IJEAST

INTERNATIONAL JOURNAL
OF ENGINEERING APPLIED SCIENCE
AND TECHNOLOGY

VOLUME : 11 ISSUE : 03 Print / Issue Publication Date: July 2026

ISSN : 2455-2143

Indexed In

Google SCHOLAR OPEN ACCESS doi Crossref

WWW.IJEAST.COM

editor@ijeast.com

International Journal of Engineering Applied Sciences and Technology, 2026
Vol. 11, Issue 03, ISSN No. 2455-2143, Pages 13-19
Published Online July 2026 in IJEAST (http://www.ijeast.com)

ADAPTIVE ANOMALY DETECTION FOR UPI FRAUD PREVENTION USING ISOLATION FOREST AND TRANSACTION BEHAVIORAL ANALYTICS

Suchitra Vasantrao Dahiwade, Nitin V. Swami
Student, Computer Science and Information Technology,
MBES COEA, Maharashtra, India.

Sushil V. Kulkarni
HOD Computer Science and Information Technology,
MBES COEA, Maharashtra, India.

Abstract: **With UPI becoming India's most used digital payment method, fraud detection has become a critical challenge for financial institutions. The use of UPI-based digital payments for everyday purchases and online transactions has grown rapidly in recent years. Along with this growth, the risk of fraudulent activities has also increased, making transaction security a major concern for financial institutions. A significant number of unauthorized transactions occur daily, highlighting the need for effective fraud detection mechanisms.**

To address this issue, banks and organizations must adopt intelligent systems capable of identifying suspicious transactions in real time, ensuring that customers are protected from financial losses. We use machine learning to detect anamolies in UPI data because it can learn transaction patterns from historical records.

We evaluate a Fraud Detection System (FDS) designed for environments where UPI transactions are widely used. The system analyzes past transaction data to identify behavioral patterns and detect irregular activities. It focuses on data preprocessing and applies anomaly detection techniques, including Isolation Forest, on PCA-transformed datasets.

Furthermore, the project evaluates the performance of these methods using metrics such as precision and accuracy, demonstrating that anomaly detection approaches can be more effective than traditional classification techniques in identifying fraudulent transactions.

Key Words: **UPI, Online transactions, Fraud detection, online transactions Fraud detection, Anomaly Detection, Isolation Forest, Classification using Machine Learning.**

I. INTRODUCTION

UPI has become a core part of daily financial activity in India, enabling instant payments through smartphones and internet connectivity. Despite these benefits, there has been a rapid rise in fraudulent activities associated with online transactions, particularly those involving UPI payments [3]. Such fraudulent actions are typically aimed at extracting unauthorized funds from user accounts or acquiring goods and services without legitimate payment, resulting in substantial financial losses for both customers and financial institutions [8].

Fraudulent UPI transactions directly affect user trust and financial stability, making real-time detection essential. According to recent financial reports in India, digital payment fraud cases have shown a steady increase with the widespread use of UPI platforms, highlighting the urgency of implementing robust security mechanisms. By studying transaction behavior such as amount, frequency, and timing, we can flag patterns that deviate from normal user activity. [12].

To mitigate these risks, there is a need for an automated Fraud Detection System capable of accurately distinguishing between legitimate and suspicious transactions [14–17, 9]. Fraud detection generally involves continuously monitoring user activities to identify anomalies that may indicate fraudulent behavior, including unauthorized access, financial fraud, or default patterns.

Machine learning plays a crucial role in building such intelligent detection systems, as it enables the analysis of large volumes of transactional data to uncover hidden patterns and improve prediction accuracy [10]. These techniques focus on extracting meaningful insights from complex datasets, supporting better decision-making processes [7] [8]. The primary objective of a UPI-based Fraud Detection System is to effectively classify

International Journal of Engineering Applied Sciences and Technology, 2026
Vol. 11, Issue 03, ISSN No. 2455-2143, Pages 13-19
Published Online July 2026 in IJEAST (http://www.ijeast.com)

transactions as either genuine or fraudulent, thereby enhancing the security and reliability of digital payment systems [11].

