An Explainable Hybrid Fraud Detection Engine for Online Payments Using Rule-Based Analysis and Machine Learning

K Varshitha[1], L Bala kishan[2], M Lasya[3], M Mukesh[4], Dr. S Shiva Prasad[5], Ms. U. Shireesha[6]
[1,2,3,4]*Student, Department of CSE (Data Science), Malla Reddy Engineering college, Secunderabad*
[5] *Professor, Department of CSE (Data Science), Malla Reddy Engineering college, Secunderabad*
[6] *Assistant Professor, Department of CSE (Data Science), Malla Reddy Engineering college, Secunderabad*
doi.org/10.64643/IJIRTV12I10-195306-459

***Abstract*—Online financial fraud is a problem because of the fast growth of digital payment systems. The old ways of finding fraud mostly use fixed rules, which do not work well against fraud patterns and often give a lot of false warnings. This project is about a way to find online payment fraud that uses a combination of rules and machine learning to get it right and do it quickly. The project uses something called SMOTE to make this way of finding fraud work better. This new way combines rules with machine learning to detect online payment fraud accurately and in real time which is a big improvement, over the old ways. Online financial fraud and online payment fraud are issues that need to be solved. The system deals with the issue of class imbalance by using a method called Synthetic Minority Over-sampling Technique or SMOTE for short. This helps the model learn about fraud patterns even when it only has a few examples of fraud to work with.A Random Forest classifier is used to figure out how likely a transaction is to be fraud. The system uses all of this information to come up with a fraud risk score that changes based on the situation. The system uses this fraud risk score to help figure out if a transaction's likely to be fraud. The Synthetic Minority Over-sampling Technique helps the model learn about fraud patterns and the Random Forest classifier helps to determine the fraud risk score. The proposed hybrid engine achieves significantly improved accuracy compared to conventional rule-based systems and provides explainable outputs to justify each prediction. Experimental results demonstrate that the system enhances detection performance, reduces false alarms, and is suitable for real-time fraud prevention in online payment platforms.**

***Index Terms*—Online Fraud Detection,Real-Time Transaction Monitoing, Hybrid Fraud Detection Model, SMOTE Data Balancing, Explainable AI(XAI), Risk Score Calculation, Random Forest Classifier**

I. INTRODUCTION

The growth of payment platforms and online financial services is getting out of control and that is making online fraud a big problem. Online fraud is really bad because it causes people and companies to lose a lot of money. It also makes people not trust banking systems.When it comes to catching fraud old systems mostly look at things like how much money is being moved or if someones account balance is too low or if an account is on a bad list. These systems are easy to use. They work fast. They are not good at catching complicated fraud that is always changing. They often send out a lot of false warnings. Digital payment platforms and online financial services are still, at risk because of this.

In the few years Machine Learning techniques have been used a lot for finding fraud. This is because Machine Learning is good at finding patterns in old data. Models like Random Forest and Logistic Regression and Neural Networks can look at a lot of transaction data. Predict when something is fraud better, than the old ways of doing things. Machine Learning systems that only use Machine Learning also have some problems. Machine Learning has its set of issues that need to be considered when using Machine Learning for fraud detection. These models are like a box. You do not know what is going on inside. They make predictions. They do not tell you why. This makes it hard to believe in them and use them in financial situations.

This project is trying to solve some problems. It wants to make a system that can help detect fraud online. This system is special because it uses two ways to

make decisions. It looks at rules that people have made. It also uses Machine Learning to make predictions. The system has a trick to make sure it is fair and gets things right. This trick is called SMOTE. It helps the system make better guesses. The system also has a part that explains why it thinks something is fraud. This means that people can understand why the system made a decision. The Online Fraud Detection system can check things in time. This means it can look at transactions and decide if they are okay before they are final. The Online Fraud Detection system is really good because it uses Machine Learning and rules to make decisions. It also uses the SMOTE technique to make sure it is fair. It has a part that explains things.

By combining rule-based logic, machine learning intelligence, balanced data processing, and explainable decision support, the proposed framework enhances fraud detection accuracy, reduces false positives, and improves system transparency. This approach bridges the gap between traditional fraud detection techniques and modern intelligent systems, making it suitable for real-world deployment in secure online financial applications.

