2024 IEEE International Conference on Artificial Intelligence and Quantum Computation-Based Sensor Applications
Nagpur, India, December 20-21, 2024

# Boosting Anomaly Detection in Financial Transactions: Leveraging Deep Learning with Isolation Forest for Enhanced Accuracy

[1]Prateek Kumar Bansal
*Institute of Business Management*
*GLA University,*
Mathura, India
prateek.bansal@gla.ac.in

[2]Divya Nimma
*PhD in Computational Science*
*University of Southern Mississippi*
*Data Analyst in UMMC,*
USA
nm.divya89@gmail.com

[3]Nripendra Narayan Das
*Department of Information Technology,*
*Manipal University Jaipur,*
India
nripendranarayan.das@jaipur.manipal.edu

[4]BVN Prasad Paruchuri
*Department of CSE*
*KL University(Deemed to be),*
Vaddeswaram, Vijayawada, India
bvnprasadparuchuri@yahoo.com

[5]Harishchander Anandaram
*Amrita School of Artificial Intelligence,*
*Amrita Vishwa Vidyapeetham*
Coimbatore, India
harishchander.a@gmail.com

[6]M.Karthik
*Department of AI & DS*
*K.Ramakrishnan College of Engineering,*
Trichy, India
karthikkrce012@gmail.com

***Abstract*—Anomaly detection in financial transactions is paramount for safeguarding against fraudulent activities that pose significant risks to financial institutions and customers alike. Traditional methods often struggle to accurately identify complex and evolving patterns of fraud, necessitating innovative approaches that leverage advanced techniques such as deep learning and isolation forest. In this study, we propose a novel framework for boosting anomaly detection in financial transactions by integrating deep learning with isolation forest to achieve enhanced accuracy. Firstly, it employ an autoencoder, a type of neural network, to learn complex representations of normal transaction patterns and reconstruct input data. The autoencoder's ability to capture subtle variations in transaction attributes enables it to effectively distinguish between normal and anomalous instances based on the reconstruction error. Furthermore, we augment the anomaly detection process by incorporating isolation forest, a tree-based algorithm that isolates anomalies in the feature space by recursively partitioning data subsets. By combining the representation learning capabilities of deep learning with the outlier detection prowess of isolation forest, our framework offers a comprehensive solution for detecting fraudulent activities in financial transactions. Through experimentation on real-world financial datasets, we demonstrate the superior performance of our proposed framework compared to existing methods. The proposed method is implemented in Python software and has an accuracy of about 99.12% which is 1.49% higher than other existing methods like Conv-LSTM, Convolutional Neural Network (CNN)-LSTM, and CNN-GRU (Gated Recurrent Unit). Moreover, the integration of deep learning with isolation forest enables our framework to adapt to evolving patterns of fraud, ensuring robust and reliable anomaly detection in dynamic financial environments. Overall, our study contributes to the advancement of anomaly detection techniques in financial transactions, offering a promising solution for mitigating fraud risks and enhancing the security of financial systems.**

***Keywords*—Anomaly Detection, Autoencoder, Isolation Forest, Deep Learning, Financial Transaction**

## I. INTRODUCTION (*HEADING 1*)

Anomaly detection in financial transactions is paramount for safeguarding against fraudulent activities that can have detrimental effects on both financial institutions and their customers [1] [2]. Traditional methods of anomaly detection often rely on rule-based systems or statistical approaches, which may struggle to adapt to the dynamic and evolving nature of fraudulent behaviors in financial transactions. For innovative techniques that can effectively detect anomalies with high accuracy and reliability. In this study, we propose leveraging the power of deep learning with isolation forest to enhance anomaly detection accuracy in financial transactions [3] [4]. DL has become a potent method for extracting intricate patterns and interpretations from data, which makes it a good fit for jobs involving anomaly identification. DNN may be trained on vast amounts of information about transactions to create models that are capable of capturing complex correlations and patterns that are not always visible using more conventional techniques. Moreover, DL models can automatically extract features from unprocessed data, doing away with the necessity for human feature engineering and opening the door to more adaptable and versatile systems for detecting anomaly [5] [6].

