

Makeathon 2023

Idea Submission

ML BASED FRAUD DETECTION

Team Members

Soumili Chakraborty

Yashika Gupta

Ankita Ghosh

Raksha Pahariya

PROBLEM STATEMENT

Develop and maintain ML-based fraud detection models that are effective at identifying evolving fraud patterns even in the presence of imbalanced data.

Fraudulent activities pose a significant problem for businesses and individuals, with the potential to cause financial and reputational damage. Traditional fraud detection techniques based on rule-based systems often fail to identify new and evolving fraud patterns, requiring experts to manually update the rules. This approach can be time-consuming, expensive, and prone to errors.

Machine learning-based fraud detection offers a more effective solution by using algorithms to analyze large amounts of data and identify patterns that indicate fraudulent activity. However, the imbalanced nature of fraud data, with a large number of non-fraudulent instances compared to a few fraudulent instances, can create bias in the model, leading to a high rate of false positives or false negatives.

PROBLEM STATEMENT

Therefore, the problem statement aims to develop and maintain ML-based fraud detection models that can effectively identify evolving fraud patterns, even in the presence of imbalanced data. This requires a comprehensive approach that includes data collection and preparation, model training using imbalanced data, model evaluation, and the submission of a project description, presentation, video, and link to the project.

By addressing these challenges, the proposed solution aims to provide businesses and individuals with a more accurate and reliable fraud detection system, ultimately helping to prevent financial losses and safeguard reputations.

SOLUTION

Solution Overview:

Our proposed app, FraudWatch is designed to detect fraud using advanced machine learning algorithms, specifically autoencoders. This will help users protect themselves against fraud by analyzing any data entered into the app and detecting fraudulent activity.

The app works by uploading the user's data into the algorithm, which then analyzes it and compares it to a pre-existing database of legitimate data. If the data entered is deemed suspicious or fraudulent, the app will trigger an alert to the user and notify the appropriate authorities.

FraudWatch is designed to be user-friendly, with a simple interface that allows for easy data entry and quick detection. The app also utilizes state-of-the-art encryption and security protocols to ensure the safety and confidentiality of user data.

SOLUTION

How does it solve the problem at hand?

Our app, which uses autoencoders to detect fraudulent activity and sends a notification to both the user and the concerned authorities upon detection, can address several challenges of developing effective ML-based fraud detection models.

- Using autoencoders allows the app to identify fraud patterns in real time, which can help prevent fraudulent transactions from occurring or limit their impact. Additionally, autoencoders can learn to identify new and evolving fraud patterns independently, reducing the need for manual updates to the detection system.
- The app's ability to notify both the user and concerned authorities upon detecting fraud can help ensure that appropriate action is taken quickly to minimize the financial and reputational damage caused by fraudulent activity. This can be particularly important in cases where large amounts of money are at stake or personal information is at risk.

SOLUTION

Impact Metrics

1. **Detection accuracy:** Percentage of fraudulent activities correctly identified by the app, as compared to the total number of fraudulent activities in the data set. Higher accuracy indicates better fraud detection and reduced financial losses for the user.
2. **False positive rate:** Measures the percentage of legitimate activities that are incorrectly identified as fraudulent by the app, as compared to the total number of legitimate activities in the data set. A lower false positive rate indicates fewer unnecessary alerts for the user and lower chances of interrupting legitimate activities.
3. **Response time:** Measures the time taken by the app to detect fraud and trigger an alert to the user and concerned authorities. A shorter response time indicates faster detection and quicker action.
4. **User adoption:** Measures the percentage of potential users who download and use the app regularly. Higher user adoption indicates greater awareness and concern about fraud, as well as trust in the app's ability to detect and prevent fraudulent activities.
5. **Cost savings:** Measures the amount of money saved by users and concerned authorities as a result of the app's fraud detection capabilities. This includes both the direct financial losses prevented by early detection of fraud and the indirect costs saved by minimizing reputational damage and legal fees.
6. **Evolution of fraud patterns:** Measures the app's ability to adapt to new and evolving fraud patterns over time, as compared to traditional rule-based systems. Higher adaptability indicates greater resilience to emerging fraud threats and a reduced need for manual updates to the detection system.

SOLUTION

Frameworks and Technologies used:

1. Data Analysis and Machine Learning:

- Pandas and NumPy for data manipulation and processing.
- Matplotlib-pyplot for data visualization and graphing.
- TensorFlow.Keras for developing and training deep learning models, specifically autoencoders.
- Sklearn.ensemble for implementing random forest classifiers.
- imblearn.over_sampling- SMOTE for oversampling imbalanced data.
- Sklearn.metrics for evaluating model performance using various metrics such as precision, recall, AUC, ROC curve, and F1 score.
- Sklearn.model_selection for tuning hyperparameters using GridSearchCV and splitting data into training and testing sets.

2. Web Development and App Development Infrastructure:

- RDBMS MySQL for database management.
- Django for web backend development.
- React for web-frontend development.
- Apache for web server management.
- Firebase Cloud Messaging and Twilio for sending notifications.
- RestAPI for creating an API for the app.
- hash lib/Django login for password/username validation.

