AI-Driven Anomaly Detection in Financial Transactions

Abstract:

This research explores the implementation of advanced anomaly detection techniques in financial transaction data using AI-driven models. Emphasis is placed on the utilization of Isolation Forest and Autoencoder models to identify irregular patterns that may indicate fraudulent activities or data integrity issues. By enhancing the ability to detect anomalies, organizations can improve their security infrastructure and data accuracy.

1. Introduction:

Financial institutions process millions of transactions daily, making it increasingly difficult to manually detect fraud and irregularities. Traditional rule-based systems are limited in adaptability and efficiency. Anomaly detection using AI provides a dynamic solution to this challenge by leveraging patterns in data to identify unusual behaviors.

2. Background and Related Work:

Anomaly detection in financial systems has evolved with advancements in artificial intelligence and machine learning. Methods such as clustering, statistical models, and more recently, deep learning, have been utilized. Prior studies highlight the limitations of conventional techniques and demonstrate the efficacy of AI-based models in high-dimensional and complex datasets.

3. Methodology:

This research applies two primary machine learning models for anomaly detection:

- Isolation Forest: This algorithm isolates anomalies instead of profiling normal data points. It works efficiently with high-dimensional datasets and is particularly effective in detecting outliers.
- Autoencoders: A type of neural network trained to reconstruct input data. Large reconstruction

errors often indicate anomalies, making autoencoders useful in unsupervised anomaly detection scenarios.

4. Implementation:

The models were trained on anonymized financial transaction datasets that include features such as transaction amount, time, location, and merchant details. Data preprocessing included normalization and feature engineering. Model performance was evaluated using metrics such as precision, recall, and F1-score.

5. Results and Analysis:

Both models demonstrated a significant improvement in detecting fraudulent transactions compared to baseline rule-based systems. Isolation Forest provided quick anomaly scores, while Autoencoders captured subtle nonlinear anomalies with higher precision.

6. Discussion:

The choice between Isolation Forest and Autoencoders depends on the specific use case, data structure, and computational resources. Combining both models can lead to a hybrid approach for enhanced detection.

7. Conclusion:

AI-driven anomaly detection offers a robust framework for identifying irregular financial transactions. By integrating models like Isolation Forest and Autoencoders, organizations can enhance their fraud detection systems, reduce false positives, and maintain data integrity.

8. Future Work:

Future research will focus on real-time anomaly detection, model interpretability, and the integration of ensemble methods to further increase accuracy and reliability.

References:

1. Liu, F. T., Ting, K. M., & Zhou, Z.-H. (2008). Isolation forest. IEEE ICDM.

2. Sakurada, M., & Yairi, T. (2014). Anomaly detection using autoencoders with nonlinear dimensionality reduction. Proceedings of the MLSDA 2014.

3. Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. ACM Computing Surveys.