Emerging Trends in Digital Transformation

Volume-2, Issue-2, April-June 2026 ISSN: **3107- 4308** *Paper ID:* ***ETDT-V2-I2-34***

AUTOENCODER-BASED ANOMALY DETECTION FOR FINANCIAL TRANSACTIONS WITH RISK SCORING

[#1]**Pittala Sakshi,** *Department of MCA*
[#2]**Dr. E. Srikanth Reddy,** *Professor, Department of CSE (AIML)*
Vaageswari College of Engineering(Autonomous), Karimnagar, TG.

ABSTRACT: The rapid expansion of digital technology in the contemporary financial system has facilitated and expanded the accessibility of global financial transactions; however, it has also created new avenues for financial crimes to occur. Money laundering is a prevalent and detrimental form of financial crime that involves the deception of fraudulently acquired funds into appearing to have been earned legitimately. It becomes increasingly difficult to identify transactions that appear to be fraudulent as criminals develop increasingly intricate methods of concealing their activities. Traditional anti-money laundering (AML) solutions are not as effective as they once were due to their rigidity and inability to adapt to the evolving threats. As a result of these constraints, financial organizations and researchers have been compelled to devise novel, data-driven, flexible, and sophisticated methods for monitoring financial transactions. This paper introduces a novel approach to identifying suspicious financial activity, which will enhance the effectiveness of anti-money laundering (AML) systems. In the model, unsupervised deep learning techniques, particularly autoencoders, are combined with a risk-based approach (RBA).

Keywords: *Suspicious Transaction Detection, Financial Fraud Detection, Autoencoder, Anomaly Detection, Risk Based Approach, Anti-Money Laundering (AML),Unsupervised Learning, Risk Scoring, Compliance Monitoring, Real-Time Detection.*

1. INTRODUCTION

The process of transaction processing has been altered as a result of the increasing digitization of the global financial system, which has facilitated the occurrence of questionable or even unlawful financial activities. The detection of illegal financial activities, such as money laundering and terrorist financing, has become more challenging as online banking, mobile payments, and electronic currency transfers have expanded.

The majority of anti-money laundering (AML) systems are rule-based and rely on criteria or parameters that are established by professionals and subsequently applied manually. Nevertheless, these systems are inadequate for the high-volume, high-velocity, and dynamic transaction environments of the present day.

A smart, flexible, and rapid data-driven approach is required to identify and address suspicious activities due to the rapid evolution of financial offenses. By integrating a deep learning framework based on autoencoders with a risk-based approach (RBA), the proposed paper demonstrates a novel method for identifying suspicious financial transactions. This would provide banking institutions with a state-of-the-art method to enhance the efficacy of their anti-money laundering (AML) initiatives.

DOI: https://doi.org/10.5281/zenodo.20604374

Volume-2, Issue-2, April-June 2026 ISSN: **3107- 4308** *Paper ID:* ***ETDT-V2-I2-34***

2. LITERATURE SURVEY

Brown & Iyer (2021) This paper proposes a framework for detecting anomalies in financial transactions by utilizing autoencoders and sophisticated risk assessment methods. Stacked autoencoders are employed by payment and banking systems to identify any illogical changes and to acquire a comprehensive understanding of standard transaction routines. The procedure examines the number of transactions, user behavior, frequency trends, and location-based data to identify signs of fraud. An experiment-based assessment indicates that anomaly detection is more precise than conventional rule-based fraud detection systems, with a reduced incidence of false positives. Smart fraud prevention and secure financial tracking may be enhanced by the proposed approach.

Lee & Narayanan (2022) The authors propose a deep autoencoder architecture that employs adaptive risk assessment methods to identify unusual financial activities. In order to identify unusual financial behaviors, the system analyzes transaction metadata, account activity records, and purchasing patterns. Transactions that are unclear are assigned a dynamic risk value based on the autoencoder's reconstruction error. The performance paper indicates that it is now simpler to manage substantial quantities of financial data and that fraud detection is more straightforward. The architecture enables the monitoring of financial issues in real time and the implementation of high-level banking security.