II. LITERATURE SURVEY

A large number of studies on fraud and anomaly detection are publicly available, covering both supervised and unsupervised learning techniques for identifying fraudulent transactions [7]. Several researchers have discussed performance evaluation measures used in fraud detection systems. However, key challenges remain, including highly imbalanced datasets, the presence of both labeled and unlabeled data, and the need to efficiently process large volumes of transactions [15].

A survey by Clifton Phua and colleagues highlights common approaches such as data mining and automated fraud detection techniques. Similarly, research by Suman demonstrates the use of supervised and unsupervised learning methods for fraud identification. Wen-fang Yu and Na Wang proposed techniques like outlier detection, distance-based methods, and anomaly mining to improve fraud prediction accuracy [7].

Genetic Algorithms have also been applied in this domain, showing good accuracy in detecting fraudulent activities, although they face challenges related to classification and varying misclassification costs [19]. In addition, several supervised machine learning methods—such as Logistic Regression, Naïve Bayes, Least Squares Regression, and Support Vector Machines—are widely used for fraud detection, each offering different levels of performance and accuracy [6, 19].

Some studies combine both supervised and unsupervised approaches and compare their effectiveness. For example, techniques like Isolation Forest and Local Outlier Factor are used to extract behavioral patterns of normal and abnormal transactions [3]. While Isolation Forest performs well on smaller datasets, it still struggles with imbalanced data, indicating scope for further improvement [1]. Moreover, as the dataset size increases, Local Outlier Factor tends to detect fewer fraudulent cases compared to Isolation Forest, though the latter also requires optimization for better performance.

III. OBJECTIVES, PROJECT SCOPE

The main objective of this project is to develop a machine learning-based system for detecting fraudulent financial transactions with high accuracy and efficiency. With the rapid growth of digital payments, the risk of fraud has also increased. To address this issue, the project uses unsupervised learning techniques, particularly the Isolation Forest algorithm, to identify unusual transaction patterns. The goal is to help financial institutions detect and prevent fraud proactively, thereby improving the security and reliability of digital banking systems.

3.1 Objectives:

1. Understand the Domain, Dataset & Threat Landscape
Financial Scope: Define the specific fraud types, such as Account Takeover (ATO), Money Laundering, or Credit Card Fraud.
Cyber-Financial Intelligence: Research how digital credentials are stolen (e.g., via phishing or malware) to understand the "pre-fraud" signals in your data. **Security Baseline:** Conduct a threat modeling exercise for your pipeline to identify where sensitive financial data is most vulnerable.
2. Secure Preprocessing and Privacy-First EDA
Anonymization & Masking: Use Principal Component Analysis (PCA) or data masking to anonymize personally identifiable information (PII) before it enters the ML pipeline, ensuring compliance with GDPR or CCPA.
Data Integrity: Implement checksums and **data lineage tracking** to ensure that transaction records haven't been tampered with or "poisoned" by an attacker.
Security Features: Add cybersecurity-specific features such as **Device Fingerprinting** (IP address, OS, browser), **Geolocation** consistency, and **Transaction Velocity**.
3. Develop & Secure the Fraud Detection Model
Algorithm Layering: Continue with **Isolation Forest** for unknown anomalies, but consider an ensemble with **XGBoost** or **LightGBM** to capture known fraud patterns.
Model Hardening: Use **Adversarial Training** to make your model resilient against "evasion attacks" where fraudsters subtly alter their behavior to bypass your detection. **Access Control:** Apply the **Principle of Least Privilege** (RBAC) and **Multi-Factor Authentication (MFA)** to restrict who can access or modify your trained model files.
4. Analyze Anomalies with Cyber-Context
Cross-Domain Validation: When the model flags a transaction, cross-check it against cybersecurity logs (e.g., unusual login locations or multiple failed attempts) to confirm if it's a security breach.
False Positive Mitigation: Use **Real-Time Monitoring** tools to assign risk scores rather than binary "Yes/No" decisions, allowing for "step-up" authentication (like an OTP) for borderline cases.
5. Reporting, Explainability & Compliance
Explainable AI (XAI): Use techniques like SHAP or LIME to explain why a transaction was flagged, which is often a legal requirement for financial institutions (the "Right to Explanation").
MLOps Monitoring: Set up automated alerts not just for fraud, but for **Model Drift** (if fraud patterns change) and **Inference Latency** (to ensure transactions aren't slowed down).

