iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** VI **Month of publication:** June 2026

DOI: https://doi.org/10.22214/ijraset.2026.79933

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue V May 2026- Available at www.ijraset.com

Fraud Detection: Anomaly Detection for Unusual Transactions

Karishma R
Velammal Engineering College, India

Abstract: ***The rapid expansion of digital financial transactions through online banking, e-commerce platforms, and mobile payment systems has significantly increased the risk of fraudulent activities, making detection a critical challenge due to the evolving nature of cyber threats and the rarity of fraudulent transactions. Traditional rule-based systems often struggle to identify new and unknown fraud patterns, leading to inefficiencies and high false-positive rates. This project presents an intelligent fraud detection system using anomaly detection techniques to identify unusual and suspicious transaction behavior by leveraging machine learning algorithms such as Isolation Forest, Autoencoders, and One-Class Support Vector Machines to model normal transaction patterns and detect deviations that may indicate fraud. By focusing on anomalies rather than relying solely on labeled data, the system can effectively identify previously unseen fraud attempts. The proposed model analyzes multiple transaction features, including transaction amount, time, frequency, and user behavior, to detect irregularities, while also supporting real-time analysis for immediate detection and response to suspicious activities. This approach improves detection accuracy while minimizing false alarms, and the system is designed to be scalable, efficient, and suitable for large financial datasets. Overall, this project demonstrates how artificial intelligence and anomaly detection can be used to build a robust, adaptive, and reliable fraud detection system that helps financial institutions reduce losses and enhance user trust.***
Keywords: Fraud Detection, Anomaly Detection, Machine Learning, Isolation Forest, Financial Security, Artificial Intelligence, Outlier Detection, Cybersecurity.

I. INTRODUCTION

The increasing reliance on digital financial transactions through online banking, e-commerce platforms, and mobile payment systems has made financial activities faster and more convenient, but it has also significantly increased the risk of fraudulent activities. Fraud detection has become a major challenge for financial institutions due to the constantly evolving nature of cyber threats and the difficulty in identifying rare and unpredictable fraudulent transactions. Traditional fraud detection methods, which are mainly rule-based, are limited in their ability to detect new and unknown fraud patterns and often result in high false-positive rates, affecting both operational efficiency and user experience. With the advancement of artificial intelligence and machine learning, more intelligent and adaptive approaches have emerged to address these challenges. In particular, anomaly detection has proven to be an effective technique for identifying unusual patterns in transaction data by learning normal behavior and detecting deviations that may indicate fraud. This project aims to develop a fraud detection system using anomaly detection techniques such as Isolation Forest, Autoencoders, and One-Class Support Vector Machines to analyze transaction data and identify suspicious activities. The system focuses on key transaction features such as amount, time, frequency, and user behavior, and is designed to support real-time detection, improving accuracy while reducing false alarms. By providing a scalable and efficient solution, this project enhances financial security and helps in building a reliable and adaptive fraud detection system.

II. FEATURES AND CITATION

The proposed fraud detection system using anomaly detection is based on several research studies that address the challenges of identifying fraudulent activities in large-scale financial systems. Research shows that detecting fraud is particularly difficult due to the highly imbalanced nature of transaction data, where fraudulent activities are rare and often hidden within normal behavior. This highlights the need for advanced techniques like anomaly detection that focus on identifying unusual patterns rather than relying solely on labeled datasets [1]. Machine learning algorithms such as Isolation Forest have been widely used for detecting outliers efficiently by isolating anomalies in large datasets, making them suitable for real-time fraud detection systems [2]. Similarly, deep learning approaches like Autoencoders have demonstrated strong performance in learning normal transaction behavior and identifying deviations through reconstruction errors [3]. One-Class Support Vector Machines further contribute by creating boundaries around normal data points and flagging anything outside as suspicious [4].

Behavioral analysis techniques, which consider factors such as transaction amount, frequency, location, and user activity patterns, have been shown to significantly improve detection accuracy while reducing false positives [5]. Additionally, real-time fraud detection systems using AI and data-driven models enhance financial security by providing instant alerts and adaptive learning capabilities [6]. These advancements collectively emphasize the growing importance of anomaly detection and artificial intelligence in building scalable, efficient, and reliable fraud detection systems.