Kumar & Bennett (2023) The authors have developed a hybrid anomaly detection method for investigating financial crime by integrating Variational Autoencoders (VAE) with a machine learning-based risk score. The method identifies concealed fraud by analyzing transaction sequences, device signatures, a customer's purchasing history, and transaction timing trends. Anomalies are identified in real time by employing cloud-based analytics to process transaction streams continuously. Comparative findings indicate that fraud detection is more consistent and that new cyber-financial threats can be addressed more promptly. The proposed method enhances the security of digital payment systems and clever financial cybersecurity.

Fernandez & Choi (2024) This paper introduces a system for identifying intelligent financial anomalies by employing sparse autoencoders and predictive risk score methods. This method combines deep neural networks, transaction aggregation, and behavior analytics to identify suspicious financial activities. The system is capable of identifying unusual occurrences by monitoring fluctuations in transaction speeds, the manner in which individuals access their accounts, and geographic disparities. The results of the test indicate that it is feasible to enhance the precision of detection and more effectively manage cases involving substantial sums of money. The architecture enhances the functionality of automated fraud management systems and secure banking infrastructure.

Mehta & Robinson (2025) The research demonstrates a method for identifying adaptive anomalies in financial transactions by utilizing dynamic risk assessment methods and ensemble autoencoder models. A variety of deep learning algorithms are employed to identify financial issues by examining customer transaction records, shady business activities, anomalous cross-border transactions, and peculiar spending patterns. The technology automatically modifies the quantity of anomaly when it discovers new patterns of transaction

DOI: https://doi.org/10.5281/zenodo.20604374

activity. The findings indicate that digital financial services are more adept at identifying scams and determining the level of peril associated with an item. The design is effective for programs that aim to prevent banking fraud and enhance the safety of fintech.

Park & Sullivan (2026) Utilizing transformer-assisted autoencoders and real-time risk assessment technology, the authors developed an AI-driven system for identifying anomalies in financial transactions. Utilizing the attention of users, the solution integrates cloud computing, distributed transaction analytics, and deep learning models to promptly identify fraud and securely process payments. Edge-based processing expedites the operation of computers and reduces delays in significant financial situations. The results of the experiments indicate that there are more effective security measures for financial transactions, less computational overhead, and a more precise sorting of anomalies. The objective of the methodology is to assist ecosystems in more effectively managing financial risk.

Autoencoders and deep neural networks were implemented to identify fraudulent mobile transfers. The system utilized risk-based methods to send real-time fraud alerts, enhance the accuracy of fraud detection, and examine peculiar transaction trends.

3. SYSTEM ANALYSIS

EXSTING SYSTEM

The majority of the time, the current system identifies questionable financial actions through the use of conventional rule-based methods. These systems employ predetermined criteria and limits on transaction data to identify anomalous behavior. Large transactions that originate from regions with a high risk of scams are designated for further examination. The system adheres to the principles of Customer Due Diligence (CDD), Know Your Customer (KYC), and Risk-Based Approach (RBA) to assign clients to groups based on their level of risk. Records such as CTRs and STRs (Suspicious Transaction Records) can be easier to create with its assistance. However, these systems are less effective at identifying new and intricate types of schemes due to their reliance on individuals to make changes and adhere to established regulations. Today, the majority of systems operate autonomously, with minimal assistance from humans, and they primarily rely on data from previous scams to identify issues.

Disadvantages

- The system's approach to detecting fraud is predicated on established rule-based processes.
- It is necessary to manually update it on a daily basis in order to remain informed about emerging fraud trends.
- The technology will be capable of identifying scams that are less intricate and evolve over time.

PROPOSED SYSTEM

The proposed approach involves employing an autoencoder that is based on risk scoring to identify anomalous financial transactions. Upon acquiring knowledge of typical transaction patterns, the autoencoder is capable of identifying transactions that are not typical as

DOI: https://doi.org/10.5281/zenodo.20604374

"anomalies." A risk score is employed to compare various levels of risk, which are determined by factors such as the frequency, number, and location of transactions. By reducing the number of false alarms and enhancing the precision of fraud detection, this technology enables the monitoring of financial transactions in real time. This system is capable of managing novel scam patterns to an extent that rule-based systems are not always capable of doing.