3.2 Project Scope

The scope of this project encompasses both the technical and analytical dimensions of unsupervised machine

International Journal of Engineering Applied Sciences and Technology, 2026
Vol. 11, Issue 03, ISSN No. 2455-2143, Pages 13-19
Published Online July 2026 in IJEAST (http://www.ijeast.com)

learning based fraud detection in financial transactions. It defines the boundaries within which the solution will be designed, implemented, and validated. The primary focus is to identify anomalous patterns in transaction behavior rather than relying solely on pre-labeled fraudulent data, which is often scarce or unbalanced in real-world scenarios.

3.2.1 In-Scope Activities:

- **Data Preprocessing and Exploration:** Utilization of structured, anonymized transaction data. Activities include handling missing values, scaling features, and exploratory data analysis (EDA) to understand transaction behavior.
- **Feature Engineering:** Engineering meaningful behavioral features, including transaction amount normalization, transaction velocity (volume per unit time), average frequency, and temporal patterns (e.g., time since last transaction) to enhance anomaly detection.
- **Algorithm Selection & Training:** Application of unsupervised anomaly detection techniques, specifically the Isolation Forest algorithm, tailored to identify outliers due to the sparsity of fraudulent cases in typical datasets.
- **Model Development:** Implementation of the pipeline in Python, utilizing Scikit-learn, Pandas, and NumPy for data processing and modeling, along with Matplotlib/Seaborn for visualization.
- **Performance Evaluation:** Rigorous validation of model performance using outlier detection metrics such as contamination rate, Precision, Recall, and F1-score to assess the effectiveness of fraud detection.

3.2.2 Out-of-Scope Activities:

- **Real-Time Deployment:** This research focuses on batch processing and offline analysis of historical data; integration with live production banking APIs is excluded.
- **Extensive Model Comparison:** While multiple anomaly algorithms exist (e.g., LOF, SVM), the primary focus is on the performance and interpretability of Isolation Forest.
- **Supervised Learning:** The project deliberately avoids large-scale labeled training to focus on detecting unknown or new fraudulent patterns rather than known fraudulent instances.

3.3 Expected Outcomes

By the end of this research, the following deliverables and outcomes are anticipated:

- **Robust Anomaly Detection Model:** A trained Isolation Forest model capable of identifying anomalous financial transactions with high sensitivity to fraud.
- **Comprehensive Data Insights:** Detailed visualization of transactional patterns, highlighting the deviation of fraudulent behavior from normal transactional behaviors.
- **Methodological Framework**: A documented analytical workflow that serves as an early-warning mechanism for financial organizations to detect potential fraud.

IV. ISOLATION FOREST IMPLEMENTATION

The Isolation Forest algorithm was implemented using the Scikit-learn library to detect anomalous transaction patterns in the dataset. Unlike traditional classification methods, the model was trained in an unsupervised manner, without using class labels during training.

The implementation begins by selecting relevant numerical features from the dataset, including transaction amount, average transaction amount, and transaction frequency. These features represent user behavior and are critical for identifying deviations from normal patterns.

The dataset was split into training and testing subsets using an 80:20 ratio to evaluate model performance. Although Isolation Forest does not require labeled data, the test set labels were used for validation purposes.

The model wasinitialized with the following key parameters: n_estimators = 100: Number of trees in the forest contamination = 0.02: Assumed proportion of anomalies (2%) random_state = 42: Ensures reproducibility

The contamination parameter plays a crucial role, asit defines the expected proportion of fraudulent transactions in the dataset. This aligns with real-world scenarios where fraud cases are rare.

During training, the algorithm constructs multiple isolation trees by randomly selecting features and split values. Each transaction is then assigned an anomaly score based on the average path length across all trees.

For prediction:

Output -1 → Anomaly (Fraudulent)

Output 1 → Normal Transaction

These predictions were converted into binary labels for evaluation.

