International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X
www.ijdim.com
Original Research Paper

Unsupervised Learning for Anomaly Detection in Financial Transactions

[1]Dr. D. Nagesh Babu,[2]Valluri Harini,[3]Uppala Mounika,[4]Vusa Yuva Gowtham Kumar

[1]Associate Professor, Dept of Computer Science and Engineering, St. Ann's College of Engineering and Technology, Chirala-523187, India.

[2,3,4]B. Tech Student, Dept of Computer Science and Engineering, St. Ann's College of Engineering and Technology, Chirala-523187, India.

ABSTRACT

The rapid growth of digital banking and online payment systems has resulted in a massive increase in financial transactions, making fraud and anomalous activities a serious concern. This project presents an Unsupervised Learning–based Anomaly Detection System for Financial Transactions, designed to identify unusual and suspicious transaction patterns without relying on labeled data. The system analyzes transaction behavior using machine learning techniques to learn normal patterns and detect deviations. A full stack web application is developed using Python (Flask) for backend processing and HTML, CSS, and JavaScript for frontend visualization. The platform provides interactive dashboards to display transaction insights and detected anomalies. The results demonstrate effective anomaly detection, real-time analysis, and improved interpretability, making the system suitable for financial monitoring and risk prevention.

KEYWORDS: ***Unsupervised process of Learning, Anomaly Detection, Financial Transactions, Machine Learning, Fraud Detection, Flask Web Application***

INTRODUCTION

The increasing use of digital financial services such as online banking, mobile payments, and e-wallets has led to a surge in transaction data. Along with convenience, this growth has also introduced risks such as fraud, misuse, and abnormal transaction behavior. Traditional fraud detection systems often depend on labeled datasets, which are difficult to obtain and may not capture new or evolving fraud patterns.

Unsupervised learning provides an effective solution by learning normal transaction behavior directly from data and identifying anomalies automatically. This project focuses on developing a machine learning–based system that detects unusual financial transactions and presents insights through a user-friendly web interface. The objective is not to replace existing security systems but to

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X
www.ijdim.com
Original Research Paper

support early identification of risky transactions and assist analysts in decision-making.

LITERATURE REVIEW

Several studies have explored anomaly detection in financial transactions using machine learning. Early approaches relied on statistical methods and rule-based systems, which were limited in scalability and adaptability.

Recent research emphasizes unsupervised techniques such as clustering, Isolation Forest, and autoencoders due to their ability to handle unlabeled data. Studies highlight that unsupervised models are effective in detecting previously unseen fraud patterns but face challenges related to interpretability and real-time deployment. Existing research also stresses the importance of visualization and user interaction for better understanding of detected anomalies. These findings motivate the development of a web-based anomaly detection system integrating machine learning with intuitive dashboards.

RELATED WORK

Financial fraud detection systems have evolved from rule-based engines to intelligent machine learning models. Traditional systems used fixed thresholds and expert-defined rules, which failed to adapt to changing transaction behaviors. Later, supervised learning models improved accuracy but required large labeled datasets.

Recent systems utilize unsupervised learning models such as clustering and isolation-based algorithms to detect abnormal transactions. However, many existing solutions lack interactive visualization, scalability, and real-time monitoring features. This project addresses these gaps by integrating unsupervised learning with a full stack web application for improved usability and transparency.

EXISTING METHOD

Existing financial fraud detection systems mainly rely on rule-based techniques or supervised learning models that require predefined rules and labeled fraud data.

In real-world financial environments, labeled data is often limited or unavailable, which reduces the effectiveness of these systems. Rule-based approaches are rigid and fail to detect new or evolving fraud patterns. Supervised models struggle to adapt when transaction behavior changes over time, leading to poor performance. Many existing systems generate a high number of false positives, increasing manual review efforts.

These systems also lack automatic learning capabilities and real-time adaptability. In addition, limited visualization and interpretability make it difficult for users to understand detected anomalies. As a result, the accuracy, scalability, and reliability of traditional fraud detection systems remain insufficient for modern financial applications.

PROPOSED METHOD

The proposed system uses unsupervised machine learning techniques to detect

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X
www.ijdim.com
Original Research Paper

anomalies in financial transaction data. The model learns normal transaction patterns and flags deviations as potential anomalies.

A Flask-based backend processes transaction data and executes the anomaly detection model. The frontend visualizes results using charts and dashboards, enabling easy interpretation. Unlike existing systems, the proposed approach does not require labelled data, supports dynamic behaviour detection, and provides an interactive user interface for monitoring and analysis.

ARCHITECTURE

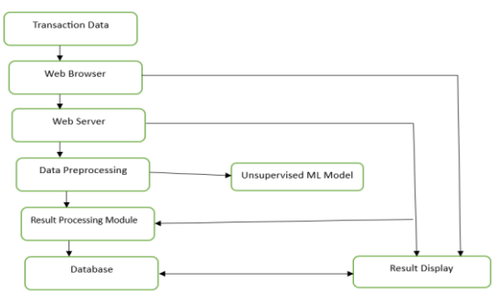

Fig 1: System Architecture

METHODOLOGY DESCRIPTION

User Interaction

Users access the system through a web browser to upload and view financial transaction data. The dashboard provides an easy interface to monitor transactions and detected anomalies. This interaction helps users analyze data without technical complexity.