III. RELATED WORKS

Several researchers have explored fraud detection using machine learning and anomaly detection techniques to address the limitations of traditional systems. Abidi et al. [7] provide a comprehensive review of fraud detection methods, highlighting the transition from rule-based systems to advanced machine learning approaches capable of handling large-scale and complex financial data. The study categorizes techniques into supervised, unsupervised, and hybrid models, emphasizing the importance of anomaly detection in identifying rare and unknown fraud patterns. Chaccour et al. [8] propose a real-time fraud detection framework using data-driven models that analyze transaction streams and detect suspicious activities instantly, demonstrating improved responsiveness and reduced financial risk. Rathnayake et al. [9] introduce a context-aware fraud detection approach that incorporates user behavior, transaction history, and environmental factors to improve detection accuracy, showing that combining contextual information significantly reduces false positives. Nair et al. [10] present a hybrid fraud detection system that integrates multiple machine learning algorithms, including decision trees and anomaly detection models, to enhance detection performance and adaptability across different datasets. Wold et al. [11] conduct a systematic review of fraud detection techniques, identifying anomaly detection as a key solution for handling imbalanced datasets where fraudulent transactions are minimal compared to normal ones. Plikynas et al. [12] propose a distributed fraud detection system that leverages cloud computing and data sharing to improve scalability and detection efficiency across financial platforms. Okolo et al. [13] develop an AI-based fraud detection model using deep learning techniques such as Autoencoders, achieving high accuracy in identifying abnormal transaction patterns through reconstruction errors. De Faria et al. [14] introduce a mobile-based fraud monitoring system that provides real-time alerts for suspicious transactions, improving user awareness and response time. Khan et al. [15] present a detailed survey of anomaly detection algorithms, comparing their effectiveness in fraud detection scenarios and highlighting Isolation Forest and One-Class Support Vector Machines as efficient techniques for large datasets. Jeamwatthanachai et al. [16] analyze user behavior patterns in financial systems and emphasize the importance of behavioral analytics in detecting fraud more accurately. Rituerto et al. [17] propose a lightweight fraud detection model using statistical and machine learning techniques that can operate without heavy infrastructure, making it suitable for practical deployment. Riehle et al. [18] develop a high-precision fraud detection system using advanced data analytics and pattern recognition, showing improved detection rates compared to traditional approaches. Chelladurai et al. [19] evaluate existing fraud detection systems and identify common challenges such as high false positives, lack of adaptability, and scalability issues, providing recommendations for improving real-world implementations. Overall, these studies highlight the growing importance of anomaly detection and artificial intelligence in developing robust, scalable, and efficient fraud detection systems capable of addressing modern financial security challenges.

Table.1. Summary Of Related Works

Reference No.	Merits	Demerits
[7]	Provides a clear classification of fraud detection techniques such as supervised, unsupervised, and hybrid models, helping re-searchers understand different approaches.	Being a review paper, it lacks practical implementation and experimental validation on real-world datasets.
[8]	Being a review paper, it lacks practical implementation and experimental validation on real-world datasets.	Requires high computational resources and may face scalability issues in large financial systems.

[9]	Incorporates user behavior and contextual data to improve fraud detection accuracy and reduce false positives.	Depends heavily on data quality and may struggle with incomplete or noisy datasets.
[10]	Combines multiple machine learning models to enhance detection performance and adaptability across datasets.	Increased model complexity leads to higher training time and difficulty in model interpretation.
[11]	Highlights the effectiveness of anomaly detection in handling imbalanced datasets where fraud cases are rare.	Limited real-time implementation and lacks detailed comparison with modern deep learning techniques.
[12]	Utilizes distributed and cloud-based systems to improve scalability and processing efficiency for fraud detection.	Raises concerns related to data privacy, security, and dependency on network infrastructure.
[13]	Uses deep learning models like Autoencoders to achieve high accuracy in detecting abnormal transaction patterns.	Requires large amounts of training data and high computational power for model training.
[14]	Provides real-time fraud alerts through mobile-based systems, improving user awareness and quick response.	Limited evaluation in large-scale environments and may generate false alarms in dynamic conditions.
[15]	Offers a comprehensive survey of anomaly detection algorithms and compares their effectiveness in fraud detection.	Does not provide implementation results and may overlook hybrid or emerging techniques.
[16]	Emphasizes the importance of behavioral analytics in detecting fraud more accurately.	Behavioral patterns may change over time, requiring continuous model updates and retraining.
[17]	Proposes a lightweight fraud detection model suitable for systems with limited resources.	May compromise accuracy compared to more complex and resource-intensive models.
[18]	Demonstrates high detection accuracy using advanced data analytics and pattern recognition techniques.	Requires complex infrastructure and may not be suitable for small-scale applications.
[19]	Identifies practical challenges such as false positives and scalability issues in existing fraud detection systems	Lacks detailed quantitative evaluation and does not propose a concrete implementation model.

IV. PROPOSED WORK

The proposed system presents an intelligent fraud detection framework based on anomaly detection techniques to identify suspicious financial transactions in large-scale datasets. The architecture integrates data preprocessing, anomaly detection algorithms, behavioral analysis, and real-time monitoring to ensure accurate and adaptive fraud detection. Unlike traditional rule-based systems that rely on predefined fraud patterns, the proposed model learns normal transaction behavior and detects deviations, making it effective against unknown and evolving fraud strategies. The system operates using a data-driven approach that combines statistical analysis with machine learning models such as Isolation Forest, Autoencoders, and One-Class Support Vector Machines.

The transaction dataset is represented as a feature space where each transaction is defined by attributes such as transaction amount, time, frequency, location, and user behavior. The fraud detection process consists of data preprocessing, anomaly scoring, model training, evaluation, and real-time detection.