3. Additional Features:

- OpenCV for face recognition.

SOLUTION

Assumptions

We have assumed that the user can be either an individual or any business owner who trusts the process and uploads his financial transactions including debit, payment, and transfer to any third parties which include his transaction number done through any payment gateway file to the database and keeps himself alert through notifications in case any fraud or anomaly is detected. The fraud includes unusual activity in the credit card regarding transfer or debit from different merchants such as healthcare professionals who have charged more to individuals or shopping platforms to charge more or insurance fraud or any money lender or external clients as well as identity theft. The notification will be sent to concerned third parties as well along with the user to take required actions. For example, it will be sent to the bank to seal the user's account in case some fraudulent payments are happening from it.

SOLUTION

Decision point

The algorithm we have chosen to detect fraud is auto encodes combined with random forests. We arrived at this choice after researching several existing models and analyzing the accuracy of each different algorithm whether it's supervised unsupervised or semi. We obtained that random forest did on the grounds of boosting and ensemble learning provides the highest accuracy and minimum false positives and false negatives in supervised learning. On the other hand, deep neural networks-based feed-forward autoencoders have been proven highly effective in anomaly detection. So combining both of them we developed this model to gain the highest accuracy.

SOLUTION

Constraints

- We have right now developed a model which can predict fraud and not process transactions. So we are looking forward to getting over this constraint by making it a secure payment gateway as well as a fraud detection app.
- Effective data storage as well as data collection
- The algorithm we are using can be boosted by using Adaboost or gradient boost. Hence we are effectively trying out ways to boost our algorithms as much as possible.
- We have right now not implemented self website check process to avoid a crash

SOLUTION

Scalability/ Usability and Ease of Implementation:

The implementation of FraudWatch using autoencoders and other advanced ML algorithms can be relatively straightforward for experienced developers with knowledge in these areas. However, the effectiveness of the app may depend on the quality and quantity of data available for training the algorithm.

The app's usability can be high, as it is designed to be user-friendly with a simple interface that enables easy data entry and quick detection. Additionally, the app's security features, such as encryption and confidentiality protocols, can enhance its usability.

The scalability of the app can also be high, as the autoencoder algorithm can learn to identify new and evolving fraud patterns, reducing the need for frequent updates to the detection system. However, the app's scalability may also depend on factors such as the size of the user base and the availability of computing resources.

Hence, the proposed app can be a highly effective solution for businesses and individuals looking to protect themselves against fraudulent activity, particularly if implemented with high-quality data and appropriate computing resources.

CONCEPT

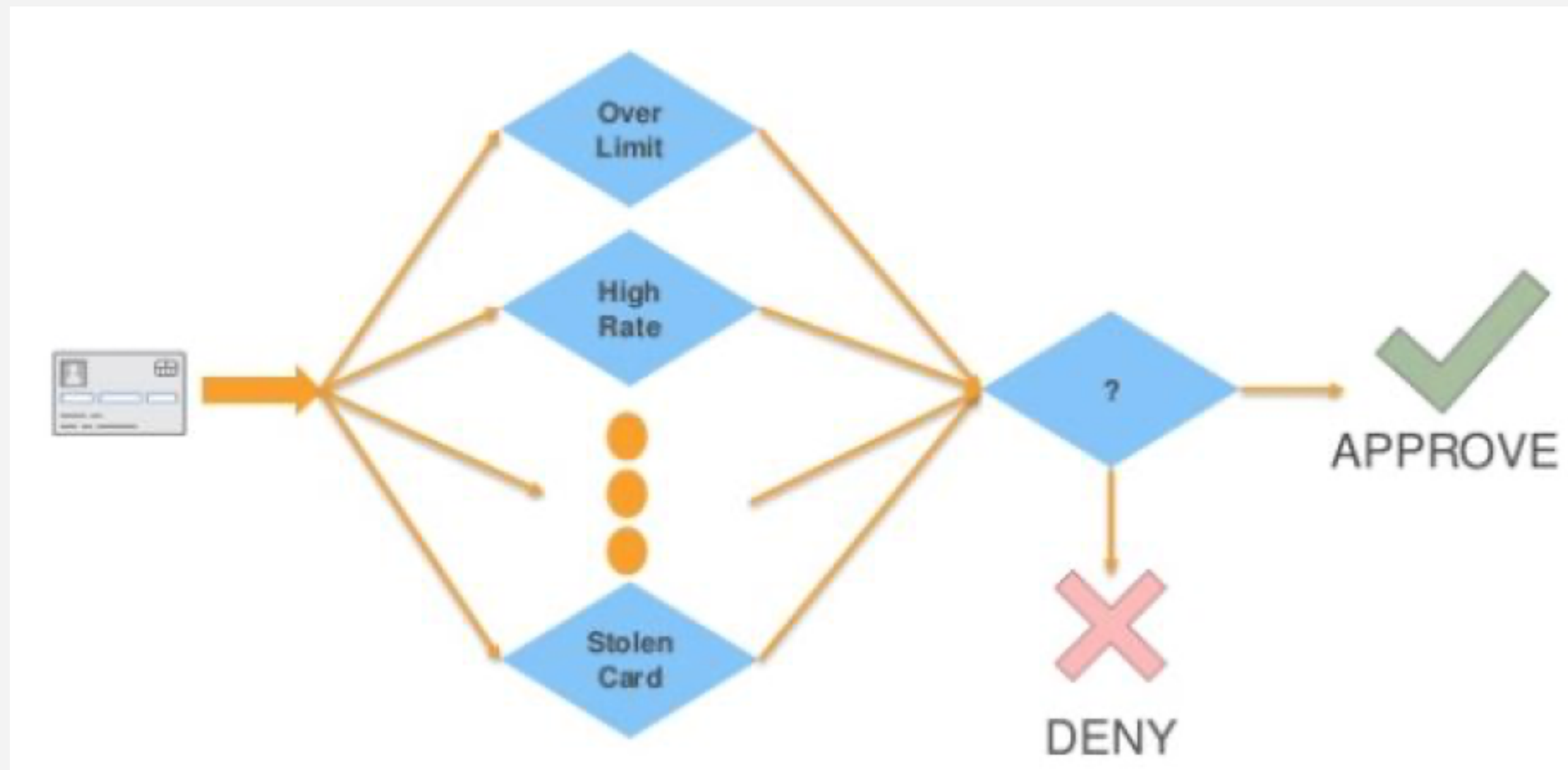
- Data will be collected by combining fraud related in sectors such as credit card, insurance, healthcare, online transaction and e commerce.
- Data Visualisation and Analysing
- Data will be PCA values of original to maintain integrity
- Comparison with the rule based approach using binary outputs and probability in ml based
- Imbalanced data will be sampled
- Important feature will be extracted and standardised
- Model training using algos.
- Evaluation

