International Journal of Computer Science and Engineering (IJCSE)
ISSN (P): 2278–9960; ISSN (E): 2278–9979
Vol. 13, Issue 2, Jul–Dec 2024; 399–436

International Academy of Science, Engineering and Technology
Connecting Researchers; Nurturing Innovations

EVALUATING ANOMALY DETECTION MODELS FOR FINANCIAL FRAUD RISK ASSESSMENT

Pradeep Jeyachandran[1], Abhishek Das[2], Arnab Kar[3], Om Goel[4], Prof. (Dr) Punit Goel[5] & Prof.(Dr.) Arpit Jain[6]

[1]University of Connecticut, 352 Mansfield Rd, Storrs, CT 06269, United States

[2]Texas A&M University, 400 Bizzell St, College Station, TX 77840, United States

[3]Duke University, Durham, NC 27708, United States

[4]ABES Engineering College Ghaziabad, India

[5]Maharaja Agrasen Himalayan Garhwal University, Uttarakhand, India

[6] KL University, Vijayawada, Andhra Pradesh, India

ABSTRACT

The increasing frequency and sophistication of financial fraud have necessitated the development of effective anomaly detection models to mitigate risks and enhance security in financial systems. This research aims to evaluate various anomaly detection techniques for their efficacy in identifying fraudulent transactions and assessing financial fraud risks. The study focuses on comparing traditional statistical methods, machine learning algorithms, and hybrid approaches to determine which models best detect outliers indicative of fraudulent activities. Key models explored include decision trees, support vector machines (SVM), neural networks, k-means clustering, and autoencoders. These models are tested using real-world financial transaction datasets, ensuring the models' applicability to diverse fraud patterns across different financial institutions. Evaluation metrics such as precision, recall, F1-score, and Area Under the Curve (AUC) are employed to assess the models' performance. The research highlights the trade-offs between model complexity, accuracy, and interpretability, offering insights into selecting the most suitable anomaly detection method based on the specific needs of a financial institution. The results indicate that while machine learning approaches like SVM and neural networks generally offer higher detection accuracy, they require more computational resources and may be harder to interpret compared to simpler models like decision trees. Overall, the study contributes to the understanding of anomaly detection in the context of financial fraud, providing a comprehensive evaluation of different models and their potential for reducing financial risks. This research aims to assist financial professionals in making informed decisions regarding fraud detection strategies.

KEYWORDS: *Anomaly Detection, Financial Fraud, Risk Assessment, Machine Learning, Decision Trees, Support Vector Machines, Neural Networks, Fraud Detection Models, Outlier Detection, Data Mining, Precision, Recall, F1-Score, AUC, Financial Security*

Article History

Received: *11 Nov 2024* | ***Revised:*** *23 Nov 2024* | ***Accepted:*** *30 Nov 2024*