1) *Data Preprocessing And Feature Engineering:* Raw transaction data is cleaned, normalized, and transformed into a structured format suitable for analysis. Missing values are handled, categorical variables are encoded, and numerical features are scaled. Feature engineering is applied to derive meaningful attributes such as transaction frequency, average spending behavior, and time-based patterns, which help improve detection accuracy.
2) *Anomaly Detection Using Isolation Forest:* The Isolation Forest algorithm is used to detect anomalies by isolating rare data points. It works by randomly selecting features and split values to construct decision trees. Transactions that require fewer splits to isolate are considered anomalies. Each transaction is assigned an anomaly score, and those exceeding a predefined threshold are flagged as potential fraud.
3) *Deep Learning With Autoencoders:* Autoencoders are used to learn compressed representations of normal transaction behavior. The model is trained to reconstruct input data, and reconstruction error is calculated for each transaction. Transactions with high reconstruction error indicate deviation from normal patterns and are classified as anomalies.
4) *One-Class Support Vector Machine (OC-SVM):* The One-Class SVM model is applied to define a boundary around normal transaction data. Transactions that fall outside this boundary are considered suspicious. This method is particularly useful when labeled fraud data is limited.
5) *Behavioral Analysis And Feature Evaluation:* The system incorporates user behavior analysis by evaluating patterns such as transaction frequency, spending habits, and time intervals. Sudden deviations from established behavior increase the anomaly score, improving the accuracy of fraud detection while reducing false positives.
6) *Hybrid Model And Decision Strategy:* To enhance robustness, the outputs of Isolation Forest, Autoencoder, and OC-SVM are combined using a weighted decision mechanism. Each model contributes to the final fraud score, and transactions are classified based on a combined threshold. This hybrid approach improves reliability and minimizes misclassification.
7) *Real-Time Fraud Detection And Alerts:* The system supports real-time transaction monitoring by analyzing incoming data streams and instantly detecting anomalies. Suspicious transactions trigger alerts for further verification, enabling quick response and preventing financial losses.

V. DYNAMIC MODEL ADAPTATION MECHANISM

When a suspicious transaction pattern is detected, the system dynamically adjusts its anomaly detection thresholds and model parameters to improve detection accuracy. Instead of relying on static rules, the anomaly score threshold is updated based on recent transaction trends and detected anomalies. The model can be retrained periodically using new transaction data, allowing it to adapt to evolving fraud patterns without rebuilding the entire system. This ensures continuous learning and improves the system's ability to detect newly emerging fraud techniques in real time.

VI. HYBRID MODEL FUSION STRATEGY

To enhance robustness and accuracy, multiple anomaly detection models are combined using a weighted fusion approach. The outputs from Isolation Forest (C_i), Autoencoder reconstruction error (C_a), and One-Class SVM (C_s) are integrated into a single fraud score:

Fraud Score = $w_1C\_i + w_2C\_a + w_3C\_s$

Subject to:

$w_1 + w_2 + w_3 = 1$

If the aggregated fraud score exceeds a predefined threshold (τ_f), the transaction is classified as fraudulent. This hybrid strategy reduces false positives and improves detection reliability by leveraging the strengths of multiple models.

VII. REAL-TIME PROCESSING AND OPTIMIZATION

The system is designed for real-time fraud detection using efficient and lightweight machine learning models. Techniques such as model optimization and data sampling are applied to reduce computational overhead and ensure fast processing. The workflow includes data collection, preprocessing, feature extraction, anomaly detection, score aggregation, and alert generation. This pipeline enables immediate identification of suspicious transactions, making the system suitable for deployment in real-world financial environments.

VIII. PERFORMANCE EVALUATION METRICS

The performance of the fraud detection system is evaluated using standard classification metrics:

- Accuracy = (TP + TN) / (TP + TN + FP + FN)
- Precision = TP / (TP + FP)
- Recall (Detection Rate) = TP / (TP + FN)
- F1-Score = 2 × (Precision × Recall) / (Precision + Recall)

Where:

TP = True Positives, TN = True Negatives, FP = False Positives, FN = False Negatives

A. Workflow

The proposed fraud detection system using anomaly detection follows a structured workflow to identify suspicious financial transactions efficiently and in real time. The process begins with collecting transaction data from various sources such as online banking systems, e-commerce platforms, and payment gateways. This raw data is then preprocessed by handling missing values, encoding categorical features, and normalizing numerical attributes to ensure consistency and accuracy. Once the data is prepared, feature engineering is applied to extract meaningful patterns such as transaction frequency, spending behavior, and time-based activity. The processed data is then passed into anomaly detection models such as Isolation Forest, Autoencoders, and One-Class Support Vector Machines, which learn the normal behavior of transactions and assign anomaly scores to detect deviations. As new transactions occur, the system continuously monitors and analyzes them in real time, comparing them against learned patterns. The decision engine evaluates the anomaly scores and determines whether a transaction is normal or potentially fraudulent based on a predefined threshold. If a suspicious transaction is detected, the system immediately triggers alerts or flags it for further verification. If the transaction is normal, it is processed without interruption. This continuous cycle of data collection, analysis, anomaly detection, and decision-making ensures accurate, scalable, and adaptive fraud detection, helping financial systems reduce risks and respond quickly to emerging threats.