Web Server

The Flask web server acts as the central controller of the system. It receives requests from the user interface and manages communication between the preprocessing module, machine learning model, and database. This ensures secure and smooth data flow.

Data Preprocessing

Transaction data is cleaned to remove missing or inconsistent values. The data is then normalized and transformed into a suitable format. This step improves the accuracy and reliability of anomaly detection.

Machine Learning Model

The unsupervised learning model learns normal transaction behavior from historical data. It identifies unusual transactions by detecting deviations from these learned patterns. This allows detection of anomalies without labeled fraud data.

Result Visualization

The system displays detected anomalies using graphs and tables. Visualization helps users quickly understand transaction trends and risk patterns. It supports better decision-making through clear insights.

Database Management

The database stores transaction records and anomaly detection results securely. It supports data retrieval for visualization and reporting. This centralized storage enables future analysis and monitoring.

RESULTS AND DISCUSSION

The system successfully identifies abnormal financial transactions and visually distinguishes them from normal ones. Interactive charts help users

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X
www.ijdim.com
Original Research Paper

understand transaction distributions and anomaly behavior. The results show improved detection accuracy without requiring labeled data. The web interface enhances accessibility and usability, making the system suitable for real-world financial monitoring applications.

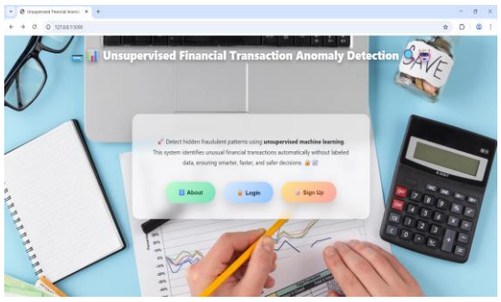

Fig 2: Home page

The homepage provides a clean and user-friendly introduction to the Unsupervised Financial Transaction Anomaly Detection system. It highlights the purpose of detecting unusual financial activities using unsupervised machine learning without labeled data. The page includes quick navigation options such as About, Login, and Sign Up, enabling users to easily access system features.

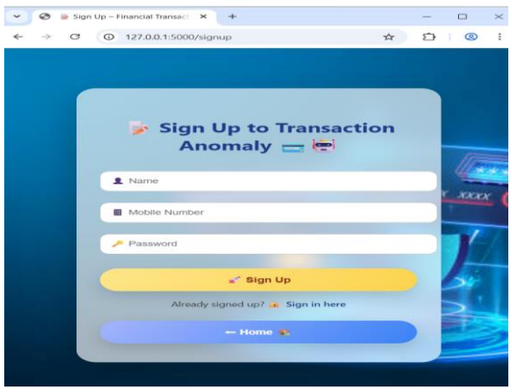

Figure 3: Sign Up Page

The Sign-Up page allows new users to create an account by entering basic details such as name, mobile number, and password. It ensures secure user registration to access the transaction anomaly detection system. After successful registration, users can log in and use the system features through their personalized dashboard**.**

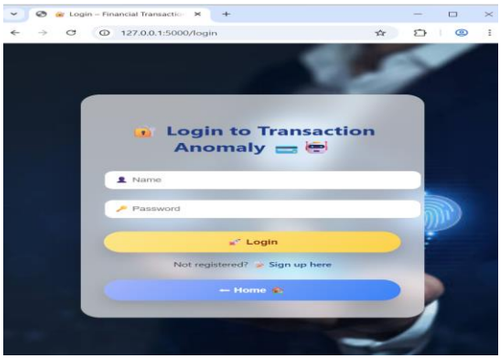

Figure 4: Login Page

The Login page allows registered users to securely access the transaction anomaly detection system using their credentials. It verifies the user details through the backend before granting access to the dashboard. This ensures data security and controlled access to system features.

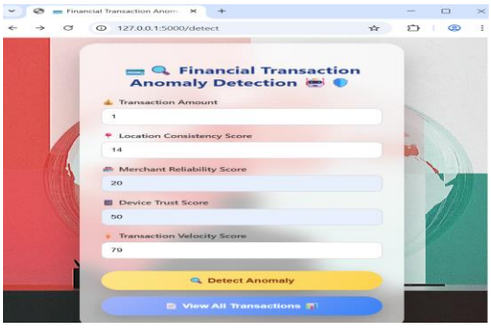

Figure 5: Transaction Anomaly Detection Page

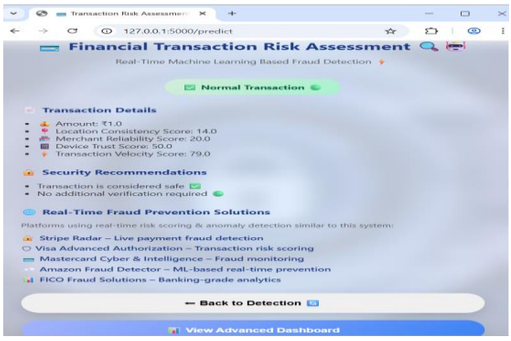

Figure 6: Transaction Risk Assessment Page

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X
www.ijdim.com
Original Research Paper

This page displays the result of the transaction analysis performed using an unsupervised machine learning model. It shows whether the transaction is normal or anomalous along with detailed transaction parameters and risk indicators. The page also provides security recommendations to help users understand the safety level of the transaction and take appropriate action.