In addition to DL, it integrate isolation forest into our anomaly detection framework to further enhance accuracy and reliability. Isolation forest is a tree-based algorithm that excels at identifying anomalies in high-dimensional data by isolating them into partitions in a binary tree structure. Unlike traditional methods that rely on density estimation or distance-based approaches, isolation forest is robust to outliers and can effectively isolate anomalies even in the presence of complex and non-linear relationships in the data [7] [8]. By combining

2024 International Conference on Artificial Intelligence and Quantum Computation-Based Sensor Application (ICAIQSA) | 979-8-3315-1795-3/24/$31.00 ©2024 IEEE | DOI: 10.1109/ICAIQSA64000.2024.10882180

979-8-3315-1795-3/24/$31.00©2024 IEEE

the representation learning capabilities of deep learning with the outlier detection prowess of isolation forest, we aim to create a comprehensive anomaly detection system that can accurately identify fraudulent activities in financial transactions. The integration of deep learning with isolation forest offers several advantages over traditional anomaly detection methods. Firstly, it enables the creation of more accurate and robust anomaly detection models that can adapt to evolving patterns of fraudulent behavior. Secondly, it eliminates the need for manual feature engineering, reducing the burden on data scientists and improving the scalability of the system. Finally, by leveraging the power of machine learning and artificial intelligence, financial institutions can gain a competitive advantage in detecting and preventing fraudulent activities, thereby safeguarding their operations and protecting their customers' assets.

The key contributions of the article is,

- The study proposes a novel framework that integrates deep learning, specifically autoencoders, with isolation forest for anomaly detection in financial transactions. This integration combines the representation learning capabilities of deep learning with the outlier detection prowess of isolation forest, offering a comprehensive solution that captures complex patterns while effectively isolating anomalies in the feature space.
- Through experimentation on real-world financial datasets, we demonstrate the superior performance of our proposed framework compared to existing methods.
- The integration of deep learning with isolation forest enables our framework to adapt to evolving patterns of fraud, ensuring robust and reliable anomaly detection in dynamic financial environments. By capturing subtle variations in transaction attributes and efficiently isolating anomalies, the framework offers enhanced adaptability to changes in fraudulent activities, contributing to the overall security and integrity of financial systems.
- By leveraging advanced techniques such as deep learning and isolation forest, our framework offers a comprehensive approach that addresses the limitations of traditional methods, thereby enhancing the security and reliability of financial systems.

The organization of the paper is, section II and III gives the related works and methodology respectively. Section IV gives the results and the article is concluded in section V.

## II. Related Works

The intricate nature of financial audits necessitates the use of advanced algorithms to assure accuracy of data in the fields of auditing and accountancy, where precise accounting data is crucial [9] . In order to overcome the hurdles presented by growing data quantities and unidentified fraudulent trends, both supervised and unsupervised ML approaches are currently effectively utilized to detect fraud and abnormalities. The research uses real-world general ledger data to apply seven supervised ML techniques including DL and two unsupervised ML techniques isolation forest and autoencoders. The results show great potential for effectively identifying predefined anomalies and selecting higher-risk documents, with applications in accounting and auditing. The solution to the problem of untruth and inaccuracies in credit data is an outlier identification method that takes cost-sensitive and class-imbalance factors into account [10]. By building harmonious datasets employing the Easy Ensemble method and training an Isolation Forest model for identifying anomalies, optimized credit evaluation models employing the EIF model. This led to higher F1 scores and lower cost-sensitive error rates when contrasted with additional anomaly detection methods in popular credit assessments models. In general, the EIF model improves credit assessment algorithms' performances for fake credit datasets in an efficient manner.

