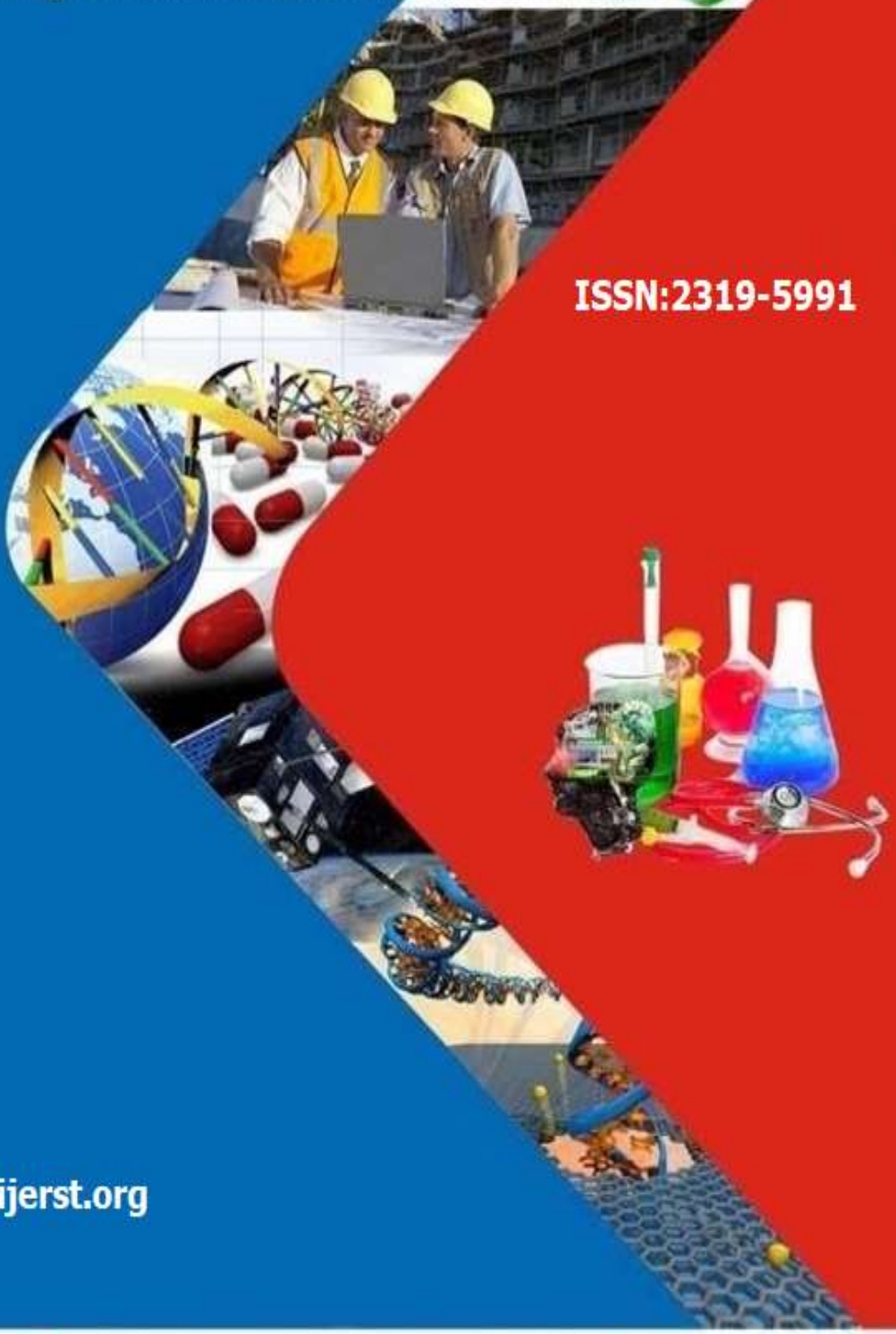
International Journal of Engineering Research and Science & Technology