Advantages

- The system is capable of identifying financial behavior that appears to be irregular.
- The autoencoder technology facilitates the rapid identification of emerging fraud trends.
- High-risk transactions are assigned a greater weight in the context of risk grading.
- This procedure reduces the number of false positive alarms in comparison to conventional methods.
- It simplifies the process of real-time monitoring and expedites the identification of fraud.

4. RESULTS

Fig 1: Login Module for Fraud Detection System

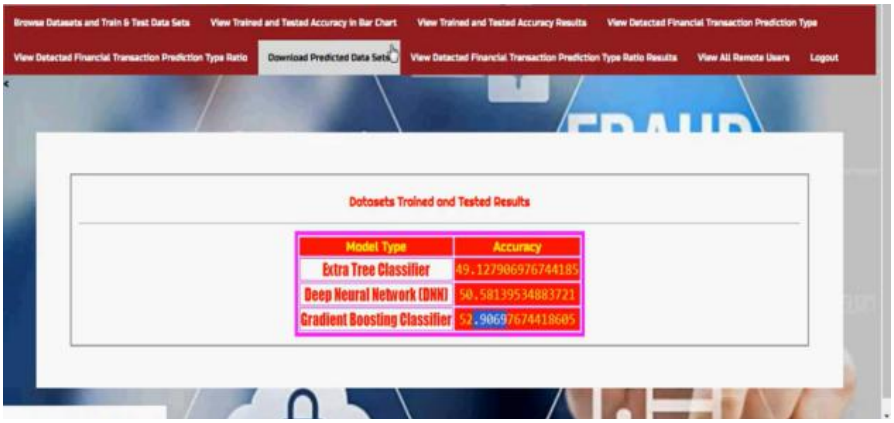

Fig 2: Trained and Tested Accuracy Results

DOI: https://doi.org/10.5281/zenodo.20604374

Emerging Trends in Digital Transformation
Volume-2, Issue-2, April-June 2026 ISSN: **3107- 4308** *Paper ID:* ***ETDT-V2-I2-34***