B. Requirements

1) Development Environment: Python-based development environments such as Jupyter Notebook or Visual Studio Code are used to design, develop, and test the fraud detection system in an efficient and structured manner.
2) Machine Learning Framework: Libraries such as TensorFlow and Scikit-learn are used to build and train anomaly detection models, including Isolation Forest, Autoencoders, and One-Class Support Vector Machines.
3) Data Processing Library: Pandas and NumPy are used for data preprocessing, cleaning, transformation, and feature engineering to prepare transaction data for analysis.
4) Visualization Tools: Matplotlib and Seaborn are used to visualize transaction patterns, anomaly distributions, and model performance metrics for better understanding and evaluation.
5) Anomaly Detection Models: Machine learning algorithms such as Isolation Forest, Autoencoders, and One-Class SVM are implemented to identify unusual patterns and detect fraudulent transactions effectively.
6) Dataset Requirement: A structured transaction dataset containing features such as transaction amount, time, user behavior, and location is required to train and evaluate the fraud detection model.
7) Deployment Environment: The system can be deployed as a web application using frameworks like Flask or Streamlit, enabling real-time fraud detection and user interaction.
8) Hardware Requirements: A standard computer system with sufficient processing power and memory is required for model training and execution, while GPU support can be used for faster computation in deep learning models.

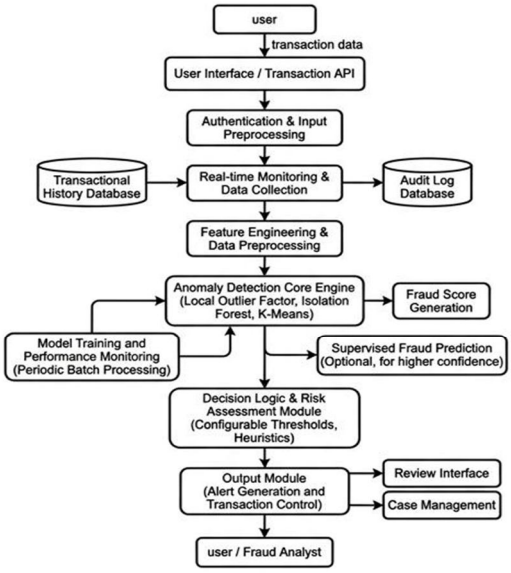


Figure 1. System Architecture for Fraud Detection using Anomaly-Based Techniques

The system architecture illustrates the workflow of fraud detection using anomaly detection techniques. The process starts when a user performs a transaction, which is captured through the interface and preprocessed for analysis. The system monitors transactions in real time and extracts important features such as amount, time, and user behavior. These features are analyzed by anomaly detection models like Isolation Forest and Autoencoders to identify unusual patterns. A fraud score is generated and evaluated by the decision module to classify transactions as normal or suspicious. If fraud is detected, alerts are generated and sent to the user or analyst for further action. as shown in Fig.1.

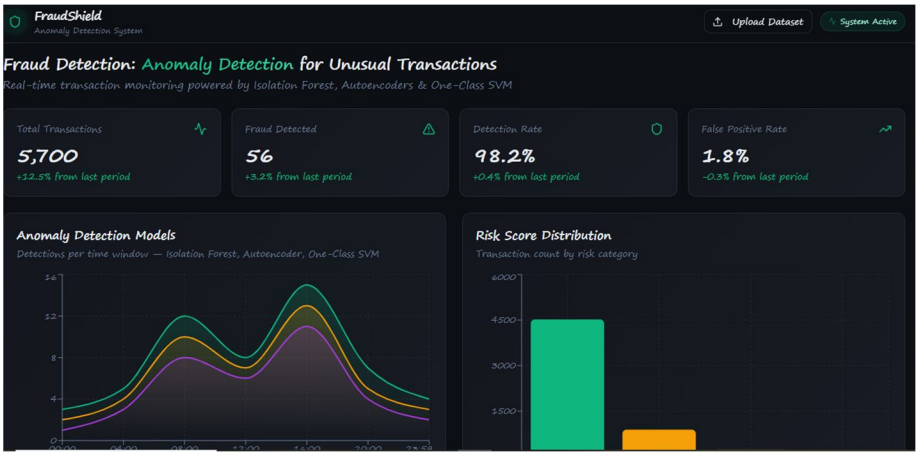


Figure 2. Fraud Detection Dashboard Interface

IX. RESULTS AND DISCUSSIONS

The Fraud Detection Dashboard provides a clear and real-time overview of transaction analysis using anomaly detection techniques. The interface displays key metrics such as total transactions, number of frauds detected, detection rate, and false positive rate, allowing users to quickly assess system performance. Visual graphs illustrate anomaly detection trends over time using models like Isolation Forest, Autoencoders, and One-Class SVM, helping in understanding unusual transaction patterns. The risk score distribution chart categorizes transactions based on their fraud probability, making it easier to identify high-risk activities. This user-friendly dashboard enables efficient monitoring, quick decision-making, and effective fraud management, as shown in Fig.2.