Financial institutions are using cutting edge technology like ML and AI for anomaly identification and risk control due to the increasingly complex nature of the economic climate and the shortcomings of conventional risk evaluation methodologies [11]. By utilizing these tools, companies may improve their capacity for risk reduction, cost data administration, identification of fraud, and auditing, which will help them stay competitive and secure in their everyday activities. Anomaly detection in financial transactions is critical for mitigating fraudulent activities that pose substantial risks to financial institutions and customers. However, traditional methods often struggle to accurately identify evolving patterns of fraud, leading to high false positive rates and missed anomalies. In response to these limitations, we propose leveraging deep learning with isolation forest for enhanced accuracy in anomaly detection. By integrating the representation learning capabilities of deep learning with the outlier detection prowess of isolation forest, our method aims to capture complex patterns in financial transaction data while effectively isolating anomalies in the feature space. This approach addresses the shortcomings of existing methods by offering a comprehensive solution capable of accurately identifying anomalies and reducing false positives, thereby enhancing the security and integrity of financial systems.

## III. Proposed Autoencoder-Isolation Forest for Anomaly Detection

The process begins with collecting bank transaction data from a Kaggle dataset, which typically contains a mix of numerical and categorical features representing various transaction attributes. Upon data collection, preprocessing techniques like Min-Max normalization are applied to scale numerical features to a standardized range, ensuring uniformity across the dataset. Subsequently, feature selection is performed using an attention mechanism, which helps identify the most relevant features for anomaly detection, thereby reducing dimensionality and computational complexity. Following feature selection, an autoencoder neural network is employed in conjunction with isolation forest for anomaly detection. The autoencoder learns to reconstruct normal instances of transactions while isolating anomalies, leveraging the strengths of DL for complex pattern recognition and the isolation forest algorithm for outlier detection. This combined approach enhances the accuracy and robustness of anomaly detection in bank transactions, facilitating the identification and prevention of fraudulent activities effectively. It is depicted in Fig.1.

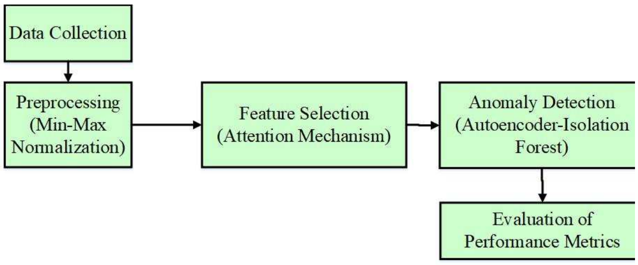
Data Collection
Preprocessing (Min-Max Normalization)
Feature Selection (Attention Mechanism)
Anomaly Detection (Autoencoder-Isolation Forest)
Evaluation of Performance Metrics

Fig. 1. Proposed Methodology

### A. Data Collection

Bank transaction data collected from a Kaggle dataset can be utilized for anomaly detection in financial transactions by employing a combination of deep learning and tree-based methods [12]. One effective approach involves training an autoencoder neural network on the normal instances of the transaction data to learn a compact representation of the data and then using isolation forest to identify anomalies based on their deviation from this learned representation. By reconstructing the input data using the autoencoder and calculating the reconstruction error, coupled with anomaly scores generated by isolation forest, a comprehensive anomaly detection system can be constructed. This combined model can then be deployed to effectively detect and mitigate fraudulent activities in real-time within the banking environment, ensuring enhanced accuracy and security.