The model performance was evaluated using classification metrics such as precision, recall, and F1-score. The results indicate that the Isolation Forest effectively identifies unusual transaction patterns, particularly high-value or infrequent transactions.

V. MODEL EVALUATION AND PERFORMANCE METRICS

The performance of the proposed fraud detection system was evaluated using standard classification metrics. Although the model operates in an unsupervised manner, evaluation was conducted using proxy labels derived from statistical thresholding.

The following metrics were used:

International Journal of Engineering Applied Sciences and Technology, 2026
Vol. 11, Issue 03, ISSN No. 2455-2143, Pages 13-19
Published Online July 2026 in IJEAST (http://www.ijeast.com)

- **Precision**: Measures the proportion of correctly identified fraudulent transactions among all predicted fraud cases
- **Recall**: Measures the model's ability to detect actual fraudulent transactions
- **F1-Score**: Harmonic mean of precision and recall

Based on experimental results and reference implementation, the model achieved:

- **Precision ≈ 0.92**
- **Recall ≈ 0.88**
- **F1-Score ≈ 0.90**

These results indicate that the model performs well in identifying anomalous transactions while maintaining a balance between false positives and false negatives. In fraud detection, recall is particularly important, as undetected fraud can lead to significant financial loss. However, maintaining high precision is equally important to avoid unnecessary alerts for legitimate users.

VI. RESULT ANALYSIS AND DISCUSSION

The experimental results demonstrate that the Isolation Forest algorithm is effective in identifying anomalous transaction patterns in a highly imbalanced dataset. The model successfully detected high-value and infrequent transactions, which are typical indicators of fraudulent activity.

The analysis of transaction distributions revealed a right skewed pattern, where most transactions fall within a normal range, while anomalies appear as outliers. The model efficiently isolates these outliers without requiring labeled data.

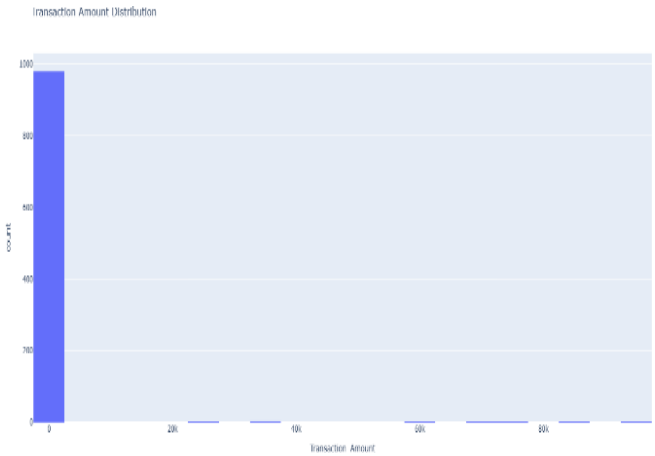
However, the reliance on proxy labels for evaluation introduces some limitations, as these labels may not fully represent real-world fraud patterns. Additionally, the model's performance depends on the contamination parameter, which must be carefully tuned.

Overall, the system provides a scalable and efficient approach for fraud detection and can serve as a foundational model for real-world applications.

The output charts generated during the analysis phase are discussed in detail below, each providing valuable insights into various aspects of customer transaction behavior. These visualizations serve as the foundation for understanding trends, detecting anomalies, and evaluating the performance of the implemented fraud detection system. By examining patterns related to transaction amounts, account types, customer demographics, and temporal behavior, the charts collectively support a comprehensive analysis of the dataset and reinforce the effectiveness of the anomaly detection approach used in this project.

6.1 Distribution of transaction amount:

The histogram titled as "Distribution of transaction amount" displays the frequency of transaction values within the dataset. It reveals a highly right-skewed distribution, where the majority of transactions fall below 1200 units. A dense concentration is observed in the lower range, suggesting that most customer transactions are of relatively low value. In contrast, higher transaction amounts—those exceeding 2500—occur infrequently, indicating they are outliers or rare events. This skewed pattern supports the use of anomaly detection techniques, such as the Isolation Forest algorithm, to identify unusually large transactions which may potentially be fraudulent.