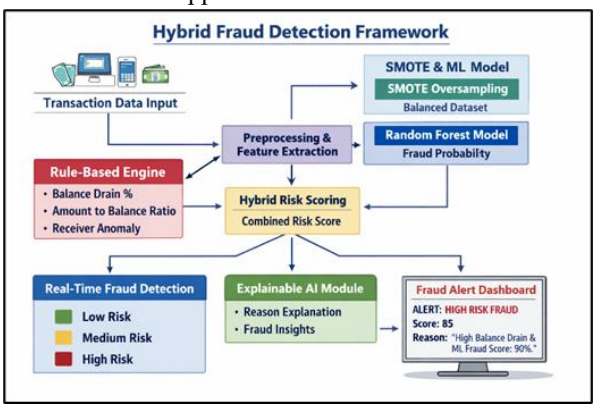


Figure 1. Hybrid Fraud Architecture

II. LITERATURE SURVEY

People have been looking into payment fraud detection a lot. This is because we do payments really fast and there are a lot of them. Also the ways people try to commit fraud with payments keep changing.At first systems to stop payment fraud mostly used a set of rules to detect fraud. These rules were like thresholds. For example if someone pays an amount of money or if their balance drops a lot or if they do a lot of transfers in a row the system would send out an alert. These rule-based systems are not hard to set up. They are easy to understand.. They have some problems. They do not do a job of catching new ways that people try to commit fraud. They also send out a lot of alerts.. The people, in charge have to keep updating the rules all the time to try to keep up with the fraud.To get around this problem the researchers started using machine learning to detect fraud. They looked at fraud as a problem that can be solved by classifying things into groups. The common methods they used include Logistic Regression, Decision Trees, Random Forest, Gradient Boosting and Naive Bayes. With these methods the machine learning models learn patterns from transactions that have been labeled.

Machine learning methods like Logistic Regression and Decision Trees are better than using rules because they can adapt to situations. However how well they work depends on how the features are chosen, the quality of the data and whether the methods are validated properly. This is especially true for machine learning methods such, as Random Forest and Gradient Boosting, which are types of machine learning. Lots of people do research on this. They find out that when we look at the data, for fake transactions it is usually very uneven. What this means is that real cases of fraud do not happen often. Because of this it is not very helpful to look at how often a model is right or wrong. This is because the models tend to favor the transactions the ones that are not fake just because there are more of them. The transaction fraud data is what gets affected by this it is the transaction fraud data that's uneven.

To deal with imbalance a lot of studies use techniques that balance the data like SMOTE random over-sampling under-sampling and hybrid sampling. SMOTE is widely used because it creates samples for the minority group and usually helps improve recall for fraud cases. The thing about oversampling is that it can also add noise or make the model overfit if you are not careful. So many papers suggest using SMOTE on the training data and then evaluating it with metrics from the confusion matrix, such, as Precision, Recall, F1-score and ROC-AUC rather than just looking at accuracy. This way you get an idea of how well the model is doing, especially when it comes to fraud cases and SMOTE.

Recent studies show that using a mix of rule-based logic and machine learning predictions is a way to get the best results. In these systems rules are used to catch

" fraud" and make sure business rules are followed while machine learning finds patterns that are not easy to see and works better with new situations.

Real-time systems have a few parts. They can look at some information about a transaction like how much money is being moved and if that is a lot compared to what is already in the account. They also use a tool that has been trained to guess how likely it is that a transaction is bad. Then they use that guess to decide if the transaction is risk, medium risk or high risk. Real-time fraud detection systems use things like balance drain percentage and amount-to-balance ratio to help make these decisions.

Finally, modern literature increasingly stresses explainable AI (XAI) because fraud decisions impact customers (blocked payments, account holds) and must be justifiable. Techniques such as feature importance, rule tracing, and explanation methods (example: SHAP/LIME concepts) help show why a transaction is flagged. Explainability improves trust for bank staff and supports compliance/audit requirements.

III.PROBLEM STATEMENT AND OBJECTIVES

3.1 PROBLEM STATEMENT

Banking and mobile wallets are getting really popular. This means that people are losing money to fraud more and more every year. Fraudsters are always coming up with ways to trick people like pretending to be someone else taking over accounts and draining all the money out. These things are very hard to catch with the systems that are in place. Banking and mobile wallets are still not completely safe, from fraudsters who do things like identity spoofing and account takeover.

The fraud detection systems we have now are mostly based on rules. They look at things like how much money's being moved how often it is being moved or how much money is in an account. These rules do not. That is a problem. They cannot keep up with ways that people are trying to commit fraud. Because of this they often miss the fraud or they send out a lot of false warnings. This is a problem for people who are not trying to commit fraud because it is an inconvenience to them. The fraud detection systems are not doing a job of figuring out what is real fraud and what is not. Fraud detection systems, like these are just not working well.

Machine learning models do a job of finding fraud but they are, like a secret box. The person using the machine learning models does not know why a transaction is considered fraud or a normal transaction. This is a problem because banks and financial institutions need to know what is going on. They do not trust automated fraud detection solutions when they do not understand how they work. Machine learning models need to be more open so that banks and financial institutions can trust them to find fraud.Most of the time the information we use to find fraud is not very balanced. This means that real transactions are a lot more common than ones. The problem with this is that it makes it hard to teach our systems to find fraud. As a result our systems do not make good predictions, about fraud cases. Fraud detection is really important. We need to work on making our systems better at finding fraud. Fraud detection systems need to be able to look at all the information and find the transactions.