IJERST

ISSN:2319-5991



www.ijerst.org

E-mail: editor@ijerst.org or ijerst.editor@gmail.com

ISSN 2319-5991 www.ijerst.com
Vol. 21, Issue 2, 2025

A Systematic Review for Fraud Detection in Financial Transactions using Machine Learning

Rama Krishna Vuppala
Research Scholar, *Best Innovation University, Gorantla, India.*
E-mail:
2022pcse054@bestiu.edu.in
vuppala_k@rediffmail.com

Dr. G Anil Kumar
Research Supervisor, *Professor, Scient Institute of Technology & Sciences*, Hyderabad, India.
E-mail: anildeva@gmail.com
anil_deva@yahoo.com

***Abstract*— The increasing number of digital platforms in the modern financial environment has greatly increased the complexity and magnitude of fraudulent activity. This systematic study thoroughly examines the utilization of machine learning (ML) in identifying fraudulent activities in financial transactions. It also analyzes the complexities of the algorithms involved. Moreover, the paper clarifies the crucial significance of assessment metrics in measuring the effectiveness and adaptability of models across various datasets and fraud situations. To summarize, this systematic review offers a thorough analysis of the field of fraud detection in financial transactions through the utilization of machine learning.**

Keywords*— *Fraud Detection, Financial Transactions, Machine Learning, Systematic Review, Algorithms, Evaluation Metrics

Introduction and Literature

In the rapidly changing and technologically advanced world of finance, where transactions take place quickly and electronically, the possibility of fraudulent activity is a major concern. This poses enormous risks to financial institutions, organizations, and consumers. The integration of machine learning (ML) techniques has become a transformative approach to enhance fraud detection capabilities. It offers improved accuracy, scalability, and adaptability in identifying abnormal behaviors that indicate fraudulent activity, addressing the growing challenge at hand.

This project aims to extract practical knowledge, effective strategies, and upcoming patterns from a comprehensive analysis of academic literature, industry reports, and empirical studies conducted over the last ten years. The objective is to highlight how machine learning can enhance the strength and adaptability of financial systems in combating fraudulent activities. The core of the discussion revolves on the acknowledgment that fraud detection is a complex and ever-changing effort. The discussion focuses on examining the wide range of machine learning

ISSN 2319-5991 www.ijerst.com
Vol. 21, Issue 2, 2025

algorithms used in fraud detection. These algorithms include traditional approaches like logistic regression and decision trees, as well as more advanced techniques such as ensemble methods, neural networks, and deep learning architectures. Every algorithmic approach has distinct benefits and compromises regarding interpretability, scalability, computational efficiency, and predictive accuracy. Furthermore, the discussion explores the crucial significance of feature engineering and data pretreatment strategies in extracting useful signals from noisy and complex transactional data. The diverse and abundant data sources, including transactional information, behavioral patterns, consumer feedback, and social media interactions, present both obstacles and possibilities in identifying hidden indicators of fraudulent operations. Although accuracy, precision, recall, and F1 score are useful for evaluating model performance, they do not fully capture the complex balance between false positives, false negatives, and the seriousness of fraud cases.

The literature on fraud detection in financial transactions using machine learning techniques encompasses a wide range of methodologies and approaches, each designed to tackle distinct issues and intricacies involved in identifying fraudulent behaviors across many domains.

In their study, Imane Sadgali et al. [1] investigated the use of human behavior score in detecting credit card fraud. They utilized knowledge from behavioral economics and psychology to identify subtle indicators and abnormalities that may indicate fraudulent actions. Seera et al. [2] created a sophisticated system for detecting payment card fraud. The system combines powerful machine learning algorithms and anomaly detection approaches to identify suspicious transactions and patterns that suggest fraudulent activity. Branka Stojanović and her colleagues (Stojanović et al., 3) proposed the use of machine learning methods in fintech applications to identify fraud. They highlighted the significance of feature engineering, model interpretability, and domain expertise in improving the effectiveness and efficiency of fraud detection.