ROUGH OVERVIEW OF PROTOTYPE

- An app which will allow us to alert us regarding fraud by storing our dataset and deploying it
- We can include admin secure system on the starting of the app such as face recognition to maintain authentication
- The alert message if fraud detected would be sent to the registered user as well as the concerned third parties to take the legible action
- The backend of the app will be integrated with the ML model that will predict whether the new transaction been done is fraudulent or not
- The alert message if fraud detected would be sent to the registered user as well as the concerned third parties to take the legible action

PRINCIPLE

Comparison with Rule based approach



PRINCIPLE

There have been over 300 predefined rule-based approaches to detect fraud. This approach might block transactions risky Block transactions as well as too frequent ones but also generates false positives. They are limited to binary outcomes whether Yes or No and fail to study the correlation between features which emerge in new ways of anomalies. Moreover, they have a fixed threshold per rule and it's difficult to determine the threshold; they don't adapt over time.

Hence to prevent these a new way that is ML based on fraud detection has been developed which not works on the output of binary classifier but rather as a distinguished output, the is probability. Hence the core principle is rather than training through a rule-based approach, we can train it by a machine learning model which we have chosen as a forest autoencoder with high dimensionality deep neural networks.

The data includes the history of not only finances but rather important identity details as well as info exchange data of individuals/Businesses which is highly dimensional. Hence deep learning techniques that as Autoencoder have been performed to scale deeply through details and detect an anomaly. Afterwards, the most effective technique with Gradient boosting has been applied to it to predict the result.