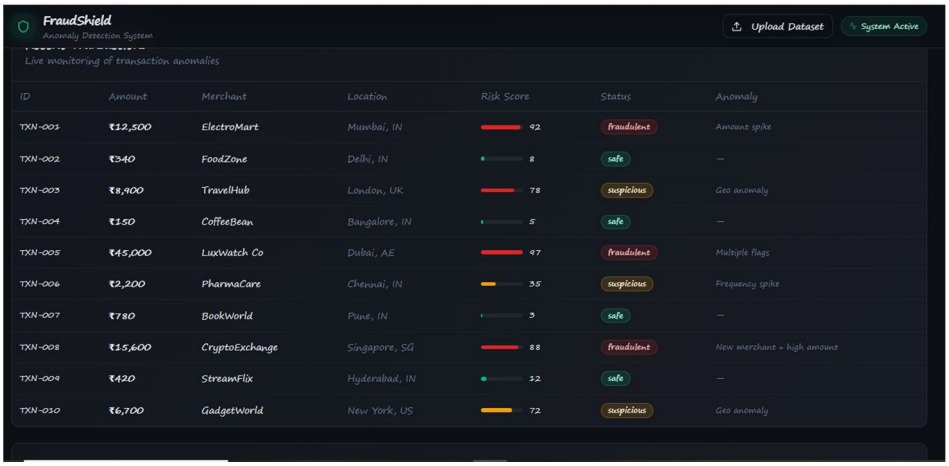


Figure 3.Transaction Monitoring Interface

The Transaction Monitoring Interface displays real-time analysis of financial transactions using anomaly detection techniques. The system continuously monitors transaction details such as amount, merchant, location, and risk score to identify suspicious activities. Each transaction is assigned a risk score based on anomaly detection models like Isolation Forest and Autoencoders, and is classified as safe, suspicious, or fraudulent. The interface also highlights the type of anomaly detected, such as unusual transaction amount, location mismatch, or frequency spikes. This allows users and analysts to quickly identify high-risk transactions and take immediate action. The clear and structured display improves decision-making and enhances the efficiency of fraud detection, as shown in Fig.3.

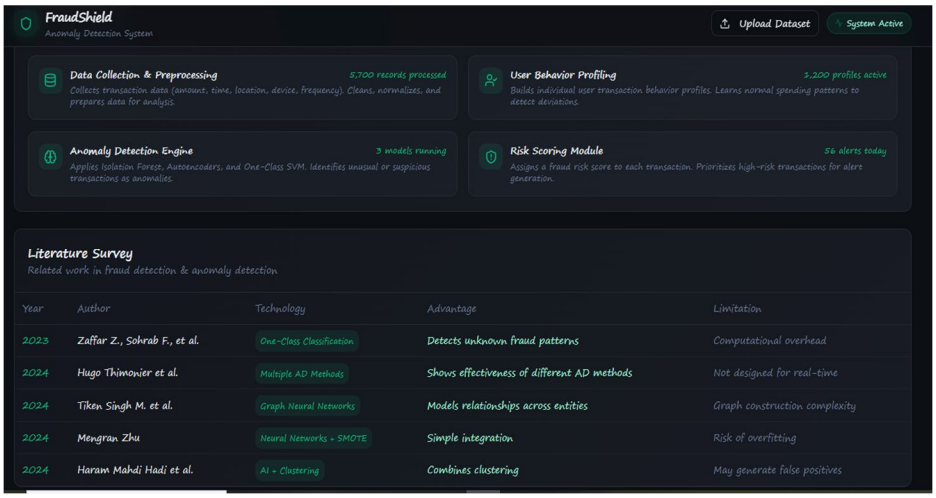


Figure 4. Fraud Detection Modules Interface

The Fraud Detection Modules Interface presents the core components of the anomaly-based fraud detection system in a structured manner. It highlights key modules such as data collection and preprocessing, user behavior profiling, anomaly detection engine, and risk scoring module. The system collects and processes transaction data, then analyzes user behavior patterns to understand normal activity. The anomaly detection engine applies models like Isolation Forest, Autoencoders, and One-Class SVM to identify unusual transactions. Based on this analysis, the risk scoring module assigns a fraud probability and generates alerts for high-risk transactions. This integrated approach improves detection accuracy, enables real-time monitoring, and enhances overall financial security, as shown in Fig.4.