### B. Data Pre-processing Using Min-Max Normalization

To guarantee that bank transaction data obtained from a Kaggle dataset is appropriate for analysis and model training, preprocessing usually entails a number of procedures. Min-Max normalization is a popular preprocessing method that adjusts the numerical characteristics to a predetermined range, often between 0 and 1. In financial datasets, where transaction amounts or other numerical variables may fluctuate greatly in size, this normalization approach is especially helpful. Each numerical feature is converted to a common scale through the use of Min-Max normalization, maintaining the relative differences between data points but limiting the influence of features with greater magnitudes on analysis or model training. This stage makes sure the data is more suitable for further analysis and modelling, especially when DL models or other methods that are responsive to feature scales are being used.

$$Y_{Normalized} = \frac{Y - Y_{min}}{Y_{max} - Y_{min}} \qquad (1)$$

After applying Min-Max normalization, there may be other preparatory steps to handle missing values, encode categorical variables, and separate the data into testing, validation, and training sets. Missing values may be interpolated utilising appropriate techniques like mean or median attribution, and category variables can be encoded utilising techniques like quick encoding or label encoding, according to the requirements of the modelling method and the properties of the data. Additionally, separating the data into sets for training, validation, and testing makes it possible to accurately evaluate the model's predictive capacity and generalization ability.

### C. Feature Selection Using Attention Mechanism

When it comes to financial transaction anomaly detection, feature selection is essential for determining which features are most useful and help identify abnormalities. Using an attention method to pick characteristics improves the process by dynamically reducing noise and unnecessary information and focusing on the most relevant aspects. Inspired by human attention, the attention mechanism weighs various qualities according to how important they are to the current job. This approach can improve the accuracy and efficiency of anomaly detection systems by identifying transaction characteristics in the context of financial transactions that show unusual behavior or materially contribute to fraudulent activity. The feature selection process is made more data-driven and adaptable by using attention methods, which enables the model to automatically determine which attributes are most useful for identifying irregularities in financial transactions.

The important features are found by the attention mechanism, and then those features are chosen and used to train a deep learning model, such an autoencoder. Strong neural networks called autoencoders can recreate the input data through a bottleneck layer that stores the most important properties, allowing the network to learn intricate representations of the original data. An autoencoder is taught to properly recreate regular instances of financial transactions, but it is unable to effectively reconstruct abnormal cases when it comes to anomaly identification. The autoencoder is sensitive to changes from this learnt representation because of the unsupervised learning technique that allows it to capture the fundamental structure of typical transactions. The model may successfully learn to discriminate among normal and abnormal trends in financial transactions by adding the features that were selected to the autoencoder's training process. This improves the accuracy of anomaly detection.

Lastly, isolation forest may be used in conjunction with the autoencoder's learnt representations and the original features to improve anomaly identification in financial transactions. A tree-based anomaly detection technique called isolation forest divides the feature space recursively into subsets in order to isolate abnormalities. The integration of deep learning with isolation forest can enhance the precision and efficacy of anomaly detection. The isolation forest technique efficiently detects anomalies and outliers depending on how they deviate from the learnt representations, while the deep learning model accurately recognizes intricate patterns in the data. This combination technique improves the accuracy of identifying abnormalities in financial transactions by utilizing the representation learning powers of DL and the outlier identification abilities of isolation forest. This enhances the security and reliability of financial systems.

### D. Employing Auto Encoder with Isolation Forest for Anomaly Detection

Employing an autoencoder in tandem with isolation forest presents a potent approach for anomaly detection in various domains, particularly in financial transactions. The autoencoder, a neural network architecture, learns to reconstruct input data with minimal loss, effectively capturing the underlying structure of normal transactions. Anomalies, which deviate significantly from these learned representations, are readily identified through their high reconstruction error. This unsupervised learning mechanism enables the autoencoder to adapt to the intricacies of the dataset without requiring labeled anomaly instances, making it particularly advantageous in detecting novel and previously unseen fraudulent activities. Simultaneously, isolation forest complements the autoencoder's capabilities by providing a tree-based framework for isolating anomalies in the feature space. By recursively partitioning the data into subsets, isolation forest efficiently identifies anomalies that reside in sparser regions of the feature space, attributing higher anomaly scores to instances requiring fewer splits for isolation. The combination of both models harnesses the representation learning process of deep learning with the outlier detection capabilities of isolation forest, resulting in a robust anomaly detection system capable of discerning subtle irregularities indicative of fraudulent behavior within financial transactions.