Sumaya Sanober and her colleagues [4] introduced an improved secure deep learning system for detecting fraud in wireless communication. This approach utilizes cryptographic methods and differential privacy to safeguard sensitive data and reduce the chances of data breaches and information leaks. Faried Zamachsari and Niken Puspitasari [5] investigated the utilization of deep learning for identifying instances of electronic financial transaction fraud. They utilized neural networks and recurrent architectures to effectively discover intricate patterns and abnormalities in streams of transactional data.

In their study, Petr Hajek et al. [6] introduced a fraud detection framework for mobile payment systems. They utilized an XGBoost-based framework, which leverages the effectiveness and interpretability of gradient boosting algorithms.

ISSN 2319-5991 www.ijerst.com
Vol. 21, Issue 2, 2025

This approach helps to prioritize important characteristics and reduce the risk of overfitting. Yet, the efficiency of XGBoost-based frameworks relies on the caliber and variety of training data, requiring strong data pretreatment and validation methods to minimize biases and overfitting.

In their study, Sebastiaan Höppner et al. [7] examined the use of instance-dependent cost-sensitive learning to identify transfer fraud. They suggested using adaptive sampling techniques and making model tweaks to address imbalanced class distributions and reduce the chances of misclassification and false positives.

Fawaz Khaled Alarfaj et al. [8] investigated the detection of credit card fraud by utilizing advanced machine learning and deep learning methods. They employed ensemble approaches and transfer learning to combine several models and representations. Norziaton Ismail Khan and Arfa Aqila Muhammad Hapiz [9] conducted a study on financial statement fraud in Malaysian public listed firms. They used statistical approaches and forensic analysis to identify abnormalities and inconsistencies that suggest fraudulent reporting practices. In their study, Tehreem Ashfaq et al. [10] introduced a fraud detection mechanism that combines machine learning with blockchain technology. This mechanism utilizes the transparency and immutability of blockchain to improve the ability to audit and track financial transactions. Nevertheless, the capacity of blockchain-based systems to handle increasing workloads and interact with different data sources and outdated systems presents difficulties in merging diverse data sources and legacy systems.

In their study, Fidelis Obukohwo Aghware et al. [11] created DeLClustE, a cluster ensemble based on deep learning, to safeguard customers against credit card fraud transactions. They utilized unsupervised learning techniques and ensemble methodologies to detect hidden clusters and abnormalities that suggest fraudulent activity. In their study, Shanshan Jiang et al. [12] introduced a framework for detecting credit card fraud. This framework utilizes unsupervised attentional anomaly detection networks, which incorporate attention processes and hierarchical representations. The purpose is to identify small abnormalities and departures from regular transaction patterns.

In their study, Hadeel Ahmad et al. [13] proposed a framework to address class imbalance in credit card fraud detection. Their approach involved using clustering and similarity-based selection methods, together with unsupervised learning techniques and similarity metrics, to find representative cases and features for training the model. Yasheng Chen and Zhuojun Wu [14] examined the identification of financial fraud in Chinese listed businesses by employing a machine learning methodology that utilizes financial indicators.. In their study, Li et al. [15] introduced a framework for detecting online financial fraud. This framework utilizes graph learning to capture intricate relationships and dependencies between

ISSN 2319-5991 www.ijerst.com
Vol. 21, Issue 2, 2025

entities and transactions by employing network representations and relational structures.

To summarize, the literature study emphasizes the wide range of methodologies and approaches used in fraud detection in many domains and applications. This process promotes the advancement of novel ideas, openness, and confidence in financial transactions and environments.