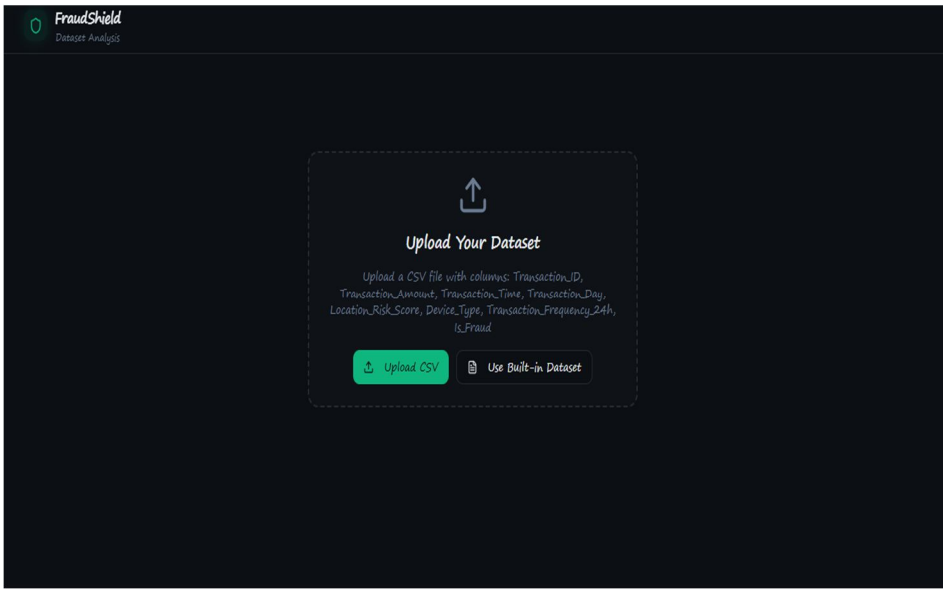


Figure 5. Dataset Upload and Analysis Interface

The Dataset Upload Interface allows users to input transaction data for fraud detection using anomaly detection techniques. The system supports uploading CSV files containing features such as transaction amount, time, location, device type, and transaction frequency. Users can either upload their own dataset or use a built-in dataset for analysis. Once the data is provided, the system processes and prepares it for anomaly detection models like Isolation Forest and Autoencoders. This interface ensures easy data handling and enables users to perform fraud analysis efficiently, as shown in Fig.5.

Figure 6. Fraud Analysis Results Interface

The Fraud Analysis Results Interface displays the final outcomes of transaction analysis performed using anomaly detection techniques. It provides a summary of total transactions, number of fraudulent and legitimate transactions, and the average fraud amount. Visual representations such as bar charts and pie charts help in understanding the distribution of fraud across different categories like device types and transaction types. The system clearly distinguishes between normal and suspicious activities, enabling quick interpretation of results. This interface helps users and analysts evaluate the effectiveness of the fraud detection model and supports informed decision-making, as shown in Fig.6.

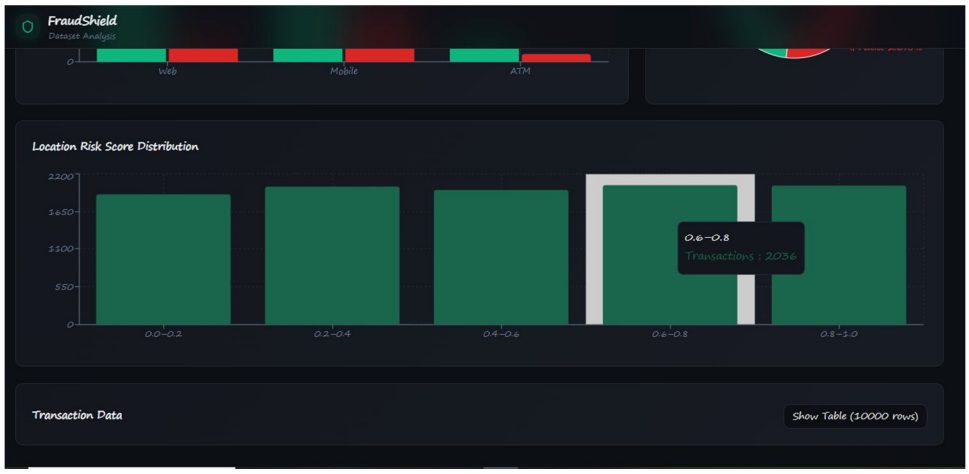


Figure 7.Risk Score Distribution Analysis Interface

The Risk Score Distribution Interface presents the analysis of transaction risk levels using anomaly detection techniques. It visualizes how transactions are distributed across different risk score ranges, helping to identify patterns of normal and suspicious activities. Higher risk score ranges indicate a greater likelihood of fraud, while lower ranges represent normal transactions. This graphical representation allows analysts to quickly understand the concentration of high-risk transactions and evaluate system performance. The interface enhances decision-making by clearly highlighting anomaly trends and supporting effective fraud detection, as shown in Fig.7.