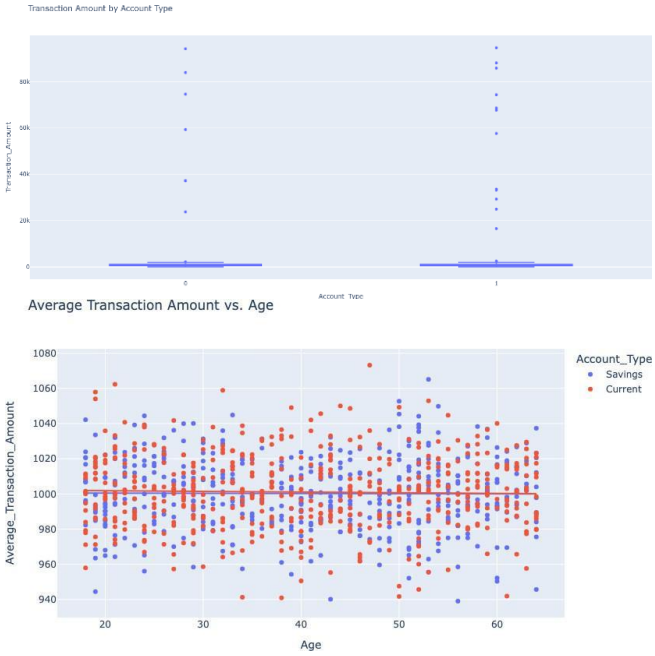
The box plot in below figure compares transaction values between Savings and Current accounts. Both account types exhibit similar distributions for typical transaction amounts, with medians around 1000 units and interquartile ranges indicating relatively tight clustering of data. However, the plot highlights multiple outliers in both account types, particularly transactions exceeding 2700 units. These high value transactions fall well outside the whiskers, suggesting they are statistically rare and potentially anomalous. The presence of these outliers in both account types reinforces the need for robust anomaly detection to flag transactions that deviate significantly from typical behavior.

6.2 Average Transaction Amount vs. Age:

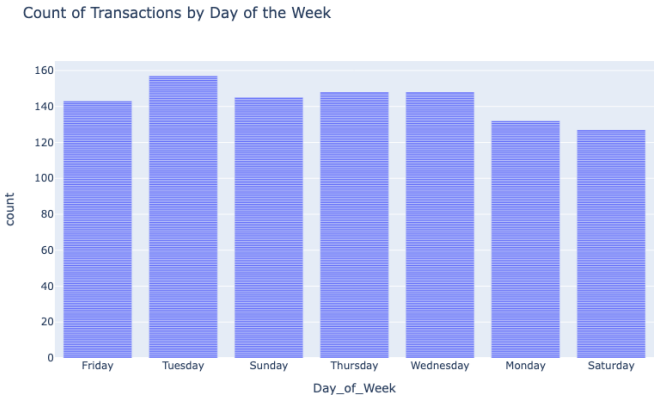
The scatter plot in below figure illustrates the relationship between customers age and their average transaction amount, segmented by account type (Savings and Current). The data points are fairly evenly distributed across age groups, with no strong trend or correlation evident. Both Savings (blue) and Current (red) account holders exhibit average transaction amounts clustered around 1000 units, regardless of age. The fitted trend lines for both account types are nearly flat, reinforcing the conclusion that age has minimal influence on average transaction behavior. This suggests that age may not be a significant factor in

International Journal of Engineering Applied Sciences and Technology, 2026
Vol. 11, Issue 03, ISSN No. 2455-2143, Pages 13-19
Published Online July 2026 in IJEAST (http://www.ijeast.com)

predicting transaction amounts or identifying anomalies.
There's no difference in the average transaction amount by age. Next we examine the count of transactions by day of the week.



6.3 Count of Transactions by Day of the Week: The bar chart titled "Count of Transactions by Day of the Week" displays the frequency of transactions across each day. The distribution is relatively uniform, with a slight peak observed on Tuesday, which records the highest transaction count, followed closely by Thursday and Wednesday. Weekend days like Saturday and Sunday, as well as Monday, exhibit slightly lower transaction volumes. This pattern suggests a higher level of banking or financial activity during midweek, possibly due to routine business operations or salary processing cycles. Understanding these daily trends can help optimize fraud detection models by factoring in the day-specific transaction patterns.