PRINCIPLE

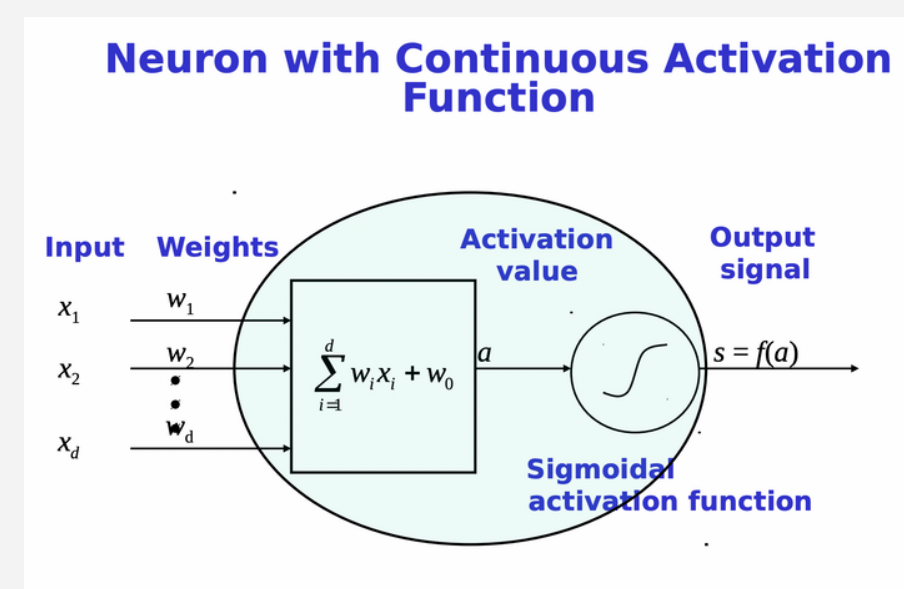
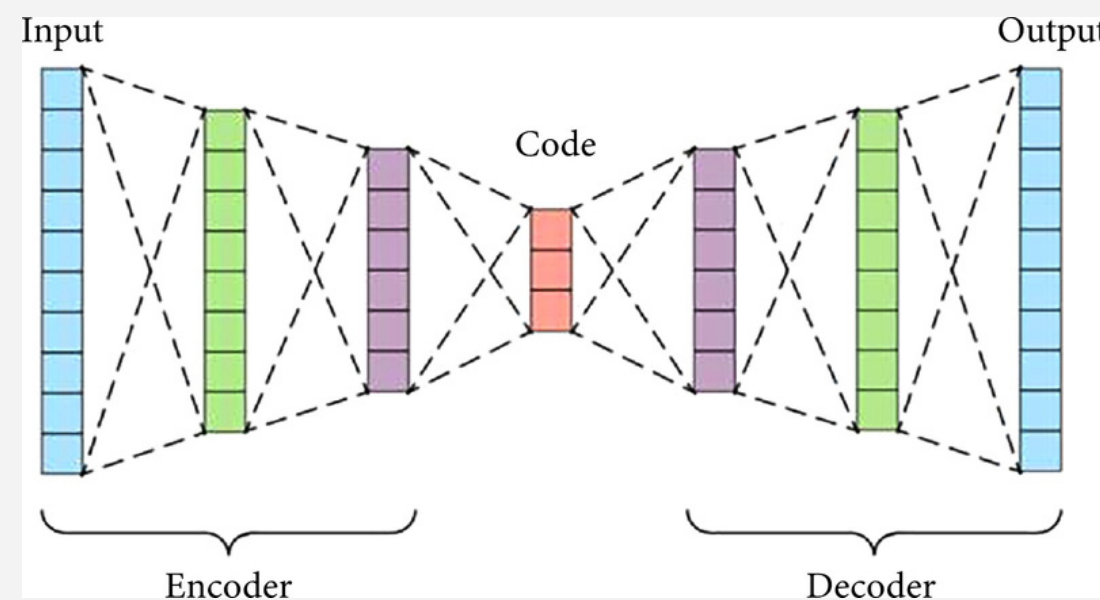
Hence in this way, we extensively reach the accurate result and this also ensures to minimize false negatives and false positives.

In addition to this, we also ensured that the user can only log in to his account and receives notifications hence we have also implemented the face lock security feature in our prototype. Moreover, Individuals don't need to keep track of transactions related to various sectors because data is prepared in such a way that it appoints the common primary key which is the user transaction number of the payment gateway and based on that it foresees every merchant this number had been contacting.

MATHEMATICAL MODEL

Random forest and deep neural networks are two schools of effective classification methods in machine learning. While the random forest is robust irrespective of the data domain, the deep neural network has advantages in handling high dimensional data. Therefore We will combine both random forest and autoencoder to detect fraud.

Autoencoders are a combination of encoders and decoders.



Encoders-It is used to reduce input sizes to a smaller representation.

Decoders-They will recreate it from the compressed data if someone wants the original data

The encoder is simply a function, which maps an input X to a hidden representation z

$$z = f(X) = B = f(A) = a_f(W_m A + b_x), \quad \text{where } W_m \text{ is the Weight, } b \text{ is the bias and } A \text{ is Activation function}$$

Let $g(z)$ be a function that maps the compressed representation z to a prediction y'

$$y' = g(z) = A' = d(B) = a_d(W'_m B + b_y), \quad \text{where } W_m \text{ is the Weight, } b \text{ is the bias and } A \text{ is Activation function}$$

MATHEMATICAL MODEL

Then we will find out the reconstruction error which minimizes the loss of reconstruction on the given dataset X and the objective

For linear reconstruction, the reconstruction loss ($L1$) is generally from the squared error

$$L(X, y) = ||X - g(f(X))||^2$$

Taking a summation of every feature in the input dataset and computing the total reconstruction error

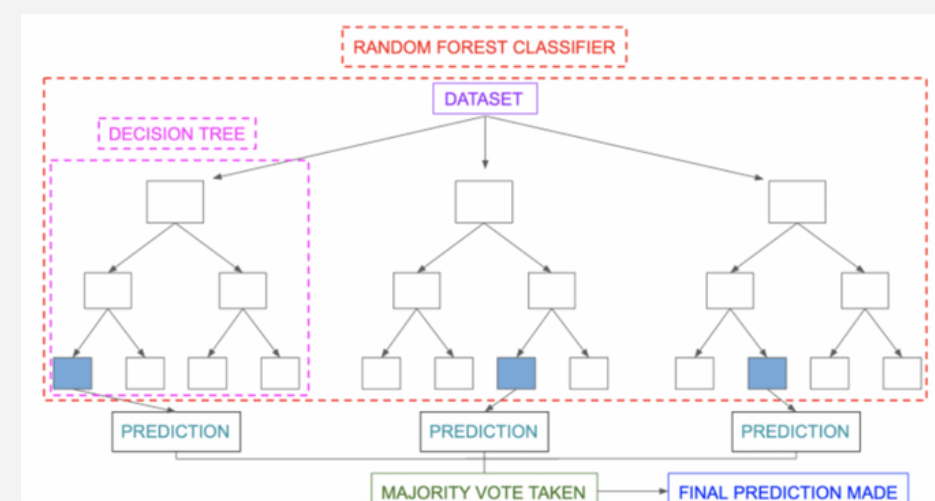
$$L(D) = (1/N) * \text{summation}\{x \text{ in } X\}(L(x, g(f(x))))$$

where N is the number of instances in D .