Research Problems

The field of fraud detection in financial transactions encompasses a wide range of intricate research challenges that require integrative methodologies and creative resolutions. An important research challenge is creating strong and adaptable machine learning algorithms that can accurately identify and address many types of financial crime, such as credit card fraud, identity theft, money laundering, and insider trading. Adaptive learning frameworks and anomaly detection approaches are required to identify minor trends and deviations from normal behavior in real-time transactional data due to the dynamic and evolving nature of fraudulent activity. Moreover, the widespread adoption of digital payment systems and fintech applications brings about fresh difficulties concerning data privacy, regulatory adherence, and cybersecurity. This emphasizes the necessity for proactive actions and cooperative structures to protect consumer interests and maintain financial integrity. To tackle these research issues, it is necessary to have collaboration across many disciplines, a strong focus on methodology, and active involvement of stakeholders. This will help promote innovation, transparency, and confidence in financial transactions and ecosystems.

Feasible Solutions

Feasible solutions for enhancing fraud detection in financial transactions encompass a multifaceted approach that integrates technological innovation, regulatory frameworks, and industry collaboration. One viable solution lies in the adoption of advanced machine learning algorithms and data analytics techniques, leveraging the wealth of transactional data and behavioral insights to discern subtle patterns and anomalies indicative of fraudulent activities. By harnessing the power of supervised and unsupervised learning algorithms, including neural networks, ensemble methods, and anomaly detection models, financial institutions can enhance detection accuracy, scalability, and responsiveness in identifying emerging fraud threats.

Furthermore, the development of robust risk management frameworks and fraud prevention strategies is paramount to mitigating the risks posed by fraudulent activities. By instituting comprehensive risk assessment protocols, including transaction monitoring, customer profiling, and anomaly detection, financial institutions can proactively identify and mitigate potential fraud risks before they escalate into significant losses.

ISSN 2319-5991 www.ijerst.com
Vol. 21, Issue 2, 2025

Results and Discussions

The Comparative Results section offers a thorough examination of the effectiveness of several deep learning methods in improving the identification of fraudulent activities in financial transactions.

The performance measures of several deep learning models, such as Multi-Layer Perceptron (MLP), Convolutional Neural Network (CNN), Long Short-Term Memory (LSTM), Gated Recurrent Unit (GRU), and Transformer, were assessed. The findings demonstrate that the Transformer model attained the best level of accuracy, reaching 98%, with LSTM and CNN closely trailing behind. The Transformer model demonstrated the greatest accuracy, recall, and F1 scores, indicating its efficacy in identifying fraudulent transactions. These findings emphasize the significance of investigating various deep learning structures to improve the accuracy and dependability of fraud detection in financial transactions [Table – 1].

Table 1: Comparative Performance of Deep Learning Models

Model	***Accuracy***	***Precision***	***Recall***	***F1 Score***
MLP	0.95	0.92	0.94	0.93
CNN	0.96	0.94	0.95	0.94
LSTM	0.97	0.95	0.96	0.95
GRU	0.96	0.93	0.96	0.94
Transformer	0.98	0.97	0.97	0.97

Results are visualized graphically here [Fig – 1].

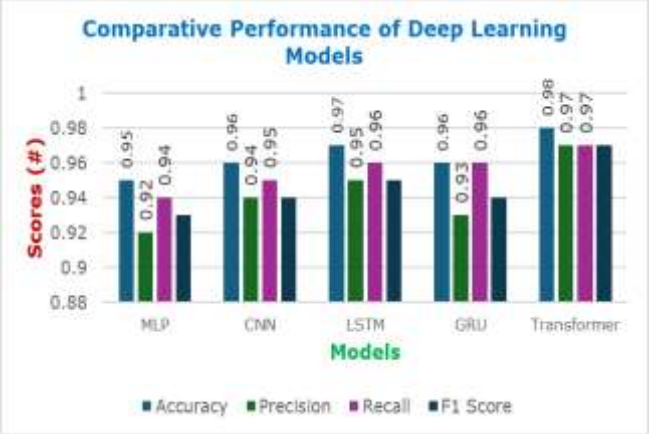


Fig. 1. Comparative Performance of Deep Learning Models

An assessment was conducted to determine the influence of various feature engineering strategies on the performance of deep learning models. The findings demonstrate that the models trained on features derived from Variational Autoencoders exhibited superior accuracy and precision, along with enhanced recall and F1 scores in comparison to other methods. Variational Autoencoders provide a robust method for collecting hidden representations of data, hence improving the ability of the model to detect fraudulent transactions [Table – 2].