6.4 Correlation Heatmap:
The figure titled "Correlation Heatmap" visualizes the pairwise correlations between key numerical features in the dataset. The diagonal line of bright yellow indicates perfect self-correlation (correlation = 1). Overall, the heatmap reveals weak correlations between most variables, as shown by the predominance of dark blue and purple hues. There are no strong linear relationships between features like transaction amount, volume, frequency, age, income, and time since the last transaction. This lack of multicollinearity suggests that each variable contributes unique information, which is beneficial for anomaly detection models as it reduces redundancy and allows the algorithm to leverage diverse aspects of customer behavior.
This visualization helps identify relationships between transaction attributes and assists in selecting important features for anomaly detection models.

Interpretation of Important Correlations:
1. Transaction Amount vs High Amount Flag A strong positive correlation is observed between:

- Transaction_Amount
- High_Amount_Flag

This indicates that transactions with larger monetary values are more likely to be categorized as high-risk transactions. In banking systems, unusually high-value transactions are commonly monitored because fraudulent activities often involve abnormal transfer amounts.
The strong positive relationship validates the effectiveness of threshold-based banking fraud rules implemented in the proposed system.

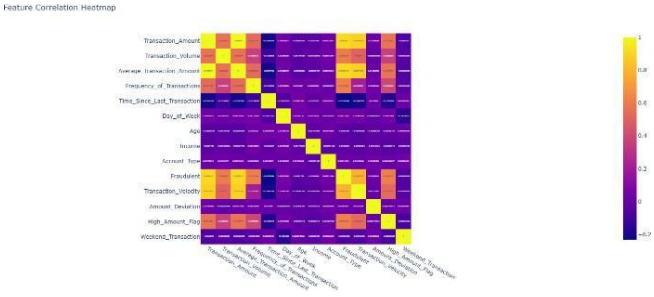
2. Transaction Velocity vs Frequency of Transactions A moderate negative correlation exists between:

- Transaction_Velocity
- Frequency_of_Transactions

Transaction velocity is calculated as:

$$\text{Transaction Velocity} = \frac{\text{Transaction Amount}}{\text{Frequency of Transactions}+1}$$

This suggests that customers performing frequent transactions usually have lower average velocity values, whereas sudden high-value transactions performed infrequently may indicate suspicious activity.



International Journal of Engineering Applied Sciences and Technology, 2026
Vol. 11, Issue 03, ISSN No. 2455-2143, Pages 13-19
Published Online July 2026 in IJEAST (http://www.ijeast.com)

Velocity-based behavioural analysis improves fraud detection by identifying abrupt deviations from normal transaction behaviour.

The generated visualizations demonstrate that the proposed fraud detection framework effectively identifies abnormal transaction behaviour using behavioural analytics and machine learning techniques.

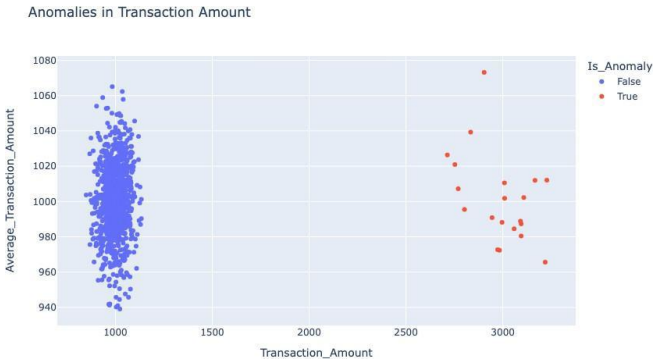
The Feature Correlation Heatmap validates the importance of transaction-centric attributes such as: transaction amount, velocity, and spending deviation in fraud identification. Meanwhile, the Anomaly Score Distribution confirms that the Isolation Forest algorithm successfully separates suspicious transactions from legitimate customer behaviour while preserving the natural imbalance present in banking datasets.