3.2 OBJECTIVES

The main things that the proposed Explainable Hybrid Machine Learning Framework for Fraud Detection wants to do are listed below:

1. It wants to help us understand how the Fraud Detection system makes decisions
2. It wants to make the Fraud Detection system better at finding fraud
3. It wants to make the Fraud Detection system explain what it does so we can trust it

The Explainable Hybrid Machine Learning Framework for Fraud Detection is going to do this by using Machine Learning to look at things that might be fraud and then explain why it thinks that. The Explainable Hybrid Machine Learning Framework for Fraud Detection is very important because it helps us stop fraud. That is what the Explainable Hybrid Machine Learning Framework for Fraud Detection is, for.

To handle class imbalance in fraud datasets using SMOTE data balancing techniques. We want to create outputs that explain why a transaction is seen as risk, medium risk or low risk. This means we need to make it clear what makes a transaction fall into one of these categories. The goal is to provide outputs, for transactions that are considered high risk, medium risk or low risk.

To improve overall detection accuracy while minimizing false positive alerts.To provide graphical dashboards for detection comparison, model comparison, and accuracy improvement analysis.To enhance trust and usability of fraud detection systems by combining transparency with intelligent decision-making.

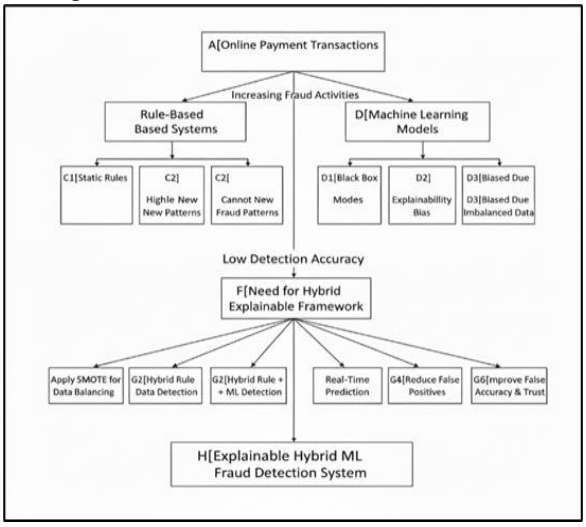


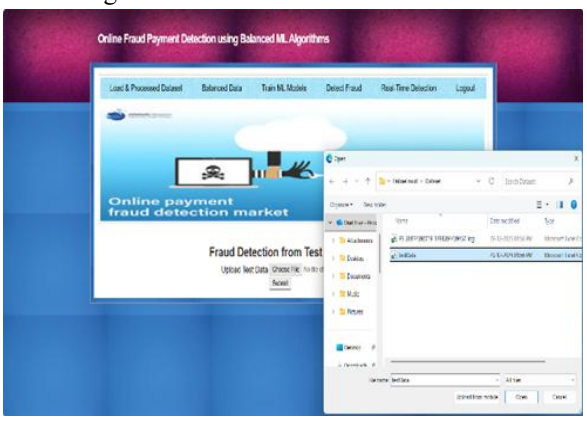
Figure 2: Limitations of Traditional Fraud Detection Systems

IV. PROPOSED METHODOLOGY

The new system uses a kind of machine learning called Explainable Hybrid Machine Learning to find online fraud payments in real time. First it looks at the transaction data. Makes sure it is all the same. It also uses a technique called SMOTE to make the fraud data more balanced because there is usually a lot normal data than fraud data. Then it uses a Random Forest model to look at the data and figure out how likely each transaction is to be fraud. At the time it uses a set of rules to look for things that might be suspicious like when someone takes out a lot of money, at once or when the amount of a transaction is really high compared to what someone normally spends or when someone is sending money to someone they do not usually send money to. The system uses Explainable Hybrid Machine Learning to do all of this and find fraud payments. The final fraud risk score is computed by combining the rule-based risk with the ML prediction probability. Based on this hybrid score, transactions are classified as low, medium, or high risk. Each decision is supported with human-readable explanations to ensure transparency and trust in the system.

4.1 Offline csv-based fraud detection system

The offline fraud detection module that uses csv files is in charge of creating a good machine learning model. This model is made using transaction data. The system uses sets of transaction data that are stored in csv files. These files have things, like how much money was sent, the balances of the sender and receiver what kind of transaction it. If it was fake or not. First the data is cleaned up by taking out missing information dealing with numbers and getting rid of things that do not matter. The csv-based fraud detection module does all this to make sure the data is good and can be used to make a model. The fraud detection module uses the transaction data from the csv files to build this model. So the important things are picked out. Made the same so all the numbers are on the same level. This really helps the machine learning algorithms learn things. The machine learning algorithms can learn better when the numbers are all in the range.



