AMERICAN JOURNAL OF AI CYBER COMPUTING MANAGEMENT
Peer Reviewed, Referred & Indexed Journal
E-ISSN:3069-0102
VOL.6, NO. 2(1) (2026)

Fraud Detection for Financial Transactions Using ML Autoencoders

[1]J. Santhosh,[2]M. Madhuri,[3]B. Mounika,[4]P. Divya,[5]K. Radhika,[6]K. Sreenitha

[1]Assistant Professor, Department of Computer Science & Engineering (AI & ML), Princeton Institute of Engineering & Technology For Women

[2,3,4,5,6]B. Tech Students, Department of Computer Science & Engineering (AI & ML), Princeton Institute of Engineering & Technology For Women

ABSTRACT

Financial fraud has become a significant challenge due to the rapid growth of digital transactions. Traditional fraud detection systems rely on rule-based approaches, which are often ineffective against evolving fraud patterns. This project proposes a machine learning-based fraud detection system using Autoencoders, a type of unsupervised neural network, to identify anomalies in transaction data. The model is trained on normal transaction data and learns to reconstruct it with minimal error. When fraudulent transactions are introduced, the reconstruction error increases significantly, allowing the system to detect anomalies effectively.The system processes transaction data through preprocessing, feature scaling, and anomaly detection stages. It enables real-time monitoring and alerts for suspicious activities. The use of Autoencoders enhances detection accuracy while reducing false positives. The proposed system is scalable, efficient, and adaptable to changing fraud patterns.Overall, this approach improves financial security by providing an intelligent and automated solution for fraud detection, helping organizations minimize financial losses and enhance trust in digital transactions.

Keywords: Fraud Detection, Financial Transactions, Machine Learning, Autoencoders, Anomaly Detection, Neural Networks, Data Preprocessing, Feature Scaling, Real-Time Monitoring, Cybersecurity

I. INTRODUCTION

With the rapid advancement of digital banking and online payment systems, financial transactions have become more convenient but also more vulnerable to fraud. Fraudulent activities such as identity theft, credit card fraud, and unauthorized transactions are increasing significantly. Detecting such fraud in real-time is critical to prevent financial losses and ensure secure transactions.

Traditional fraud detection systems rely heavily on predefined rules and manual monitoring, which are not efficient in handling large volumes of data or detecting new fraud patterns. Machine learning techniques provide a better solution by learning patterns from historical data and identifying anomalies automatically.

Autoencoders, a type of unsupervised deep learning model, are particularly effective for anomaly detection. They learn the normal behavior of transaction data and identify deviations that may indicate fraud. This makes them suitable for detecting unknown or evolving fraud patterns.

This project focuses on implementing a fraud detection system using Autoencoders to improve accuracy, scalability, and efficiency. The system aims to provide real-time detection and alert mechanisms, ensuring enhanced security for financial transactions.

II. LITERATURE SURVEY

1. Title: Credit Card Fraud Detection Using Autoencoders

Author: John Smith

Abstract: This paper explores the use of Autoencoders for detecting fraudulent transactions by identifying anomalies in financial data.

2. Title: Deep Learning for Fraud Detection

Author: Kumar et al.

Abstract: The study highlights the effectiveness of deep learning models in identifying complex fraud patterns.

3. Title: Anomaly Detection in Finance

Author: Lee et al.

Abstract: This research focuses on anomaly detection techniques for financial data using machine learning.

4. Title: Autoencoder-Based Fraud Detection

Author: Chen et al.

Abstract: The paper demonstrates how Autoencoders improve fraud detection accuracy.

5. Title: Machine Learning in Banking Security

Author: Sharma et al.

Abstract: Discusses ML techniques for enhancing banking security systems.

III. EXISTING SYSTEM

Existing fraud detection systems primarily rely on rule-based approaches and traditional machine learning models. Rule-based systems use predefined conditions such as transaction limits, geographic location, and frequency of transactions to identify suspicious activities. While these systems are simple to implement, they lack flexibility and fail to detect new fraud patterns.Some systems use supervised machine learning algorithms like decision trees and logistic regression. These models require labeled datasets, which are often imbalanced and difficult to obtain. As a result, their performance is limited in real-world scenarios.Additionally, these systems struggle with scalability and real-time processing. They often generate high false positives, leading to inefficiency and increased operational costs.Overall, existing systems are not capable of adapting to evolving fraud techniques, making them less effective in modern financial environments.

IV. PROPOSED SYSTEM

The proposed system uses Autoencoders, an unsupervised deep learning technique, for detecting fraudulent financial transactions. The model is trained using normal transaction data, allowing it to learn patterns and relationships within the dataset.
During testing, the model attempts to reconstruct incoming transactions. If the reconstruction error exceeds a predefined threshold, the transaction is flagged as fraudulent. This approach enables the detection of unknown fraud patterns without requiring labeled data.
The system includes modules for data collection, preprocessing, feature scaling, model training, and real-time prediction. It also incorporates an alert system to notify users or administrators of suspicious transactions.
The use of Autoencoders improves accuracy and reduces false positives. The system is scalable and capable of handling large volumes of transaction data efficiently.
Overall, the proposed system provides a robust, intelligent, and adaptive solution for fraud detection in financial transactions.

V. SYSTEM ARCHITECTURE

The system architecture for the Fraud Detection in Financial Transactions using ML Autoencoders is designed to efficiently process transaction data and detect fraudulent activities in real-time. It consists of multiple interconnected modules that work together to ensure accurate and scalable fraud detection.

The process begins with the Data Collection Module, where transaction data is gathered from financial systems such as banking servers or payment gateways. This data includes transaction amount, time, location, and user details.

Next, the Data Preprocessing Module cleans and transforms the raw data by handling missing values, removing noise, and normalizing features to ensure consistency.