After training the encoder model we can use the compressed representations Z to be trained under Random forest to predict the target variable

$$y' = h(Z)$$

Random forest algorithm works through Decision Trees. Decision trees use a flowchart-like tree structure to show the predictions that result from a series of feature-based splits. It starts with a root node and ends with a decision made by leaves. It consists of 3 components which are the root node, decision node, and leaf node. The node from where the population starts dividing is called a root node. The nodes we get after splitting a root node are called decision nodes and the node where further splitting is not possible is called a leaf node



MATHEMATICAL MODEL

To select the root node in a random forest, we will use Gini Index which helps us to know how much impurity this particular node has

$$\begin{aligned} \text{Gini Index} &= 1 - \sum_{i=1}^n (P_i)^2 \\ &= 1 - [(P_+)^2 + (P_-)^2] \end{aligned}$$

The training process for the random forest involves minimizing the following objective function:

$$O(D) = \text{summation}\{X \text{ in } D\} L(y, h(Z))$$

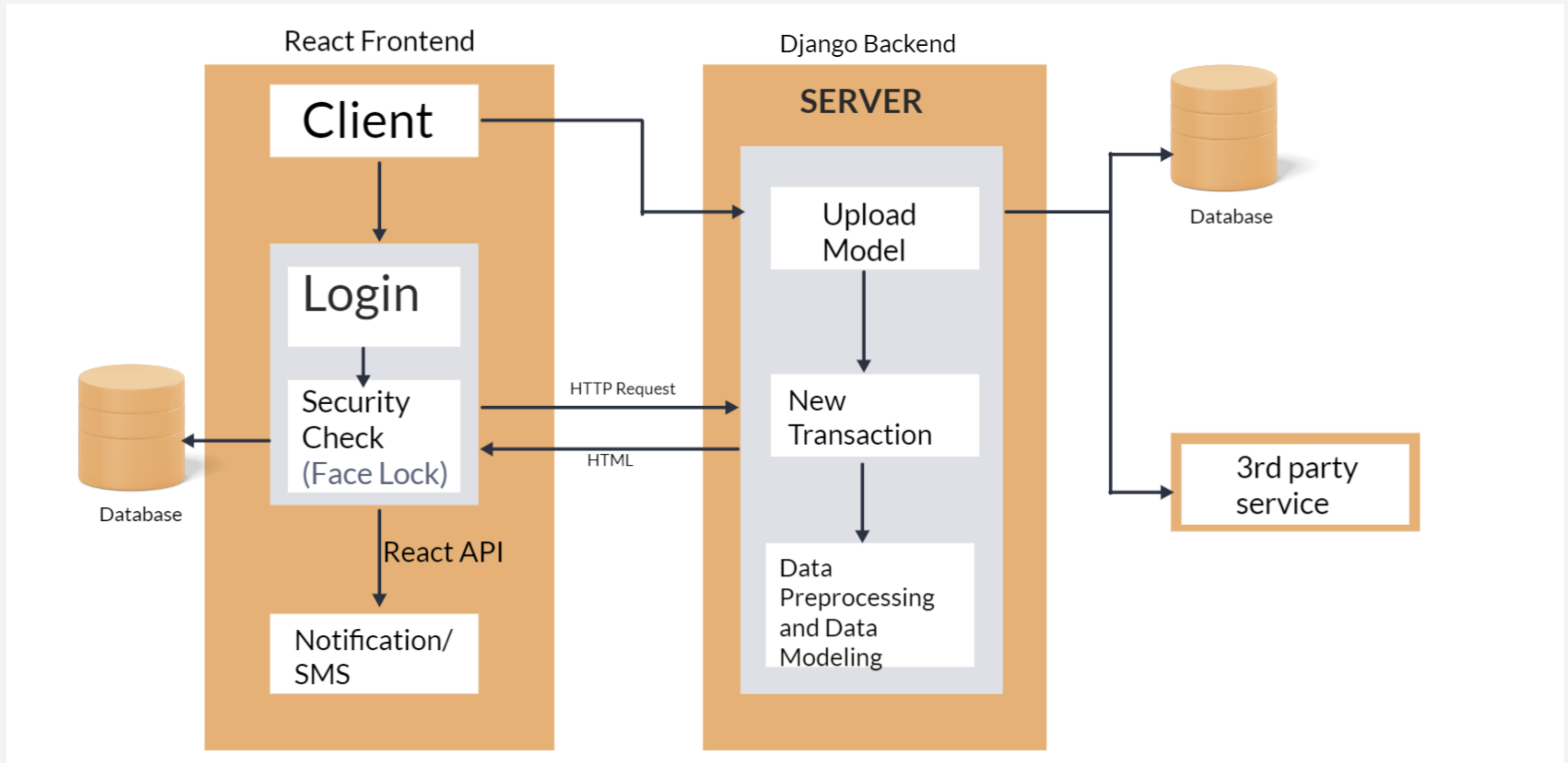
where L is the loss function used to measure the error between the predicted values and the actual values.