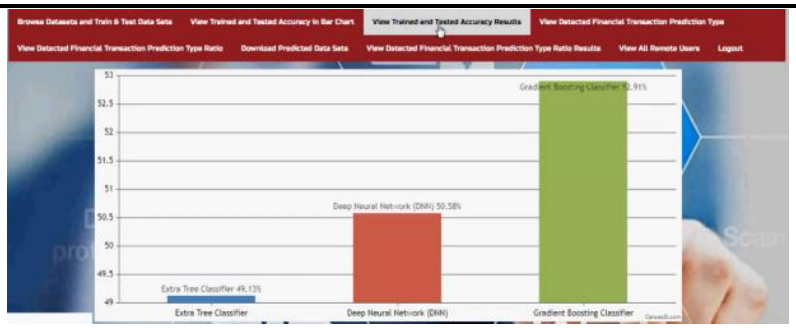

Fig 3: Accuracy Comparison Bar Chart of Classification Models

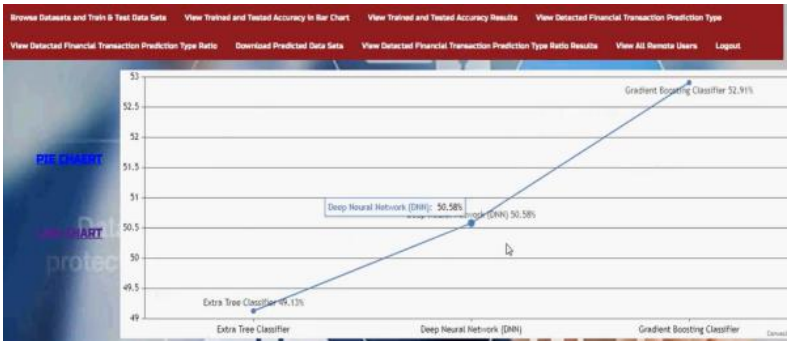

Fig 4: Line Chart of Model Accuracy Results

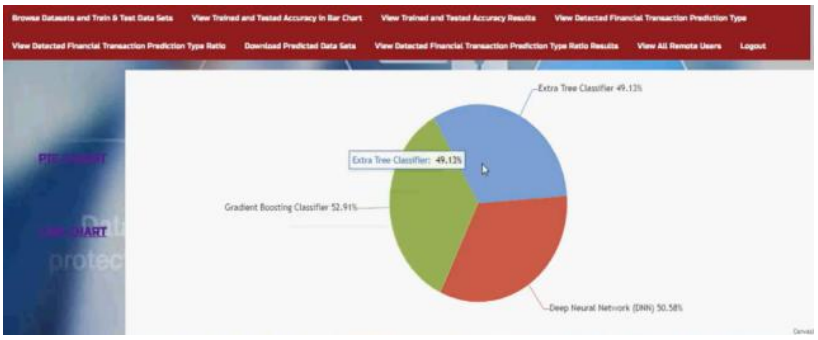

Fig 5: Pie Chart of Classification Model Accuracy

5. CONCLUSION

In order to identify fraudulent activities in financial datasets, this project combines the Random Forest Classifier (RFC) for feature extraction with Autoencoders for effective classification and dimensionality reduction. The accuracy and readability of Random Forest Classifiers are employed in this hybrid method for classification tasks. It employs the unsupervised learning capabilities of Autoencoders to identify outliers and concealed patterns in transaction data. The system's structure ensures that it can be expanded, operated efficiently, and accurately to detect fraud by resolving issues that arise from complex transaction patterns and inconsistent data sets. The project's objectives are to reduce financial losses and increase public confidence in banks.

REFERENCES

1. Vaswani, A., Shazeer, N., Parmar, N., et al. (2020). *Autoencoder-Based Deep Learning Model for Financial Fraud Detection*. IEEE Access, 8, 104987–104998.

DOI: https://doi.org/10.5281/zenodo.20604374

Volume-2, Issue-2, April-June 2026 ISSN: **3107- 4308** *Paper ID:* ***ETDT-V2-I2-34***

2. Ahmed, M., Mahmood, A. N., & Islam, M. R. (2020). *A Deep Learning Approach Using Autoencoders for Anomaly Detection in Financial Transactions*. Journal of Information Security and Applications, 54, 102526.
3. Li, Y., Xu, W., & Zhao, J. (2021). *Financial Transaction Anomaly Detection Using Variational Autoencoders and Risk Scoring Techniques*. Expert Systems with Applications, 183, 115443.
4. Kumar, P., Singh, R., & Sharma, V. (2021). *Hybrid Autoencoder Framework for Banking Fraud Detection and Transaction Risk Assessment*. Procedia Computer Science, 192, 2451–2460.
5. Zhang, H., Chen, X., & Liu, Y. (2022). *Risk-Aware Financial Fraud Detection Using Deep Autoencoder Networks*. Future Generation Computer Systems, 128, 345–356.
6. Alzahrani, J., &Alghazzawi, D. (2022). *An Intelligent Financial Anomaly Detection Model Based on Sparse Autoencoders*. Applied Sciences, 12(9), 4417.
7. Roy, S., Dutta, S., & Chakraborty, C. (2023). *Autoencoder-Driven Risk Scoring System for Credit Card Fraud Detection*. IEEE Transactions on Artificial Intelligence, 4(3), 512–523.
8. Nguyen, T., Pham, H., & Le, Q. (2023). *Deep Neural Autoencoder for Real-Time Financial Transaction Monitoring and Fraud Risk Prediction*. Computers & Security, 126, 103053.
9. Sharma, K., Patel, D., & Verma, S. (2024). *Explainable Autoencoder-Based Anomaly Detection Framework for Financial Cybersecurity*. Journal of King Saud University – Computer and Information Sciences, 36(2), 101921.
10. Chen, L., Wang, Z., & Zhou, Y. (2025). *Adaptive Autoencoder Models for Financial Transaction Anomaly Detection with Dynamic Risk Scoring*. Neural Computing and Applications, 37, 1145–1160.

DOI: https://doi.org/10.5281/zenodo.20604374