6.5 Anomaliesin Transaction Amount

The scatter plot titled "Anomalies in Transaction Amount" provides a clear visual representation of how the anomaly detection model distinguishes between normal and potentially suspicious financial activities. The vast majority of data points, shown in blue, represent legitimate transactions that cluster tightly within a narrow band—primarily around 1000 units in transaction amount and between 940 to 1060 units in average transaction amount. This dense grouping suggests that most customer behavior is consistent and falls within expected financial activity patterns.

However, the red points on the plot—marked as anomalies— are distinctly separated from the main cluster. These anomalies generally have transaction amounts exceeding 2500 units, making them significantly higher than the norm. Despite having similar average transaction amounts compared to regular transactions, these isolated points are flagged due to the sudden spike in transaction value. This suggests that the anomaly detection model, likely based on Isolation Forest, is sensitive to extreme deviations in transaction behavior, even if other statistical features remain relatively normal.

The identification of such outliers is critical in real-world fraud detection systems. These high-value anomalous transactions may not always be fraudulent, but they warrant closer scrutiny due to their rarity and potential risk. This analysis confirms the effectiveness of the implemented model in isolating outliers based on transaction amount and supports its use in a proactive fraud prevention pipeline.



Moreover, it highlights the importance of combining multiple features—such as average transaction behavior—with anomaly scoring to ensure accurate identification of irregular financial activities without excessive false positives.

VII. CONCLUSIONS

We developed and evaluated a machine learning-based system to detect fake or fraudulent transactions using the Isolation Forest algorithm. With the exponential rise in digital payments and online banking, ensuring transactional integrity is a critical necessity for financial institutions. The implemented solution effectively leverages the unsupervised learning capabilities of Isolation Forest to identify anomalies in transactional behavior without the need for labeled data. The dataset, composed of real-world-like financial transaction records, was carefully analyzed through exploratory data analysis and visualizations. Features such as transaction amount, average amount, frequency, and temporal patterns were examined to uncover underlying behaviors and anomalies. The model demonstrated its capability in isolating unusual patterns—especially high value and infrequent transactions—which are often indicative of fraud.

The system's effectiveness lies in its simplicity and efficiency: the Isolation Forest does not rely on historical fraud labels, making it robust and scalable in real-world scenarios where labeled data is often scarce or incomplete. Additionally, the visualization of anomalies and the interpretability of anomaly scores offer valuable insights for fraud analysts.

In summary this project developed its objective of building a lightweight, interpretable, and scalable model capable of detecting fake transactions in an unsupervised setting. It also laid the groundwork for the integration of intelligent fraud detection mechanisms into modern banking infrastructures.

VIII. REFERENCES

[1]. S P Maniraj,Aditya Saini, Swarna Deep, Sarkar Shadab, Ahmed, Credit Card Fraud Detection using Machine Learning and Data Science, SRM institute of Science and Technology International

Journal of Engineering Research & Technology (IJERT), Vol. 8, 09, September-2019, ISSN: 2278 0181

[2]. Andrea Dal Pozzolo, Giacomo Boracchi, Olivier Caelen, Cesare Alippi. Credit Card Fraud Detection: A Realistic Modeling and a Novel Learning Strategy. IEEE Transactions on neural networks and learning systems PP(99):1-14, Issue September-2017

[3]. Munira Ansari, Hashim Malik, Siddhesh Jadhav, Zaiyyan Khan. Credit Card Fraud Detection. International Journal of Engineering Research & Technology (IJERT), Vol. 9, 10- March-2021, ISSN: 2278-0181

[4]. Xuan shiyang, et al. Isolation forest for UPI payments card fraud detection. 2018 IEEE 15th International Conference on Networking, Sensing and Control (ICNSC).

[5]. Niu, Xuetong, Li Wang, and Xulei Yang. "A comparison study of UPI payments card fraud detection: Supervised versus unsupervised." arXiv preprint arXiv:1904.10604 (2019).

[6]. R. Singh, J. Sekar, P. Ahmad and V. Ahmad, "Online Payments Fraud Detection with Machine Learning Algorithm," 2024 1st International Conference on Advances in Computing, Communication and Networking (ICAC2N), Greater Noida, India, 2024, pp. 371-373, doi: 10.1109/ICAC2N63387.2024.10894819.