Figure 7: Transaction Records Page

This page displays a detailed list of all processed financial transactions along with their parameters and risk status. Each transaction is categorized as normal or low risk based on the anomaly detection results. The tabular view helps users track transaction history and analyze risk patterns efficiently.

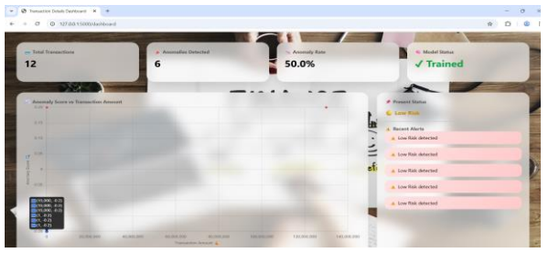

Figure 8: Transaction Details Dashboard

The dashboard provides an overall summary of transaction activity, including total transactions, detected anomalies, anomaly rate, and model status. It visually represents anomaly scores against transaction amounts using graphs for better analysis. The dashboard also shows current risk status and recent alerts to support real-time monitoring and decision-making.

CONCLUSION

This project demonstrates the effectiveness of unsupervised learning in detecting anomalies in financial transactions. By combining machine learning with full stack web development, the system provides accurate detection, clear visualization, and real-time insights. It serves as a practical and scalable solution for financial anomaly detection and risk analysis.

FUTURE SCOPE

Future enhancements may include real-time transaction streaming, integration with deep learning models, advanced visualization techniques, automated alerts, and deployment in cloud-based financial systems for large-scale monitoring.

REFERENCES

[1] Harini, D. P. (2013). Two Level Intrusion Detection For Detecting Intruders in Multitier Web Applications. *International Journal of Engineering & Science Research*, *3*, 472-478.

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

[3] F. T. Liu, K. M. Ting, and Z. H. Zhou, “Isolation Forest,” *IEEE International Conference on Data Mining (ICDM)*, pp. 413–422, 2008.

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

[5] S. Bhattacharyya, S. Jha, K. Thara Kunnel, and J. Westland, "Data mining for credit card fraud detection," *Decision Support Systems*, vol. 50, no. 3, pp. 602–613, 2011.

[6] A. Dal Pozzolo, O. Bontempi, and G. Stoick, "Adaptive machine learning for credit card fraud detection," *IEEE Symposium on Computational Intelligence*, 2015.

[7] M. Goldstein and S. Uchida, "A comparative evaluation of unsupervised anomaly detection algorithms," *PLoS ONE*, vol. 11, no. 4, 2016.

[8] A. Patcha and J. M. Park, "An overview of anomaly detection techniques," *Information Systems*, vol. 30, no. 4, pp. 223–249, 2007.

[9] N. Japkowicz and S. Stephen, "The class imbalance problem: A systematic study," *Intelligent Data Analysis*, vol. 6, no. 5, pp. 429–449, 2002.

[10] H. He and E. A. Garcia, "Learning from imbalanced data," *IEEE Transactions on Knowledge and Data Engineering*, vol. 21, no. 9, pp. 1263–1284, 2009.

[11] T. Fawcett, "An introduction to ROC analysis," *Pattern Recognition Letters*, vol. 27, no. 8, pp. 861–874, 2006.

[12] S. Axelsson, "The base-rate fallacy and the difficulty of intrusion detection," *ACM Transactions on Information and System Security*, vol. 3, no. 3, pp. 186–205, 2000.

[13] M. Carcillo, Y. Bontempi, and G. Snoeck, "Scarff: A scalable framework for streaming credit card fraud detection," *Information Fusion*, vol. 41, pp. 182–194, 2018.

[14] J. Stefanowski, "Handling data uncertainty and imprecision in machine learning," *International Journal of Applied Mathematics and Computer Science*, vol. 20, no. 1, pp. 181–190, 2010.

[15] T. Hastie, R. Tibshirani, and J. Friedman, *The Elements of Statistical Learning*, Springer, 2009.

[16] I. Goodfellow, Y. Bengio, and A. Courville, *Deep Learning*, MIT Press, 2016.

[17] M. Zanin, F. D. Valle, and S. Boccaletti, "Anomaly detection in financial time series," *Chaos, Solitons & Fractals*, vol. 45, no. 3, pp. 256–262, 2012.

[18] J. Quinlan, *C4.5: Programs for Machine Learning*, Morgan Kaufmann, 1993.

[19] A. Bahnsen, D. Aouada, and B. Ottersten, "Cost-sensitive decision trees for fraud detection," *Expert Systems with Applications*, vol. 39, no. 16, pp. 12264–12275, 2012.

[20] S. Hochreiter and J. Schmid Huber, "Long short-term memory," *Neural Computation*, vol. 9, no. 8, pp. 1735–1780, 1997.