A. Comparative Analysis

Comparative analysis of Isolation Forest against traditional rules[1]
Implementing Autoencoders for credit card fraud[5]
One-Class SVM performance in low-label scenarios[4]
Real-time user behavior analysis using risk scoring

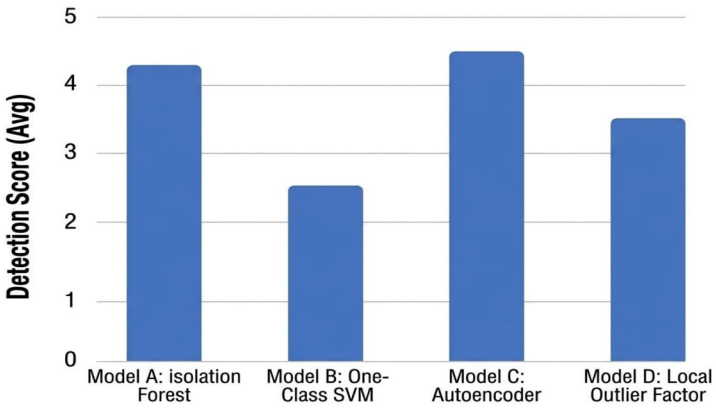


Figure 8. Comparative Analysis Based on Navigation Reliability Score

Fraud detection reliability refers to how accurately and consistently a system can identify fraudulent transactions while minimizing false positives. Traditional rule-based systems depend on fixed patterns and often fail to detect new or evolving fraud behaviors, while supervised machine learning models improve accuracy but require large labeled datasets and may struggle with unseen anomalies. Other approaches such as clustering and statistical techniques provide some flexibility but lack real-time adaptability and can produce higher false alarms. In contrast, the proposed system uses anomaly detection methods like Isolation Forest, Autoencoders, and One-Class SVM to detect unusual transaction patterns without relying heavily on labeled data. It continuously analyzes user behavior and identifies deviations in real time, improving detection accuracy and adaptability. The addition of a risk scoring mechanism further enhances decision-making by reducing false positives. As a result, the proposed system offers a more scalable, efficient, and reliable fraud detection solution compared to existing methods, as illustrated in Fig.8.