The overall objective of the combined model is to minimize the following function:

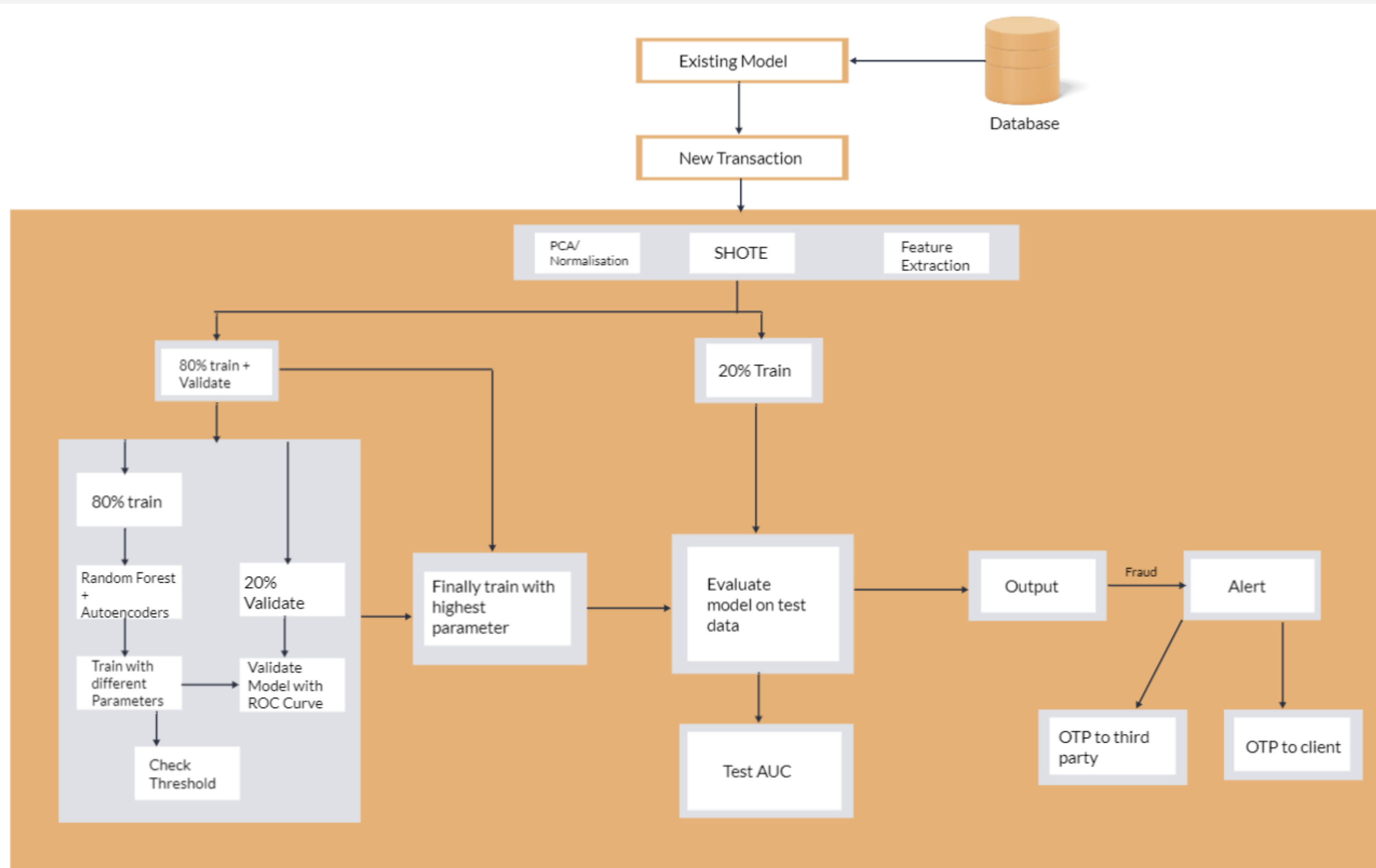
$$J(D) = L(D) + O(D)$$

where $L(D)$ is the reconstruction error of the autoencoder and $O(D)$ is the error of the random forest.