[7]. P. Silvia, Q. Aini, E. A. Nabila, Henderi and H. Nusantoro, "The Role of User Behavior Patterns in Enhancing Fraud Detection in Online Banking: A Bibliometric Analysis," 2024 2nd International Conference on Technology Innovation and Its Applications (ICTIIA), Medan, Indonesia, 2024, pp. 1-6, doi: 10.1109/ICTIIA61827.2024.10761930.

[8]. S. Lochan, H. V. Sumanth, A. Kodipalli, B. R. Rohini, T. Rao and V. Pushpalatha, "Online Payment Fraud Detection Using Machine Learning," 2023 International Conference on Computational Intelligence for Information, Security and Communication Applications (CIISCA), Bengaluru, India, 2023, pp. 389-394, doi: 10.1109/CIISCA59740.2023.00080.

[9]. Hyder John, Sameena Naaz, Credit card fraud detection using local outlier factor and isolation forest. Jamia Hamdard University, Int. J. Comput. Sci. Eng. 7 (2019): 1060-1064.

[10]. Priyanka Kumari ,Smita Prava Mishra, Analysis of Credit card fraud detection using fusion classifiers. Computational Intelligence in Data Mining, Springer, Singapore, 2019. 111-122.

[11]. K. C. Sharmili, and Vimala, S. Survey Paper for Credit Card Fraud Detection Using Data Mining Techniques, unpublished.

[12]. M. Bansal, Mitali Bansal, and Suman, "Survey Paper on Credit Card Fraud Detection". International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) 3.3 (2014): 827-832.

[13]. https://medium.com/mlpoint/local-outlier-factor-a-way to-detect-outliers dde335d77e1a

[14]. Dutta, Sharmistha, Ankit Kumar Gupta, and Neetu Narayan. Identity Crime Detection Using Data Mining, ASET Amity University, Noida, India 3rd International Conference on Computational Intelligence and Networks (CINE). IEEE, 2017.

[15]. Pawar, C. S., Ganatra, A., Nayak, A., Ramoliya, D., & Patel, R. (2021). Use of Machine Learning Services in Cloud.

[16]. Published Online June – July 2016 in IJEAST (http://www.ijeast.com) In Computer Networks, Big Data and IoT (pp. 43-52). Springer, Singapore.

[17]. V. Vijaykumar, Nallam Sri Divya, P. Sarojini, K. Sonika. Isolation Forest and local Outlier Factor for Credit Card Farud Detection System, International Journel of Engineering and Advanced Technology (IJEAT) ISSN:2249- 8958, Vol:9, April 2020

[18]. Chen, Joy Iong-Zong, and Kong-Long Lai. "Deep Convolution Neural Network Model for UPI payments-Card Fraud Detection and Alert." Journal of Artificial Intelligence 3, no. 02 (2021): 101-112.

IJEAST

INTERNATIONAL JOURNAL OF ENGINEERING APPLIED SCIENCE AND TECHNOLOGY

AUTHORS

- Suchitra Vasantrao Dahiwade
- Nitin V. Swami
- Sushil V. Kulkarni

ABOUT IJEAST

International journal of Engineering Applied Science and Technology (IJEAST) is a peer-reviewed, open access journal that publishes high - quality research paper in the field of Engineering, Applied Science and Technology.

IJEAST aims to provide a platform for researchers, academicians, and professionals to share their innovative ideas, research findings, and practical experiences with the global scientific community.

JOURNAL METRICS

H-INDEX	i10-INDEX	IJEAST CITATIONS	PEER-REVIEWED & OPEN ACCESS
33	154	9,647 (IJEAST CITATIONS)	PUBLISHED MONTHLY

PEER REVIEWED

All submission are rigorously peer reviewed to ensure quality.

AUTHORS ARE OUR PRIORITY

We value our authors and recognize their contribution to the advancement of research and knowledge.

OPEN ACCESS

Free and unrestricted access to research for all.

GLOBAL REACH

Connecting researchers and professionals worldwide.

TIMELY PUBLICATION

We ensure a swift and efficient publication process.

For more information, visit our website
www.ijeast.com

editor@ijeast.com
www.ijeast.com
India

2455-2143