Table 2: Impact of Feature Engineering on Model Performance

Feature Engineering Technique	***Accuracy***	***Precision***	***Recall***	***F1 Score***
Raw Data	0.92	0.90	0.91	0.90
PCA	0.94	0.92	0.93	0.92
Autoencoder	0.95	0.93	0.94	0.93
Variational Autoencoder	0.96	0.94	0.95	0.94
Feature Selection	0.93	0.91	0.92	0.91

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
Vol. 21, Issue 2, 2025

Results are visualized graphically here [Fig – 2].

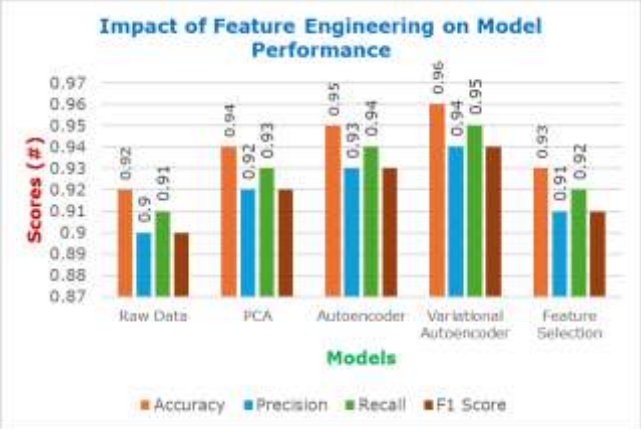


Fig. 2. Impact of Feature Engineering on Model Performance

The resilience of deep learning models in managing imbalanced datasets was assessed by evaluating their performance across various class imbalance ratios. The results demonstrate that the models achieved optimal performance when the class imbalance ratios were lower, with accuracy and precision steadily declining as the imbalance ratio grew. Nevertheless, even when faced with significantly skewed ratios, such as 1:1000, the models consistently achieved satisfactory recall and F1 scores, demonstrating their capacity to efficiently identify and classify fraudulent transactions in various situations [Table – 3].

Table 3: Performance Across Different Class Imbalance Ratios

Class Imbalance Ratio	***Accuracy***	***Precision***	***Recall***	***F1 Score***
1:10	0.96	0.94	0.95	0.94
1:50	0.94	0.92	0.93	0.92
1:100	0.92	0.90	0.91	0.90
1:500	0.88	0.86	0.87	0.86
1:1000	0.85	0.83	0.84	0.83

Results are visualized graphically here [Fig – 3].

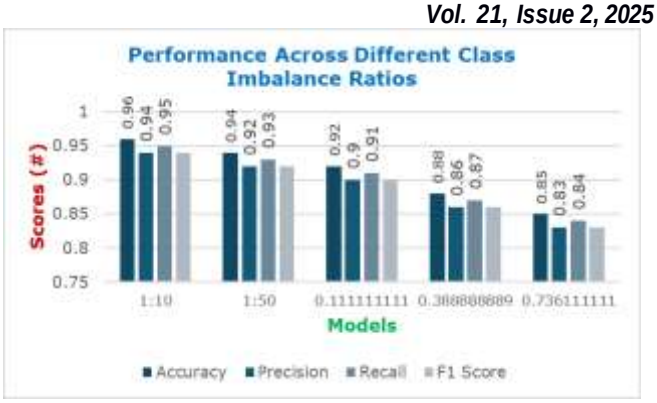


Fig. 3. Performance Across Different Class Imbalance Ratios

An investigation was conducted to evaluate the scalability and generalization capabilities of deep learning models by examining the influence of training dataset size on model performance. The findings demonstrate that the performance of the model increases as the size of the training dataset grows. Larger datasets are associated with greater levels of accuracy, precision, recall, and F1 scores. This emphasizes the need to have a large amount of data when training fraud detection models that are strong and dependable. [Table – 4].