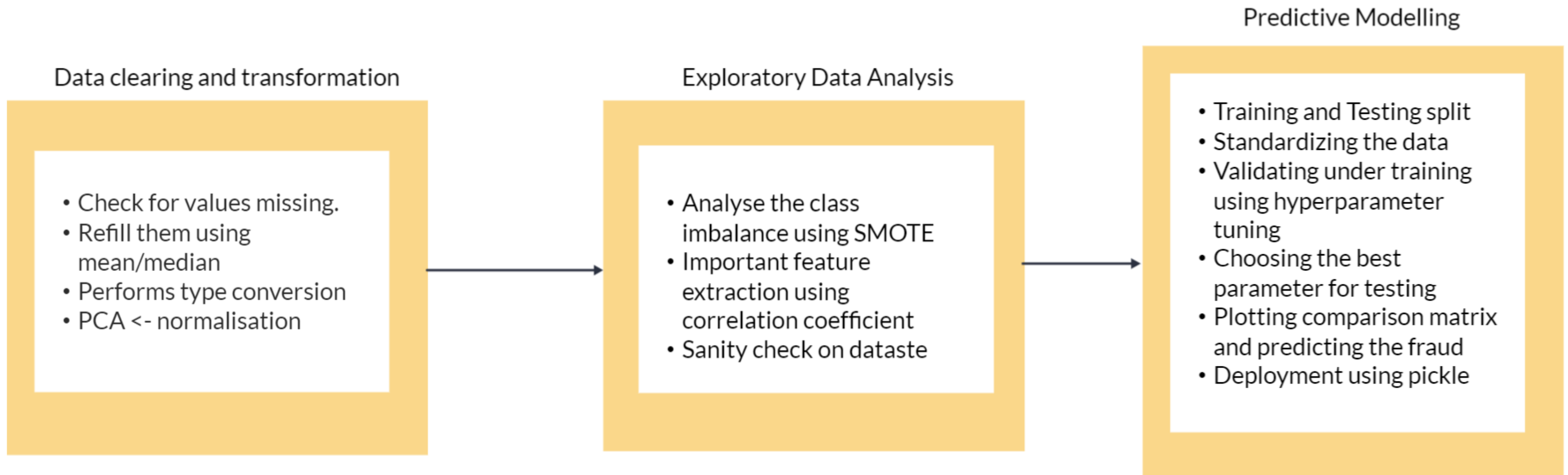
ARCHITECTURAL DESIGN



THE BACKEND OF ML MODEL



ANALYSIS OF ML MODEL



WIREFRAME

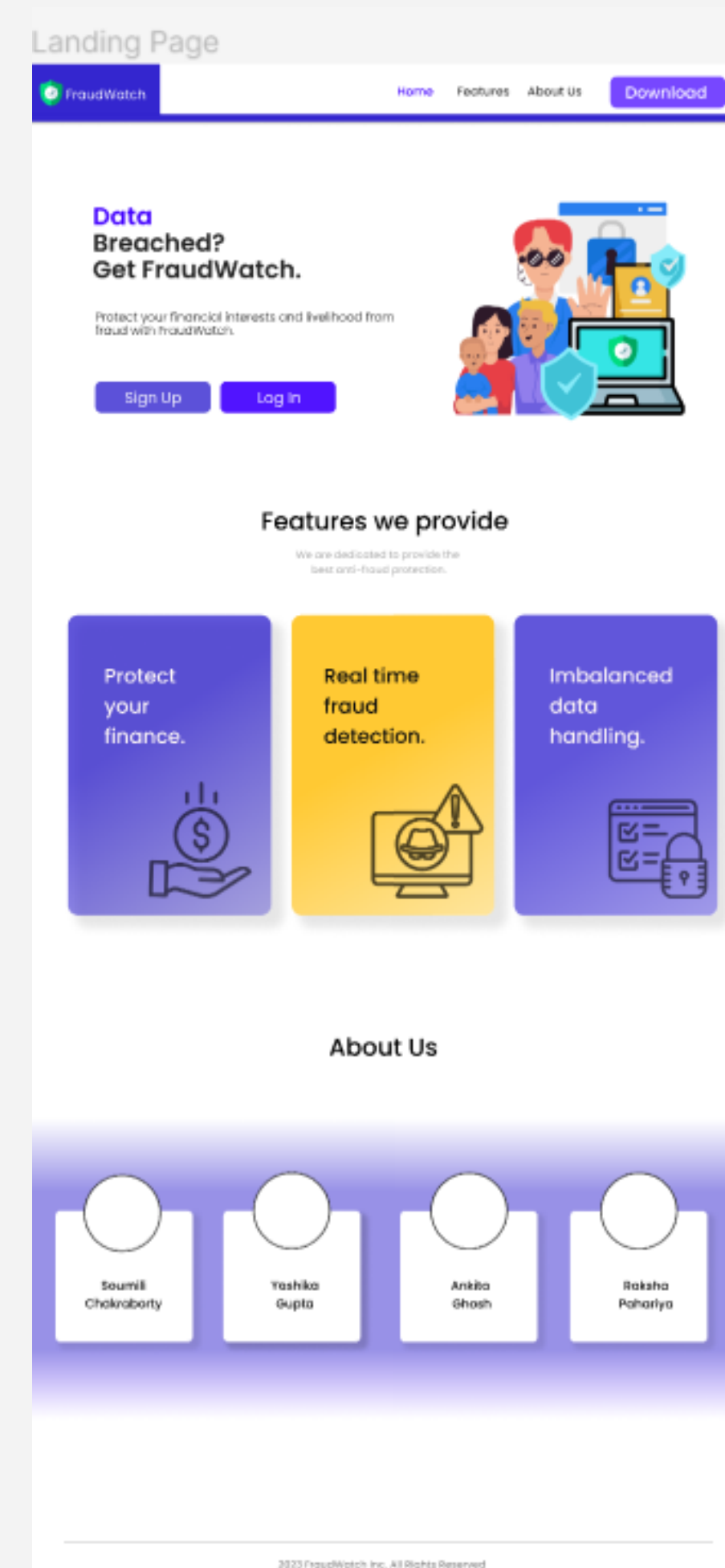
Complete wireframe figma link- [FraudWatch](#)

The wireframe for the ML based Fraud Detection system is as follows-

1. Landing Page:

The landing page of FraudWatch has been created to introduce the application.