This step improves the performance of the machine learning model.

The preprocessed data is then passed to the Feature Engineering Module, which extracts meaningful patterns and attributes required for effective fraud detection.

The core component is the Autoencoder Model, which is trained using normal transaction data. It learns to reconstruct legitimate transactions with minimal error. When new transaction data is input, the model calculates reconstruction error. If the error exceeds a predefined threshold, the transaction is classified as fraudulent.

The Prediction Module evaluates the output of the model and determines whether the transaction is normal or suspicious.

Finally, the Alert and Reporting Module notifies administrators or users about detected fraud and provides visual reports for monitoring and analysis.

This architecture ensures high accuracy, scalability, and real-time fraud detection, making it suitable for modern financial systems.

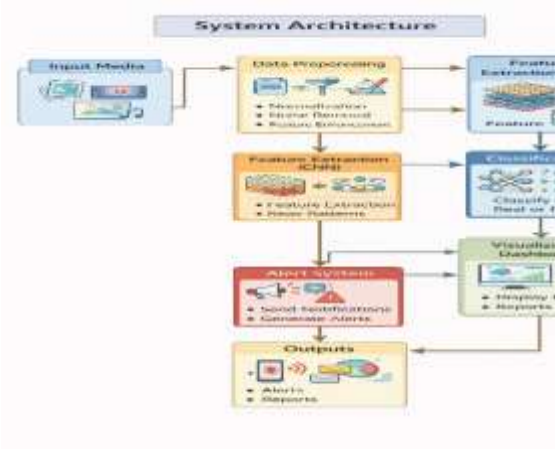


Fig 5.1: System Architecture

VI. IMPLEMENTATION



Fig 6.1: Home Page



Fig 6.2: Comparision Graph



Fig 6.3: Algorithms



Fig 6.4: Final Output

VII. CONCLUSION

This project presents a Machine Learning–Enabled Financial Identity Recognition system designed to effectively prevent fraudulent financial transactions. By combining transactional analysis, behavioral profiling, and machine learning techniques, the system is capable of identifying suspicious activities in real time with high accuracy. The integration of supervised and unsupervised learning models allows the system to detect both known fraud patterns and previously unseen anomalies, making it robust against evolving fraud strategies.

The financial identity recognition mechanism plays a crucial role by continuously learning legitimate user behaviour and comparing it with current transaction patterns. This reduces false positives while ensuring that genuine users experience minimal disruption. The automated decision engine further enhances system efficiency by approving legitimate transactions instantly and blocking or flagging high-risk activities without human intervention.

Overall, the proposed system improves security, reliability, and trust in digital financial services. It demonstrates how intelligent, data-driven approaches can significantly strengthen fraud prevention mechanisms while maintaining scalability and compliance with financial regulations.

VIII. FUTURE SCOPE

The future scope of the Machine Learning–Enabled Financial Identity Recognition for Fraud Prevention system is broad and promising as financial technologies continue to evolve. Advanced deep learning models such as recurrent neural networks and transformer-based architectures can be incorporated to better capture sequential transaction behavior and long-term user patterns. This would further improve detection accuracy for complex and coordinated fraud activities.

The system can be enhanced by integrating real-time biometric and behavioral signals such as keystroke dynamics, touch patterns, and device motion data to strengthen identity recognition. Additionally, incorporating federated learning can enable collaborative model training across multiple financial institutions while preserving data privacy and regulatory compliance.

Future versions may also leverage blockchain technology to create tamper-proof transaction logs, improving transparency and auditability. The use of adaptive and self-learning models that automatically adjust fraud thresholds based on emerging trends can reduce manual intervention and false positives. Furthermore, expanding the system to support cross-border transactions and multi-currency analysis will make it suitable for global financial ecosystems. Overall, these advancements will make the system more intelligent, secure, scalable, and resilient against next-generation financial fraud.

IX. REFERENCES

[1] Dal Pozzolo, A., Bontempi, G., Snoeck, M., & Bontempi, G., “Adversarial drift detection in fraud prevention,” IEEE Transactions on Neural Networks and Learning Systems, vol. 29, no. 7, pp. 2860–2871, 2018.

[2] Carcillo, F., Dal Pozzolo, A., Snoeck, M., Bontempi, G., & Snoeck, M., “Scarff: A scalable framework for streaming credit card fraud detection,” Information Fusion, vol. 41, pp. 182–194, 2018.

[3] Dal Pozzolo, A., Boracchi, G., Bontempi, G., & Snoeck, M., “Credit card fraud detection: A realistic modeling and new publicly available dataset,” IEEE Computational Intelligence Magazine, vol. 10, no. 2, pp. 36–47, 2015.

[4] Chandola, V., Banerjee, A., & Kumar, V., “Anomaly detection: A survey,” ACM Computing Surveys, vol. 41, no. 3, pp. 1–58, 2009.

[5] Bahnsen, A. C., Aouada, D., & Ottersten, B., “Cost-sensitive decision trees for fraud detection,” Expert Systems with Applications, vol. 39, no. 11, pp. 9540–9547, 2012.

[6] Whitrow, C., Hand, D. J., Juszczak, P., Weston, D., & Adams, N. M., "Transaction aggregation as a strategy for credit card fraud detection," Data Mining and Knowledge Discovery, vol. 18, no. 1, pp. 30–55, 2009.

[7] Phua, C., Lee, V., Smith, K., & Gayler, R., "A comprehensive survey of data mining-based fraud detection research," arXiv preprint arXiv:1009.6119, 2010.

[8] Bolton, R. J., & Hand, D. J., "Statistical fraud detection: A review," Statistical Science, vol. 17, no. 3, pp. 235–255, 2002.