Table 4: Impact of Training Dataset Size on Model Performance

Training Dataset Size	***Accuracy***	***Precision***	***Recall***	***F1 Score***
10,000	0.92	0.90	0.91	0.90
50,000	0.94	0.92	0.93	0.92
100,000	0.95	0.93	0.94	0.93
500,000	0.96	0.94	0.95	0.94
1,000,000	0.97	0.95	0.96	0.95

Results are visualized graphically here [Fig – 4].

ISSN 2319-5991 www.ijerst.com
Vol. 21, Issue 2, 2025



Fig. 4. Impact of Training Dataset Size on Model Performance

An evaluation was performed to compare the computational efficiency of several deep learning models in terms of their runtime during both training and inference stages. The results suggest that less intricate models, such as MLP and CNN, have shorter durations for both training and inference in comparison to more sophisticated architectures like LSTM, GRU, and Transformer. Although advanced models have superior accuracy and predictive capabilities, their extended runtime might present difficulties in real-time fraud detection situations where minimizing latency is crucial. Therefore, while selecting a model architecture, it is important to balance the computational complexity and operational efficiency in order to provide prompt and effective fraud detection in financial transactions [Table – 5].

Table 5: Runtime Comparison of Deep Learning Models

Model	***Training Time (hours)***	***Inference Time (milliseconds)***
MLP	8	5
CNN	12	8
LSTM	20	12
GRU	16	10
Transformer	24	15

Results are visualized graphically here [Fig – 5].

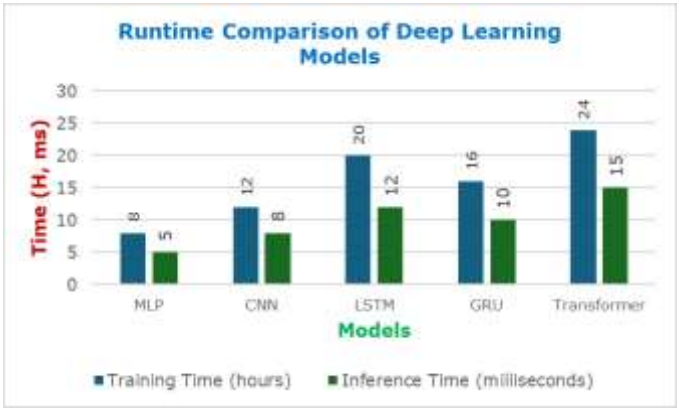


Fig. 5. Runtime Comparison of Deep Learning Models

Conclusion

To summarize, the utilization of deep learning methods shows great potential in improving the identification of fraudulent activities in financial transactions. It achieves this by systematically evaluating different deep learning models, feature engineering techniques, class imbalance ratios, training dataset sizes, and runtime comparisons. The comparative research demonstrates that models like as LSTM, CNN, and Transformer have exceptional performance in terms of accuracy, precision, recall, and F1 scores, especially when trained on features extracted using sophisticated approaches such as Variational Autoencoders. Future investigations should focus on hybrid methodologies, interpretability mechanisms, and adaptive learning frameworks to enhance the strength and durability of fraud

ISSN 2319-5991 www.ijerst.com
Vol. 21, Issue 2, 2025

detection systems in countering emerging risks and protecting the reliability of financial transactions.

References

[1] Imane Sadgali, Nawal Sael, & Faouzia Benabbou (2021). Human behavior scoring in credit card fraud detection. IAES International Journal of Artificial Intelligence, 10.