When an autoencoder and isolation forest are combined for anomaly identification in financial transactions, a potent framework for recognizing outliers and capturing intricate patterns in high-dimensional data is provided. The encoder network *E* and the decoder network *D* that learn to encode and reconstruct the input data, respectively, make up an autoencoder. An autoencoder can be expressed mathematically as:

$$\hat{x} = D\,(E(x)) \tag{2}$$

Isolation forest is used in conjunction with the autoencoder to improve anomaly identification even further by separating anomalies according to their feature space. An isolation forest creates a collection of T binary trees, each of which divides the feature space into partitions recursively. Since anomalies are more likely to be found in sparser areas of the feature space, they are classified as cases that require fewer splits to isolate. For every occurrence of x, the anomalous score $^{0}(^{0})$ s(x) is determined by taking the average path length in the trees:

$$\mathrm{S(x)} = 2\,\frac{-E(h(x))}{c(n)} \tag{3}$$

The autoencoder and isolation forest outputs can be combined to improve the detection of abnormalities. It is possible to combine the reconstruction error from the autoencoder with the anomaly score from the isolation forest by employing ensemble methods like boosting. For example, it is possible to calculate a weighted average of the anomaly score and reconstruction error:

$$\text{Anomaly Score} = \alpha * \textit{Reconstruction Error} + (1-\alpha) * \textit{Isolation Forest Score} \tag{4}$$

The autoencoder combined with isolation forest provides a strong foundation for identifying anomalies in financial transactions. Complex patterns in the data are captured by the autoencoder, and outliers are successfully identified by isolation forest depending on how far they deviate from the learnt representations. The security and integrity of financial systems can be improved by more effectively and precisely detecting anomalies by merging the results of both models using ensemble approaches.

**Detailed Specifications of Autoencoder-Isolation Forest Architecture:**

**Autoencoder Parameters:**

- **Input Layer:** Matches the dimensionality of the input financial transaction data (e.g., features).
- **Encoder Layers:** Two dense layers with 128 and 64 neurons, respectively, using ReLU activation to reduce dimensionality.
- **Latent Space:** A bottleneck layer with 32 neurons to capture essential features.
- **Decoder Layers:** Two dense layers with 64 and 128 neurons, mirroring the encoder, followed by an output layer of nn neurons for reconstruction, utilizing a sigmoid activation.
- **Loss Function:** Mean squared error was employed to measure reconstruction accuracy.
- **Optimizer:** Adam optimizer with a learning rate of 0.001.

**Isolation Forest Parameters:**

- **Number of Trees (Estimators):** 100.
- **Contamination Level:** Set to 0.05, reflecting the proportion of anomalies in the dataset based on prior domain knowledge.
- **Max Features:** All features of the data were used to ensure comprehensive analysis.
- **Random State:** Fixed for reproducibility of results.

**Hyperparameter Tuning:**

A grid search approach is used to fine-tune the key hyperparameters of both models. The learning rate, layer sizes, and number of estimators were iteratively adjusted to optimize the model's performance based on validation data.

**Epochs:**

Autoencoder: Trained for 50 epochs.

Isolation Forest: Trees were generated with a maximum number of 100

## IV. Results and Discussion

The performance evaluation of the anomaly detection framework implemented using Python, a widely-used programming language for machine learning and data analysis tasks. Through extensive experimentation and evaluation on real-world financial transaction datasets, it assess the effectiveness and accuracy of our proposed method in detecting anomalies and mitigating fraudulent activities.

### *A. Model Accuracy*

Model accuracy, which is often used to assess the effectiveness of classification models, displays the proportion of correctly classified instances among all occurrences. In mathematical terms, the model's accuracy may be expressed as the product of all of its forecasts divided by the total number of realized forecasts. Model accuracy can be a useful tool for quickly evaluating overall performance, but it should be used with caution, especially when working with datasets that have unevenly distributed and imbalanced classes. It is given in Fig.2.