The dataset is a problem because it has a lot of genuine transactions and not many fraudulent ones. This is an issue that needs to be fixed. The dataset is usually very imbalanced after we get it ready. To make the dataset better we use the method. The smote method helps us make fake fraud samples so that the dataset is balanced. We divide the dataset into two parts: the training set and the testing set.

We use the training set to teach machine learning models, like the random forest model the logistic regression model and the gradient boosting model. The performances of the models are looked at using things, like how accurate they are how precise they are, how well they remember things and something

called the f1-score when they are tested with a special set of data. The models are tested on the test dataset to see how well they do. The test dataset is used to evaluate the performances of the models.

Finally, the best performing trained model is selected and saved. This trained model is not used directly by end users but is deployed into the real-time fraud detection engine. Thus, the offline module acts as the backbone of the system, ensuring that the real-time prediction module is powered by a well-trained, smote-optimized and highly accurate fraud detection model.

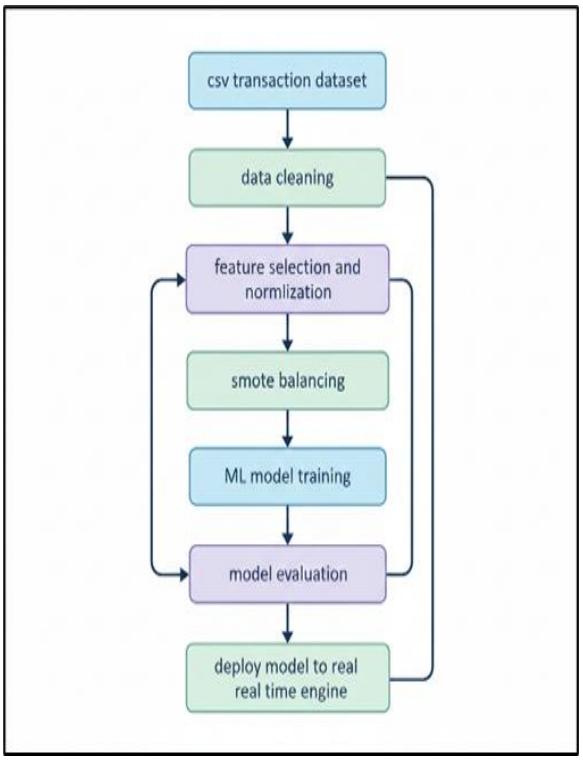


Figure 3: Offline ml training flow

4.2 Real-time explainable hybrid fraud detection architecture

The fraud detection system is made to find transactions right away and it also tells us why it made those decisions. This system looks at real time information about each transaction like how much money's being sent how much money the sender has, how much money the receiver has and any changes to their balances. We get this information from the website.

First we look at all this information in a step called preprocessing. In this step we do things like figure out how much of the senders money is being used for the transaction compare the transaction to the senders balance and check if the receivers balance is changing a lot. We do all this to help the fraud detection system make decisions, about fraudulent transactions. The processed features are then sent to the trained machine learning model. This machine learning model gives us a fraud probability score. This score tells us how likely it is that the transaction is fraudulent.

At the time the rule-based engine looks at the transaction. It checks for things like fund transfers or if the receivers balance suddenly increases a lot or if the transaction is really big compared to other transactions.The machine learning model and the rule-based engine both give us their results. We combine these results using a method called hybrid risk scoring. This gives us a risk score, for the transaction. The final risk score is what we use to decide if the transaction is safe or not.

The system looks at this score. Decides if the transaction is low risk, medium risk or high risk right away. We want to be clear about how we make these decisions. So we have a module that looks at what rules were used and how much the machine learning probability affected the decision. This module makes explanations that people can understand, like "we saw a drop in your balance" or "our machine learning model thinks there is a high chance of fraud, with this transaction". The final result and its explanations are then displayed instantly on the user dashboard, enabling users and administrators to understand not only the fraud decision but also the reasoning behind it.

V. METHODOLOGY

The way the proposed hybrid fraud detection system works is to make sure it can find fraud in payment transactions quickly and accurately. It also has to be easy to understand how it makes these predictions.The system starts by getting information about transactions in time. This information includes things like how much money's being sent how much money the sender has, how much money the receiver has and how much money they have after the transaction.

The hybrid fraud detection system is important because it helps stop fraud when people make payments online.

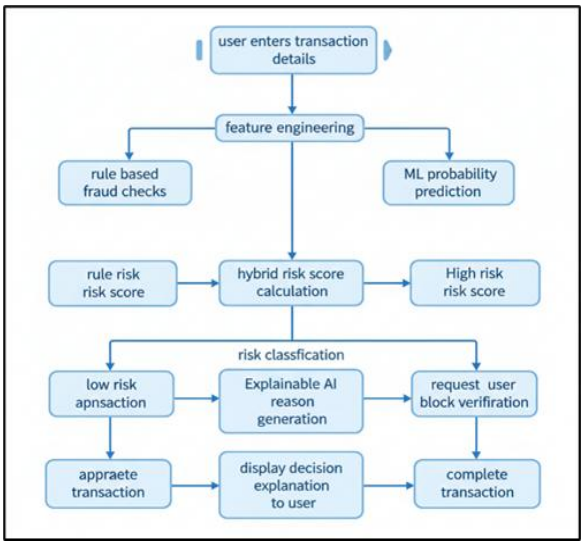


Figure 4: Real-time hybrid fraud flow

When the transaction data is received a feature engineering module changes the information into important signs of fraud such as the balance drain percentage, the amount-to-balance ratio and the sudden increase in the receivers balance. These new features are really important, for finding financial behaviour in transaction data. The transaction data and the new features work together to help identify activity that we would not be able to find just by looking at the raw transaction data.

The special features that we made are then made normal using a trained scaler. Sent to a machine learning classifier, where a random forest model figures out the chance of fraud. At the time a rule-based detection engine looks at the transaction using rules that experts already know such, as when someone takes out a lot of money makes really big transfers or acts strangely when getting money.

```
from imblearn. over_sampling import SMOTE
from sklearn. preprocessing import StandardScaler

scaler = StandardScaler ()
x_scaled = scaler.fit_transform(x)

smote = SMOTE (random_state=42)
x_resampled, y_resampled = smote.fit_resample (x_scaled, y)
```

The system gets results from the rule engine and the machine learning model. Then a hybrid risk scoring mechanism puts these results together to get a fraud risk score. This way the system uses the things about machine learning and the rule engine. The machine learning model can adapt to things and the rule engine is reliable because it uses rules that are specific to the domain. When the system has the risk score it puts the transaction into one of three groups: low risk, medium risk or high risk, for fraud.

Finally, an explainable ai layer generates human-readable explanations highlighting the factors responsible for the decision. These insights are displayed in the real-time dashboard, allowing users and analysts to clearly understand the reasoning behind each fraud classification.

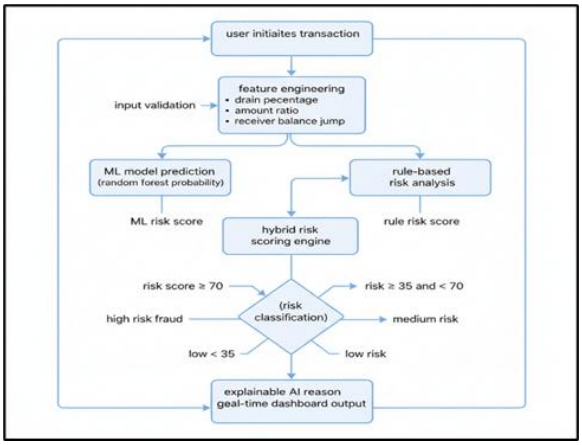


Figure 5: Fraud detection workflow

VI. MACHINE LEARNING IMPLEMENTATION

The proposed system uses a combination of new ways of learning. This system teaches itself by using machine learning and explainable real-time risk analysis together. The system learns from transaction data. Then the system is used in a real-time environment to detect fraud. The fraud detection environment is where the system actually checks for fraud in time using the real-time risk analysis and the classical machine learning that the system learned from the historical transaction data of the proposed system.

6.1 Data Preprocessing and Balancing using SMOTE

In the world fraud datasets are not balanced at all. The number of transactions is much higher than the number of fraud transactions. This is a problem because it means that the models we use to detect fraud are not very good at learning what fraud looks like. To fix this problem we need to clean up the dataset and make sure all the information is consistent. Then we

need to balance the dataset so that it has a mix of real and fraud transactions. We do this by using a technique called synthetic minority oversampling technique or smote for short which helps us get a better balance of fraud transactions, in the dataset.
Steps involved:

- Remove null values and irrelevant features
- Encode categorical variables
- Normalize numerical attributes using standard scaler
- Apply smote to generate synthetic fraud samples

Important code snippet

6.2 Hybrid model training and evaluation
So we use a forest classifier after balancing the data. This is because a random forest classifier is really good at dealing with things that're not straightforward and data that has some mistakes in it. The random forest classifier we train is then used to predict the chance that a transaction's fraudulent for each transaction. The random forest classifier gives us the probability of fraud, for each transaction. When we want to see how good a model is we use things, like accuracy, precision, recall, f1-score and confusion matrix to check it. We look at the accuracy to see how often the model gets it right. We also look at the precision, recall and f1-score of the model to get an idea. The confusion matrix of the model is also very important to check. So we use accuracy, precision, recall, f1-score and confusion matrix to evaluate the model.

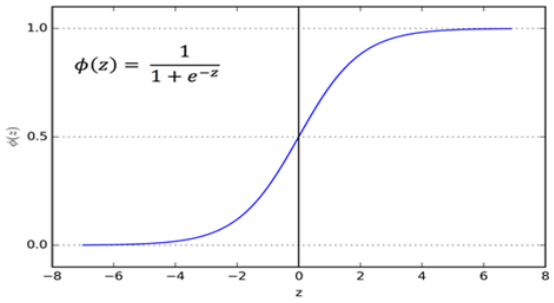


Figure 6: Logistic Regression

6.3 Real-time explainable prediction engine
For real-time detection the trained model works with a rule-based risk scoring system. The system checks each transaction that comes in. It looks at each transaction using the trained model and the rule-based risk scoring system. ML probability score domain-specific rule conditions (balance drain, transaction ratio, receiver behavior)

```
ml_prob = rf. predict_proba(testData) [0][1]
risk_score += ml_prob * 25
```

This hybrid decision mechanism produces three outcomes:

- low risk – normal transaction
- medium risk – needs verification
- high risk – fraud detected

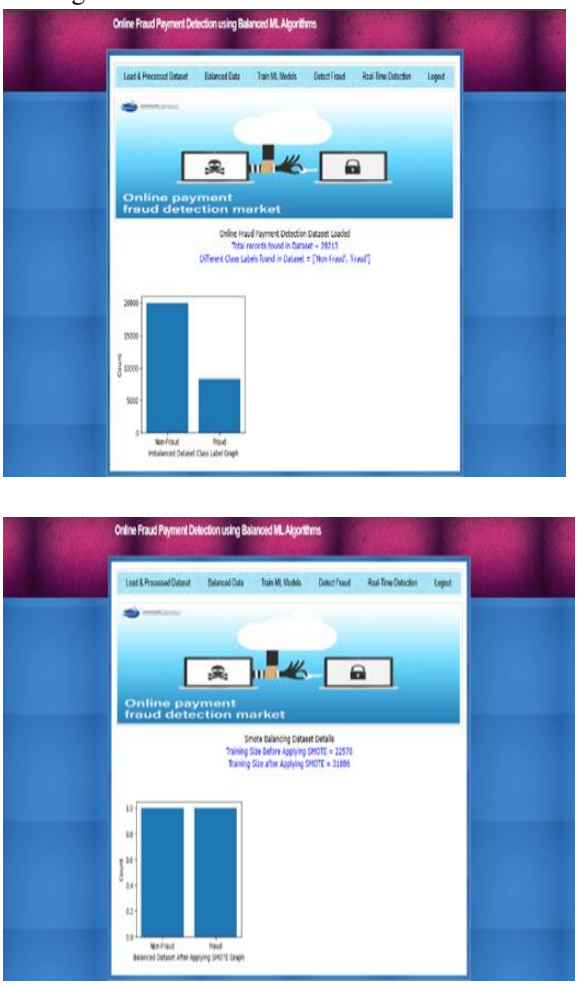
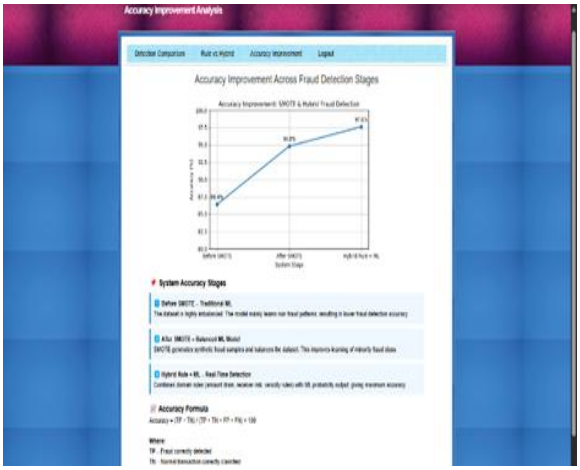


Figure 6: Imbalanced Fraud Dataset &Balanced Dataset using SMOTE

VII. RESULTS

The performance of the proposed explainable hybrid fraud detection framework was evaluated using a real-world online payment transaction dataset. The system was tested under three configurations: traditional rule-

based detection, standalone machine learning without data balancing, and the proposed hybrid rule + ML System with SMOTE and real-time explainable logic. The evaluation was conducted using accuracy, fraud detection rate, false positive rate, and real-time risk classification.



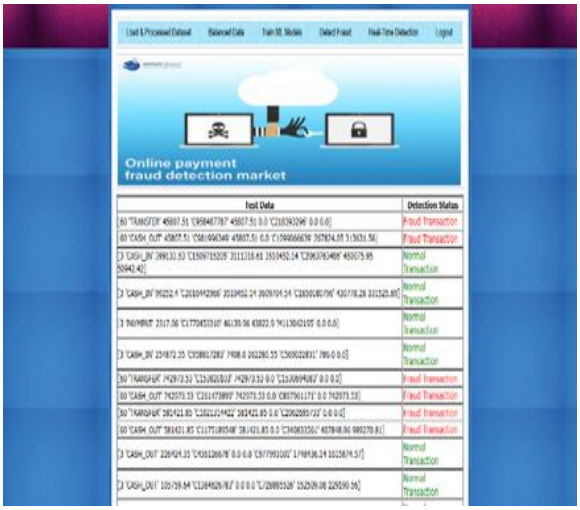
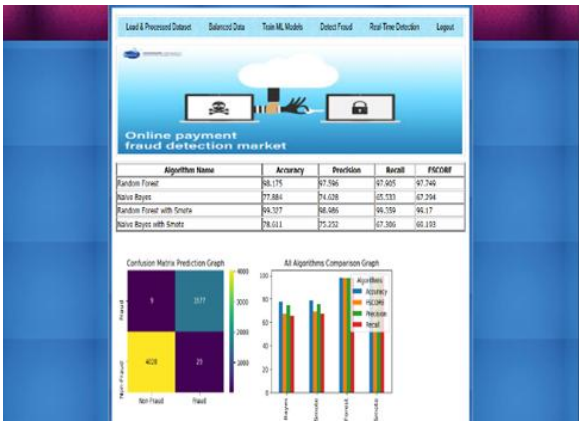


Figure.7 Identification of malware

7.1 Performance Comparison of Detection Models

The old system that used rules to make decisions got it right 67% of the time. This is because it used limits like how much money could be moved and basic balance checks. The problem is that it could not keep up with fraud patterns.

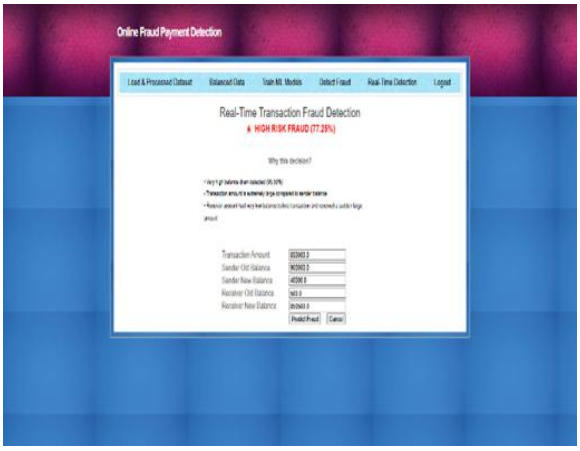
The machine learning model that worked alone and did not use SMOTE was a bit better. It got it right 80.21% of the time. However this model had a problem with class imbalance. It also made mistakes by saying some fake transactions were transactions.



When we used SMOTE and combined it with the hybrid decision engine the new system was much better. The new system got it 99.10% of the time. This is an improvement, over the old system and the machine learning model that worked alone. The hybrid decision engine and SMOTE really helped the new system to be very accurate and stop fraud. The analysis of the confusion matrix showed that it was really good at finding the transactions and not so good at missing them. This means that the system can find transactions most of the time. The confusion matrix analysis is very important because it helps us understand how well the system is working. The confusion matrix analysis tells us that the system is good, at detecting transactions.

7.2 Real-Time Detection and Explainability Analysis

The real-time fraud detection module was tested using live transaction inputs, where transactions were dynamically classified into low, medium, and high-risk categories. High-risk transactions exhibited features such as extreme balance drain, large transaction-to-balance ratios, abnormal receiver account behavior, and high ML fraud probabilities. The explainable AI module generated detailed reasoning for every prediction, highlighting key fraud indicators such as “very high balance drain,” “sudden receiver balance spike,” and “ML model predicts high fraud likelihood.” This not only improved transparency but also enabled banking personnel to understand the decision process clearly. The results demonstrate that the proposed real-time hybrid framework effectively balances security and user convenience while providing reliable, interpretable fraud detection.



VIII. CONCLUSION

This project presents a real-time online payment fraud detection system that identifies fake transactions effectively. It combines rule-based verification with advanced machine learning models to improve fraud prediction accuracy. Unlike traditional rule-only approaches, the proposed method adapts well to new and evolving fraud patterns. Experimental evaluation shows that the conventional rule-based system detects only limited fraud cases and generates more false alerts. In contrast, the hybrid model achieves 99.10% accuracy while significantly reducing false alarms. The system continuously monitors important transaction features such as transaction amount, frequency of transfers, receiver behavior, and spending patterns. These real-time features help detect suspicious transactions more precisely. A Fraud Risk Score is generated to support quick decision-making and prioritize high-risk payments. An Explainable AI (XAI) module is integrated to justify why a transaction is marked as fraud or legitimate. This transparency is highly important for banks and financial institutions for auditing and compliance. The dashboard supports efficient fraud monitoring and improves operational response. Future enhancements can include deep learning models like LSTM and Graph Neural Networks (GNNs) for capturing complex fraud trends. The system can also be scaled using Apache Kafka streaming for high-volume real-time transactions. Additionally, adaptive learning can be added to update the model automatically against emerging fraud techniques. Overall, the proposed framework ensures accurate, explainable, and scalable fraud prevention in digital payment platforms.

REFERENCES

[1] A. Dal Pozzolo, G. Bontempi, and M. Snoeck, “Adaptive machine learning for credit card fraud detection,” IEEE Computational Intelligence Magazine, vol. 10, no. 1, pp. 33–46, Feb. 2015.

[2] F. Carcillo, A. Dal Pozzolo, M. Snoeck, and G. Bontempi, “Scarff: A scalable framework for streaming credit card fraud detection,” Information Fusion, vol. 68, pp. 43–61, Apr. 2021.

[3] N. V. Chawla, K. W. Bowyer, L. O. Hall, and W. P. Kegelmeyer, “SMOTE: Synthetic minority over-sampling technique,” Journal of Artificial Intelligence Research, vol. 16, pp. 321–357, Jun. 2002.

[4] A. Dal Pozzolo, G. Bontempi, and M. Snoeck, “Adversarial drift detection in credit card fraud detection,” IEEE Transactions on Neural Networks and Learning Systems, vol. 29, no. 11, pp. 5547–5560, Nov. 2018.

[5] A. C. Bahnsen, A. Stojanovic, D. Aouada, and B. Ottersten, “Cost-sensitive decision trees for fraud detection,” Expert Systems with Applications, vol. 42, no. 21, pp. 7363–7371, Nov. 2015.

[6] S. M. Lundberg and S. I. Lee, “A unified approach to interpreting model predictions,” Advances in Neural Information Processing Systems (NeurIPS), pp. 4765–4774, 2017.

[7] M. T. Ribeiro, S. Singh, and C. Guestrin, “Why should I trust you? Explaining the predictions of any classifier,” Proceedings of the ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, pp. 1135–1144, Aug. 2016.

[8] L. Breiman, “Random forests,” Machine Learning, vol. 45, no. 1, pp. 5–32, Oct. 2001.

[9] C. Phua, V. Lee, K. Smith, and R. Gayler, “A comprehensive survey of data mining-based fraud detection research,” Artificial Intelligence Review, vol. 34, no. 3, pp. 261–285, Oct. 2010.

[10] T. Fawcett and F. Provost, “Adaptive fraud detection,” Data Mining and Knowledge Discovery, vol. 1, no. 3, pp. 291–316, Sept. 1997.

[11] H. He, Y. Bai, E. A. Garcia, and S. Li, “ADASYN: Adaptive synthetic sampling approach for imbalanced learning,” IEEE International Joint Conference on Neural Networks, pp. 1322–1328, Jun. 2008.

[12] Z. H. Zhou, Ensemble Methods: Foundations and Algorithms, Boca Raton, FL, USA: Chapman & Hall/CRC, 2012.
[13] F. Dal Pozzolo, G. Bontempi, and M. Snoeck, "Handling concept drift in credit card fraud detection," IEEE Symposium Series on Computational Intelligence, pp. 1–8, Dec. 2014.
[14] European Central Bank, "Card fraud statistics in the European Union," ECB Annual Financial Report, Frankfurt, Germany, 2020.
[15] Kaggle, "IEEE-CIS Fraud Detection Dataset," Kaggle Competition, 2019.
[16] S. Satla and C. S. Shieh, "Multi-model Telugu speech recognition: Improving ASR with dialect classification and optimization techniques," Traitement du Signal, vol. 42, no. 6, pp. 3159–3169, 2025. doi: 10.18280/ts.420611.
[17] D. Kothandaraman, N. Praveena, K. Varadarajkumar, S. Satla, and W. Abera, "Intelligent forecasting of air quality and pollution prediction using machine learning," Adsorption Science & Technology, vol. 2022, 2022.
[18] S. Shivaprasad and M. Sadanandam, "Dialect identification using modified features with deep neural networks," Traitement du Signal, vol. 38, no. 6, pp. 1793–1799, Dec. 2021. doi: 10.18280/ts.380622.