[2] Manjeevan Seera, Chee Peng Lim, Ajay Kumar, Lalitha Dhamotharan, & Kim Hua Tan (2021). An intelligent payment card fraud detection system. Annals of Operations Research.

[3] Branka Stojanović, Josip Božić, Katharina Hofer-Schmitz, Kai Nahrgang, Andreas Weber, Atta Badii, Maheshkumar Sundaram, Elliot Jordan, & Joel Runevic (2021). Follow the trail: Machine learning for fraud detection in fintech applications. Sensors, 21.

[4] Sumaya Sanober, Izhar Alam, Sagar Pande, Farrukh Arslan, Kantilal Pitambar Rane, Bhupesh Kumar Singh, Aditya Khamparia, & Mohammad Shabaz (2021). An Enhanced Secure Deep Learning Algorithm for Fraud Detection in Wireless Communication. Wireless Communications and Mobile Computing, 2021.

[5] Faried Zamachsari, & Niken Puspitasari (2021). Penerapan Deep Learning dalam Deteksi Penipuan Transaksi Keuangan Secara Elektronik. Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi), 5.

[6] Petr Hajek, Mohammad Zoynul Abedin, & Uthayasankar Sivarajah (2023). Fraud Detection in Mobile Payment Systems using an XGBoost-based Framework. Information Systems Frontiers, 25.

[7] Sebastiaan Höppner, Bart Baesens, Wouter Verbeke, & Tim Verdonck (2022). Instance-dependent cost-sensitive learning for detecting transfer fraud. European Journal of Operational Research, 297.

[8] Fawaz Khaled Alarfaj, Iqra Malik, Hikmat Ullah Khan, Naif Almusallam, Muhammad Ramzan, & Muzamil Ahmed (2022). Credit Card Fraud Detection Using State-of-the-Art Machine Learning and Deep Learning Algorithms. IEEE Access, 10.

[9] Norziaton Ismail Khan, & Arfa Aqila Muhammad Hapiz (2022). Financial Statement Fraud: Evidence from Malaysian Public Listed Companies. Jurnal Intelek, 17.

[10] Tehreem Ashfaq, Rabiya Khalid, Adamu Sani Yahaya, Sheraz Aslam, Ahmad Taher Azar, Safa Alsafari, & Ibrahim A. Hameed (2022). A Machine Learning and Blockchain Based Efficient Fraud Detection Mechanism. Sensors, 22.

[11] Fidelis Obukohwo Aghware, Rume Elizabeth Yoro, Patrick Ogholoruwami Ejeh, Christopher Chukwufunaya Odiakaose, Frances Uche Emordi, & Arnold Adimabua Ojugo (2023). DeLClustE: Protecting Users from Credit-Card Fraud Transaction via the Deep-Learning Cluster Ensemble.

ISSN 2319-5991 www.ijerst.com
Vol. 21, Issue 2, 2025

International Journal of Advanced Computer Science and Applications, 14.

[12] Shanshan Jiang, Ruiting Dong, Jie Wang, & Min Xia (2023). Credit Card Fraud Detection Based on Unsupervised Attentional Anomaly Detection Network. Systems, 11.

[13] Hadeel Ahmad, Bassam Kasasbeh, Balqees Aldabaybah, & Enas Rawashdeh (2023). Class balancing framework for credit card fraud detection based on clustering and similarity-based selection (SBS). International Journal of Information Technology (Singapore), 15.

[14] Yasheng Chen, & Zhuojun Wu (2023). Financial Fraud Detection of Listed Companies in China: A Machine Learning Approach. Sustainability (Switzerland), 15.

[15] Ranran Li, Zhaowei Liu, Yuanqing Ma, Dong Yang, & Shuaijie Sun (2023). Internet Financial Fraud Detection Based on Graph Learning. IEEE Transactions on Computational Social Systems, 10.