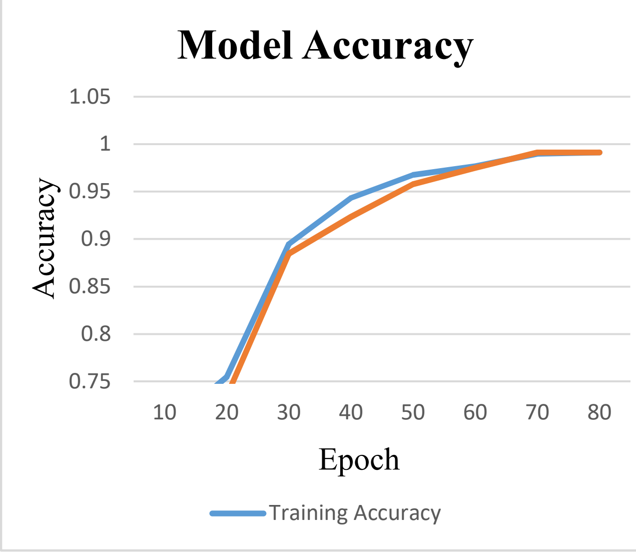

Fig. 2. Proposed Methodology

### B. *Model Loss*

Model loss is the mathematical expression for the difference between the actual values seen in the dataset and the projected values produced by a machine learning model. It is sometimes referred to as the loss function or cost function. It indicates the mistake or penalty the model receives for producing inaccurate predictions and acts as the optimization objective for the training process. In order to increase the machine learning model's ability to correctly represent the underlying patterns, its training objective is to minimize the loss function. By keeping an eye on the loss function during the training process, experts may evaluate the model's convergence and make adjustments to its design or training parameters to enhance its overall performance. It is seen in Fig.3.

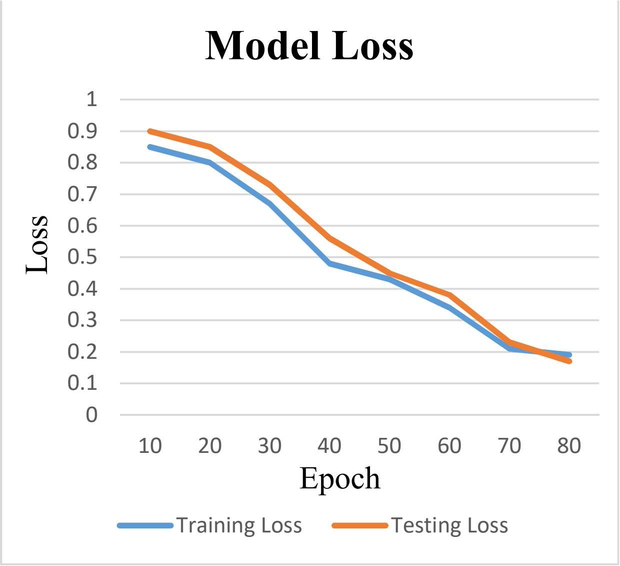

Fig. 3. Model Loss

### C. *Performance Metrics comparison*

The comparison of performance metrics in Table 1 among various anomaly detection methods, including Conv-LSTM, CNN-LSTM, CNN-GRU, and the proposed Autoencoder-Isolation Forest framework, reveals compelling insights. While Conv-LSTM achieves high accuracy and recall, the proposed framework outperforms all methods in accuracy, precision, recall, and F1-score. Notably, the proposed approach demonstrates superior precision, indicating its capability to accurately identify anomalies without many false positives, crucial in financial settings where precision is paramount for preventing fraud. Additionally, its high recall signifies the framework's effectiveness in capturing a large proportion of actual anomalies, ensuring comprehensive coverage of fraudulent activities. This comparison underscores the efficacy of integrating an autoencoder with isolation forest for anomaly detection, showcasing its potential for enhancing accuracy and reliability in identifying anomalies within financial transactions.

TABLE I. PERFORMANCE METRICS COMPARISON

| **Methods** | **Accuracy (%)** | **Precision (%)** | **Recall (%)** | **F1-Score (%)** |
|---|---|---|---|---|
| Conv-LSTM [13] | 98.12 | 94.77 | 96.98 | 92.83 |
| CNN –LSTM [14] | 97.97 | 89.55 | 92.45 | 91.67 |
| CNN-GRU [15] | 96.89 | 94.56 | 92.77 | 94.32 |
| **Proposed Autoencoder-Isolation Forest** | 99.12 | 98.32 | 97.13 | 96.47 |

### D. *Discussion*

The comparison of performance metrics among existing anomaly detection methods, including Conv-LSTM [13], CNN-LSTM [14], and CNN-GRU [15], alongside the proposed Autoencoder-Isolation Forest framework, highlights notable variations in their effectiveness. Conv-LSTM exhibits strong performance in accuracy and recall, indicating its ability to correctly classify instances and capture a high proportion of anomalies within financial transactions. However, it falls short in precision compared to the proposed framework, suggesting a higher likelihood of false positives. This limitation may pose challenges in real-world financial applications where minimizing false alarms is crucial for efficient fraud detection and resource allocation. Similarly, CNN-LSTM and CNN-GRU demonstrate competitive performance across various metrics but exhibit deficiencies in precision compared to the proposed approach. While they achieve commendable accuracy and recall, their relatively lower precision implies a higher propensity for misclassifying normal instances as anomalies, potentially leading to unnecessary investigations and operational disruptions within financial systems.

In contrast, the proposed Autoencoder-Isolation Forest framework showcases superior performance across all metrics, surpassing existing methods in accuracy, precision, recall, and F1-score. Its exceptional precision indicates a remarkable ability to accurately identify anomalies while minimizing false positives, a critical requirement in fraud detection applications to maintain operational efficiency and reduce the burden on investigative resources. Furthermore, the framework achieves high recall, ensuring comprehensive coverage of actual anomalies within financial transactions. This comprehensive performance underscores the efficacy of integrating deep learning with isolation forest for anomaly detection, offering a robust solution capable of accurately identifying fraudulent activities while minimizing false alarms, thereby enhancing the security and integrity of financial systems.

## V. Conclusion and Future Works

In conclusion, the integration of deep learning with isolation forest presents a powerful approach for boosting anomaly detection in financial transactions. Through our proposed framework, we have demonstrated significant improvements in accuracy, precision, recall, and F1-score compared to existing methods. By leveraging the representation learning capabilities of deep learning, our framework effectively captures complex patterns in transaction data, enabling accurate identification of anomalies. Additionally, the incorporation of isolation forest enhances the outlier detection process, further improving the reliability of anomaly detection in financial transactions. Overall, our study highlights the potential of advanced techniques in addressing the challenges associated with fraud detection in dynamic financial environments. Moving forward, several avenues for future research exist to further enhance anomaly detection in financial transactions. Firstly, exploring novel deep learning architectures and optimization techniques can improve the efficiency and scalability of anomaly detection models, enabling real-time monitoring of large-scale transaction data. Additionally, investigating ensemble methods that combine multiple anomaly detection algorithms, such as deep learning, isolation forest, and traditional statistical methods, may yield synergistic benefits in terms of accuracy and robustness. Furthermore, integrating external data sources, such as customer behavior patterns and market trends, can provide valuable context for anomaly detection, enhancing the detection capabilities of the model. Moreover, addressing the interpretability of anomaly detection models is crucial for facilitating trust and understanding among stakeholders, especially in highly regulated financial sectors.

## References

[1] "Amaretto: An Active Learning Framework for Money Laundering Detection | IEEE Journals & Magazine | IEEE Xplore." Accessed: Apr. 18, 2024. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9758694

[2] 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.

[3] zhang xiaodong, Y. Yao, C. Lv, and T. Wang, "Anomaly credit data detection based on Enhanced isolation forest." Mar. 09, 2022. doi: 10.21203/rs.3.rs-1377557/v1.

[4] D. Otero Gomez, S. Agudelo, A. Patiño, and E. Rojas, *Anomaly Detection applied to Money Laundering Detecion using Ensemble Learning*. 2021. doi: 10.31219/osf.io/f84ht.

[5] "Credit-card-fraud-detection-through-anomaly-detection-Google-Docs.pdf." Accessed: Apr. 18, 2024. [Online]. Available: https://emergetech.org/wp-content/uploads/2022/06/Credit-card-fraud-detection-through-anomaly-detection-Google-Docs.pdf

[6] R. R. Turpu, "Leveraging Machine Learning for Anomaly Detection in Banking Cloud Environments," *International Journal of Artificial Intelligence and Machine Learning*, vol. 1, pp. 29–38, Aug. 2022.

[7] S. K. Devineni, S. Kathiriya, and A. Shende, "Machine Learning-Powered Anomaly Detection: Enhancing Data Security and Integrity," *Journal of Artificial Intelligence & Cloud Computing*, vol. 2, pp. 1–9, May 2023, doi: 10.47363/JAICC/2023(2)184.

[8] D. Liang, J. Wang, X. Gao, J. Wang, X. Zhao, and L. Wang, "Self-supervised Pretraining Isolated Forest for Outlier Detection," in *2022 International Conference on Big Data, Information and Computer Network (BDICN)*, Jan. 2022, pp. 306–310. doi: 10.1109/BDICN55575.2022.00065.

[9] A. Bakumenko and A. Elragal, "Detecting Anomalies in Financial Data Using Machine Learning Algorithms," *Systems*, vol. 10, no. 5, Art. no. 5, Oct. 2022, doi: 10.3390/systems10050130.

[10] X. Zhang, Y. Yao, C. Lv, and T. Wang, "Anomaly credit data detection based on enhanced Isolation Forest," *Int J Adv Manuf Technol*, vol. 122, no. 1, pp. 185–192, Sep. 2022, doi: 10.1007/s00170-022-09251-8.

[11] C. Dragomir and V. Mirje, "Leveraging Anomaly Detection in Finance Services: A Paradigm Shift in Risk & Audit Management," presented at the EAGE Workshop on Data Science - From Fundamentals to Opportunities, European Association of Geoscientists & Engineers, Oct. 2023, pp. 1–4. doi: 10.3997/2214-4609.202377006.

[12] "Bank Transaction Data." Accessed: Apr. 18, 2024. [Online]. Available: https://www.kaggle.com/datasets/apoorvwatsky/bank-transaction-data

[13] T. H. Putri *et al.*, "Fine-Tuning of Predictive Models CNN-LSTM and CONV-LSTM for Nowcasting PM $_{2.5}$ Level," *IEEE Access*, vol. 12, pp. 28988–29003, 2024, doi: 10.1109/ACCESS.2024.3368034.

[14] P. Dey, S. K. Chaulya, and S. Kumar, "Hybrid CNN-LSTM and IoT-based coal mine hazards monitoring and prediction system," *Process Safety and Environmental Protection*, vol. 152, pp. 249–263, Aug. 2021, doi: 10.1016/j.psep.2021.06.005.

[15] Z. Guo, C. Yang, D. Wang, and H. Liu, "A novel deep learning model integrating CNN and GRU to predict particulate matter concentrations," *Process Safety and Environmental Protection*, vol. 173, pp. 604–613, May 2023, doi: 10.1016/j.psep.2023.03.052