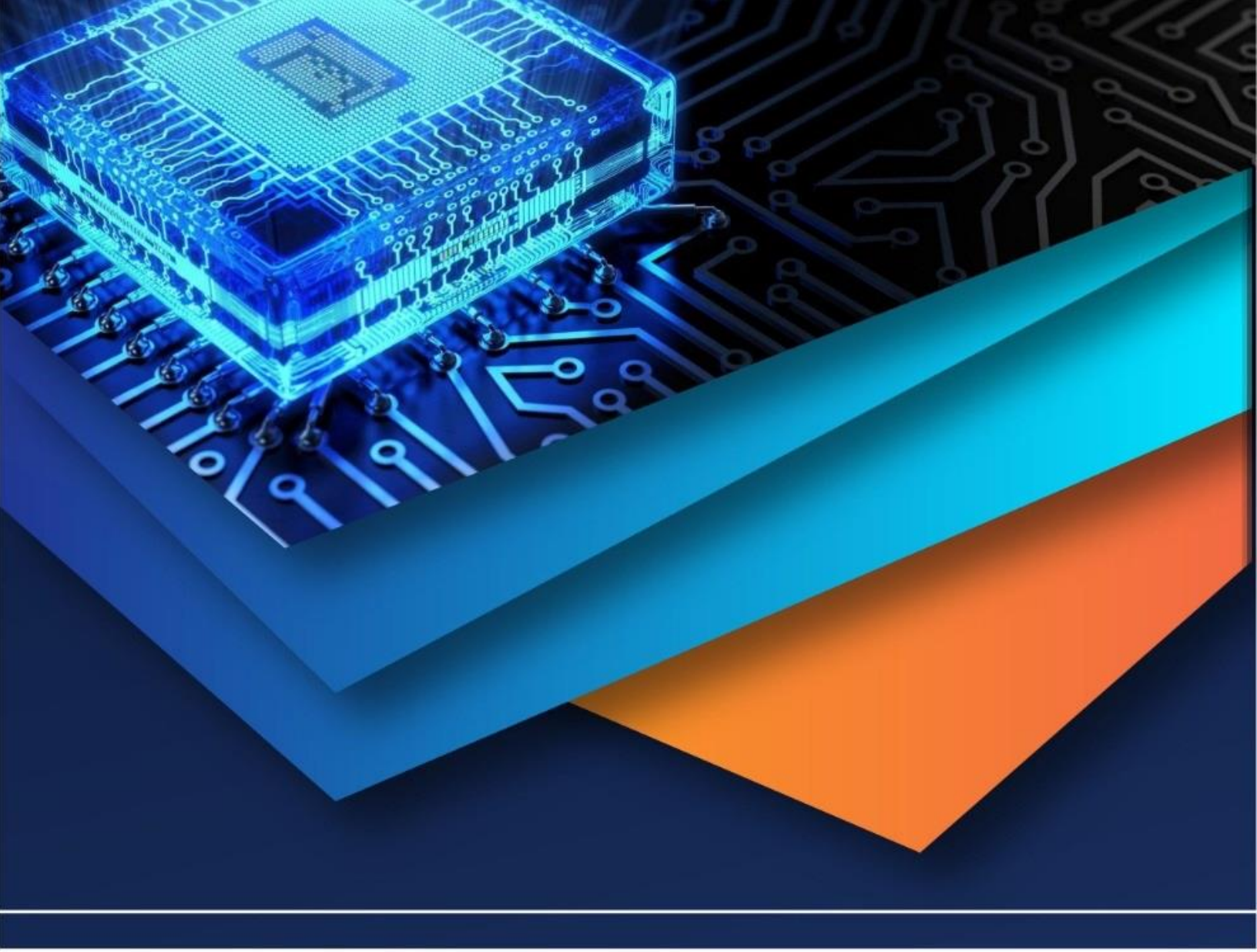
X. CONCLUSION AND FUTURE WORKS

This project presents an efficient fraud detection system using anomaly detection techniques to identify unusual and suspicious financial transactions. By leveraging machine learning models such as Isolation Forest, Autoencoders, and One-Class Support Vector Machines, the system learns normal transaction behavior and detects deviations without relying heavily on labeled data. The proposed approach supports real-time monitoring, improves detection accuracy, and reduces false positives, making it suitable for modern financial systems. Additionally, the system is scalable, cost-effective, and adaptable to large datasets, ensuring practical deployment in real-world environments. While the current model demonstrates strong performance, future enhancements can further improve its effectiveness by integrating advanced deep learning techniques, incorporating more detailed user behavior analytics, and improving model adaptability to evolving fraud patterns. The system can also be extended with real-time deployment in banking applications, enhanced visualization dashboards, and automated response mechanisms, ultimately contributing to more secure and intelligent financial transaction systems.

REFERENCES

[1] Varun Chandola, Arindam Banerjee, Vipin Kumar. "Anomaly Detection: A Survey." ACM Computing Surveys, vol. 41, no. 3, 2009, pp. 1–58.
[2] Markus M. Breunig, Hans-Peter Kriegel, Raymond T. Ng, Jörg Sander. "LOF: Identifying Density-Based Local Outliers." ACM SIGMOD, 2000.
[3] Fei Tony Liu, Kai Ming Ting, Zhi-Hua Zhou. "Isolation Forest." IEEE International Conference on Data Mining (ICDM), 2008.
[4] Jinghui Chen, Saket Sathe, Charu Aggarwal. "Outlier Detection with Autoencoder Ensembles." SIAM International Conference on Data Mining, 2017.
[5] Bernhard Schölkopf, John C. Platt, John Shawe-Taylor. "Estimating the Support of a High-Dimensional Distribution." Neural Computation, 2001.
[6] Dal Pozzolo Andrea, Olivier Caelen, Reid A. Johnson, Gianluca Bontempi. "Calibrating Probability with Undersampling for Unbalanced Classification." IEEE Symposium Series on Computational Intelligence, 2015.
[7] Phua Clifton, Vincent Lee, Kate Smith, Ross Gayler. "A Comprehensive Survey of Data Mining-based Fraud Detection Research." arXiv, 2010.
[8] Bhattacharyya Siddhartha, Sanjeev Jha, Kurian Tharakunnel, J. Christopher Westland. "Data Mining for Credit Card Fraud: A Comparative Study." Decision Support Systems, 2011.
[9] Carcillo Fabrizio, Dal Pozzolo Andrea, Le Borgne Yann-Aël. "Scarff: A Scalable Framework for Streaming Credit Card Fraud Detection." Information Fusion, 2019.

[10] Fiore Ugo, De Santis Alfredo, Perla Francesco. "Using Generative Adversarial Networks for Improving Classification Effectiveness in Credit Card Fraud Detection." Information Sciences, 2019.
[11] Chalapathy Raghavendra, Chawla Sanjay. "Deep Learning for Anomaly Detection: A Survey." arXiv, 2019.
[12] Ahmed Mohiuddin, Mahmood Abdun Naser. "A Survey of Network Anomaly Detection Techniques." Journal of Network and Computer Applications, 2016.
[13] Jurgovsky Johannes, Granitzer Michael. "Sequence Classification for Credit Card Fraud Detection." Expert Systems with Applications, 2018.
[14] Zheng Li, Yue Zhao. "PyOD: A Python Toolbox for Scalable Outlier Detection." Journal of Machine Learning Research, 2019.
[15] Ngai Eric W.T., Hu Yong, Wong Y.H. "The Application of Data Mining Techniques in Financial Fraud Detection: A Classification Framework." Decision Support Systems, 2011.
[16] Bolton Richard J., Hand David J. "Statistical Fraud Detection: A Review." Statistical Science, 2002.
[17] Bahnsen Alejandro Correa, Stojanovic Aleksandar. "Cost Sensitive Credit Card Fraud Detection Using Bayes Minimum Risk." IEEE International Conference on Data Mining, 2013.
[18] Whitrow Christopher, Hand David J. "Transaction Aggregation as a Strategy for Credit Card Fraud Detection." Data Mining and Knowledge Discovery, 2009.
[19] Randhawa Karan, Loo Khin Wee. "Credit Card Fraud Detection Using AdaBoost and Majority Voting." IEEE Access, 2018.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY