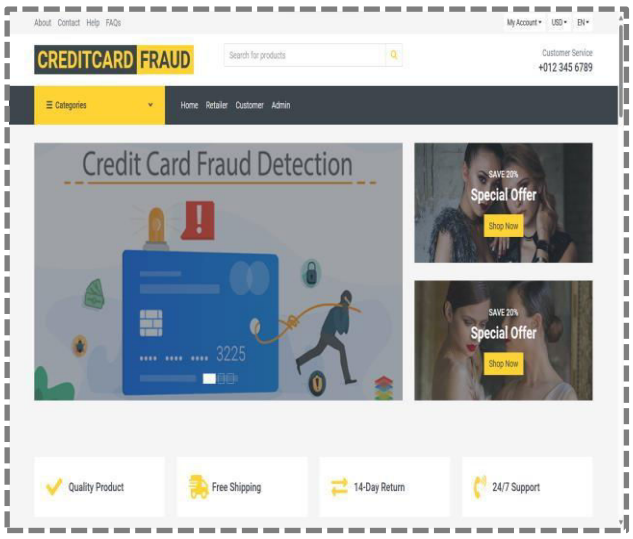
(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

biases and regulatory standards, etc. Therefore, addressing these issues is imperative to guarantee the conscientious and ethical implementation of these algorithms in technological advancements . Nonetheless, the potential benefits of these algorithms—such as improved risk management, enhanced fraud detection, and optimized lending decision processes—make them an indispensable tool for the future financial sector. As fintech continues to disrupt traditional finance, the synergy between cutting-edge machine learn- ing techniques and traditional finance increases, helping to secure the financial sector. The deployment of new algorithms enables more secure, efficient, and reliable financial systems worldwide. This symbiotic relationship will not only strengthen the financial sector but also foster economic growth and stability, benefiting individuals and businesses .

IV. SYSTEM ARCHITECTURE



V. RESULTS

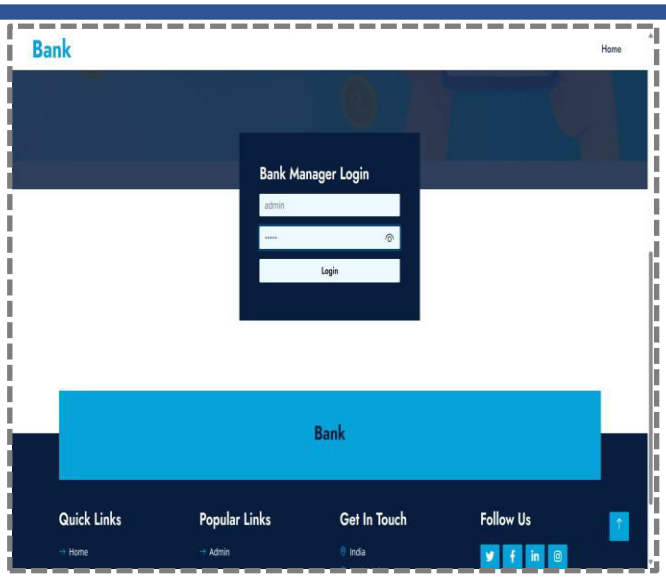


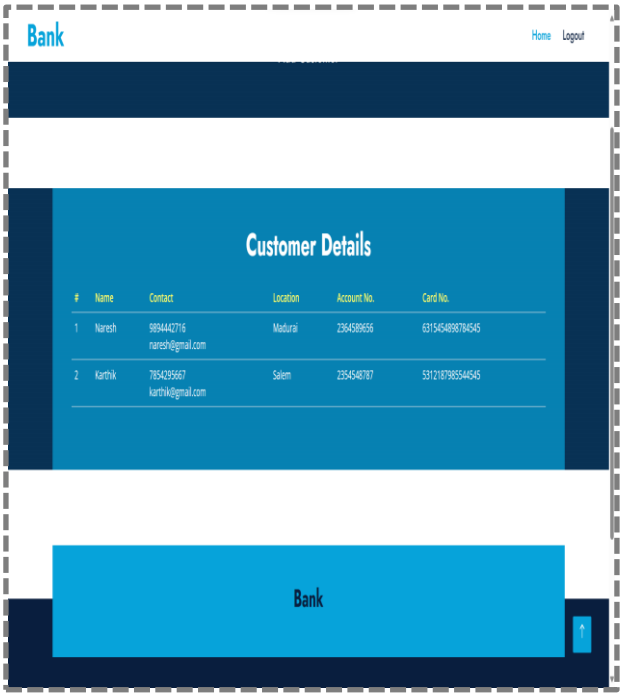
© 2025 IJMRSET | Volume 8, Issue 7, July 2025| DOI:10.15680/IJMRSET.2025.0807049

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)





VI. CONCLUSION

In this study, we introduced an Optimized Deep Event-based Network (OptDevNet) framework for detecting and prevent- ing fraudulent transactions. The motivation for this work comes from the increasing security threat posed by credit card fraud (CCF), which presents a significant challenge to financial institutions. Fraudsters continuously employ new techniques to compromise the security of these systems. Moreover, we noted in the literature that the effectiveness of these systems relies on machine learning (ML)-)-enabled algorithms, which privately depend on specific use cases and the features of the input data to perform this task. Traditional deep learning (DL) algorithms, such as convolutional neural networks (CNNs), have shown promising results compared to ML algorithms, but they have yet to achieve remarkable results. We evaluated the proposed model against rival algo- rithms, including support vector machines (SVM), logistic regression, random forest, and K-nearest neighbors (KNN) on the CCFD dataset. Our analysis achieves an exceptional accuracy by surpassing both the evaluated algorithms and existing state-of-the-art schemes. Notably, we

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

observed that the performance on unseen data improved as class imbalance increased. Given that, we are confident that the proposed model will effectively meet the requirements of involved stakeholders.

REFERENCES

1. R. B. Sulaiman, V. Schetinin, and P. Sant, ''Review of machine learning approach on credit card fraud detection,'' *Hum.-Centric Intell. Syst.*, vol. 2, nos. 1–2, pp. 55–68, 2022.
2. 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,'' *J. King Saud Univ., Comput. Inf. Sci.*, vol. 35, no. 1,pp. 145–174, Jan. 2023.
3. Y. Zhang, M. Jamjoom, and Z. Ullah, ''Double deep Q-network next- generation cyber-physical systems: A reinforcement learning-enabled anomaly detection framework for next-generation cyber-physical sys- tems,'' *Electronics*, vol. 12, no. 17, p. 3632, Aug. 2023.
4. N. S. Alfaiz and S. M. Fati, ''Enhanced credit card fraud detection model using machine learning,'' *Electronics*, vol. 11, no. 4, p. 662, Feb. 2022.
5. E. Esenogho, I. D. Mienye, T. G. Swart, K. Aruleba, and G. Obaido, ''A neural network ensemble with feature engineering for improved credit card fraud detection,'' *IEEE Access*, vol. 10, pp. 16400–16407, 2022.
6. J. F. Roseline, G. B. S. R. Naidu, V. S. Pandi, S.A. Rajasree, and N. Mageswari, ''Autonomous credit card fraud detection using machine learning approach,'' *Comput. Elect. Eng.*, vol. 102, Sep. 2022, Art. no. 108132.
7. I. Park, D. Kim, J. Moon, S. Kim, Y. Kang, and S. Bae, ''Searching for new technology acceptance model under social context: Analyzing the determinants of acceptance of intelligent information technology in digital transformation and implications for the requisites of digital sustainability,'' *Sustainability*, vol. 14, no. 1, p. 579, Jan. 2022.
8. T. Hewavitharana, S. Nanayakkara, A. Perera, and P. Perera, ''Modifying the unified theory of acceptance and use of technology (UTAUT) model for the digital transformation of the construction industry from the user perspective,'' *Informatics*, vol. 8, no. 4, p. 81,Nov. 2021.
9. P. K. Sadineni, ''Detection of fraudulent transactions in credit card using machine learning algorithms,'' in *Proc. 4th Int. Conf. I-SMAC*, Oct. 2020,pp. 659–660.
10. J. R. D. Kho and L. A. Vea, ''Credit card fraud detection based on transaction behavior,'' in *Proc. IEEE Region 10 Conf. (TENCON)*, Nov. 2017, pp. 880–884.
11. Y. Timofeyev and T. Busalaeva, ''Current trends in insurance fraud in Russia: Evidence from a survey of industry experts,'' *Secur. J.*, vol. 34, no. 1, pp. 1–25, Mar. 2021.
12. N. Tyagi, A. Rana, S. Awasthi, and L. K. Tyagi, ''Data science: Concern for credit card scam with artificial intelligence,'' in *Cyber Security in Intelligent Computing and Communications*. Singapore: Springer, 2022,pp. 115–128.
13. M. J. Madhurya, H. L. Gururaj, B. C. Soundarya, K. P. Vidyashree, andB. Rajendra, ''Exploratory analysis of credit card fraud detection using machine learning techniques,'' *Global Transitions Proc.*, vol. 3, no. 1,pp. 31–37, Jun. 2022.
14. A. Ali, S. A. Razak, S. H. Othman, T. A. E. Eisa, A. Al- Dhaqm, M. Nasser,T. Elhassan, H. Elshafie, and A. Saif, ''Financial fraud detection based on machine learning: A systematic literature review,'' *Appl. Sci.*, vol. 12, no. 19, p. 9637, Sep. 2022.
15. G. K. Kulatilleke, ''Challenges and complexities in machine learning based credit card fraud detection,'' 2022, *arXiv:2208.10943*.
16. J. K. Afriyie, K. Tawiah, W. A. Pels, S. Addai-Henne, H.Dwamena,E. O. Owiredu, S. A. Ayeh, and J. Eshun, ''A supervised machine learning algorithm for detecting and predicting fraud in credit card transactions,'' *Decis. Anal. J.*, vol. 6, Mar. 2023, Art. no. 100163.
17. D. Prusti, J. K. Rout, and S. K. Rath, ''Detection of credit card fraud by applying genetic algorithm and particle swarm optimization,'' in *Proc. 3rd Int. Conf. MIND*. Singapore: Springer, Jan. 2023, pp. 357–369.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com