It showcases the features of the application and provides a sign up and log in button for the users. It also has a download button which allows the users to download the application. The landing page also contains an About Us section with details of the team members.



WIREFRAME

2. Login/ Sign up Screen:

Every new user has to set up an account on FraudWatch using the sign up page. They need to enter their details and click on continue for creating their account. If a user already has an account he/she should click on the Login button at the bottom of the page and enter their credentials to access the application.

3. Dashboard:


Once logged in, users will see the dashboard, which will provide an overview of the frauds detected. The dashboard includes a graph that shows the number of fraud cases detected. It also displays alert messages when fraudulent activities are detected. A log of all the alert messages is also present in the dashboard.

Sign/Login Page

9:41

←

Protect your finance right now.



Sign Up

Email

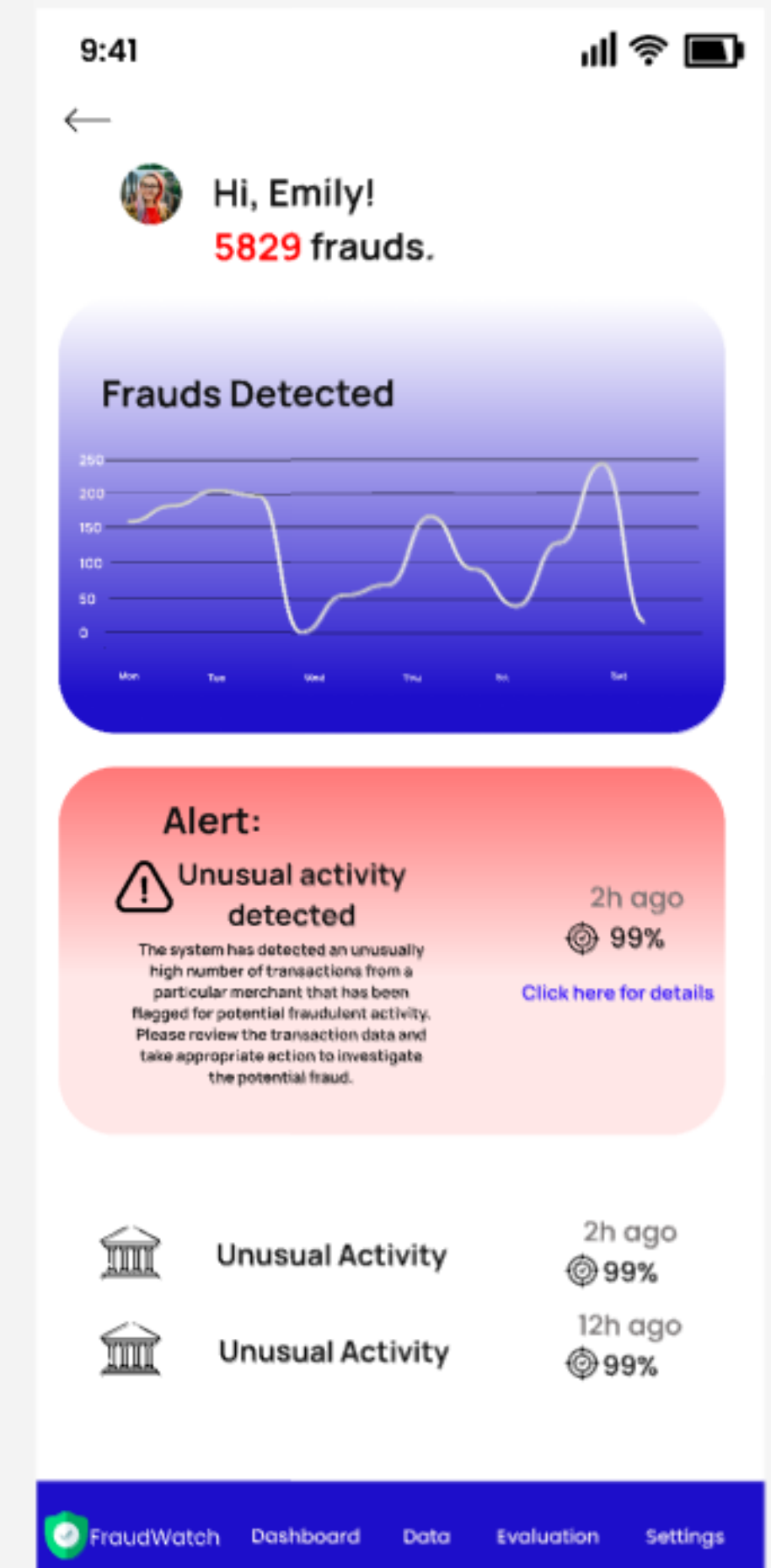
Name

Mobile

Continue

Joined us before? [Login](#)

Dashboard

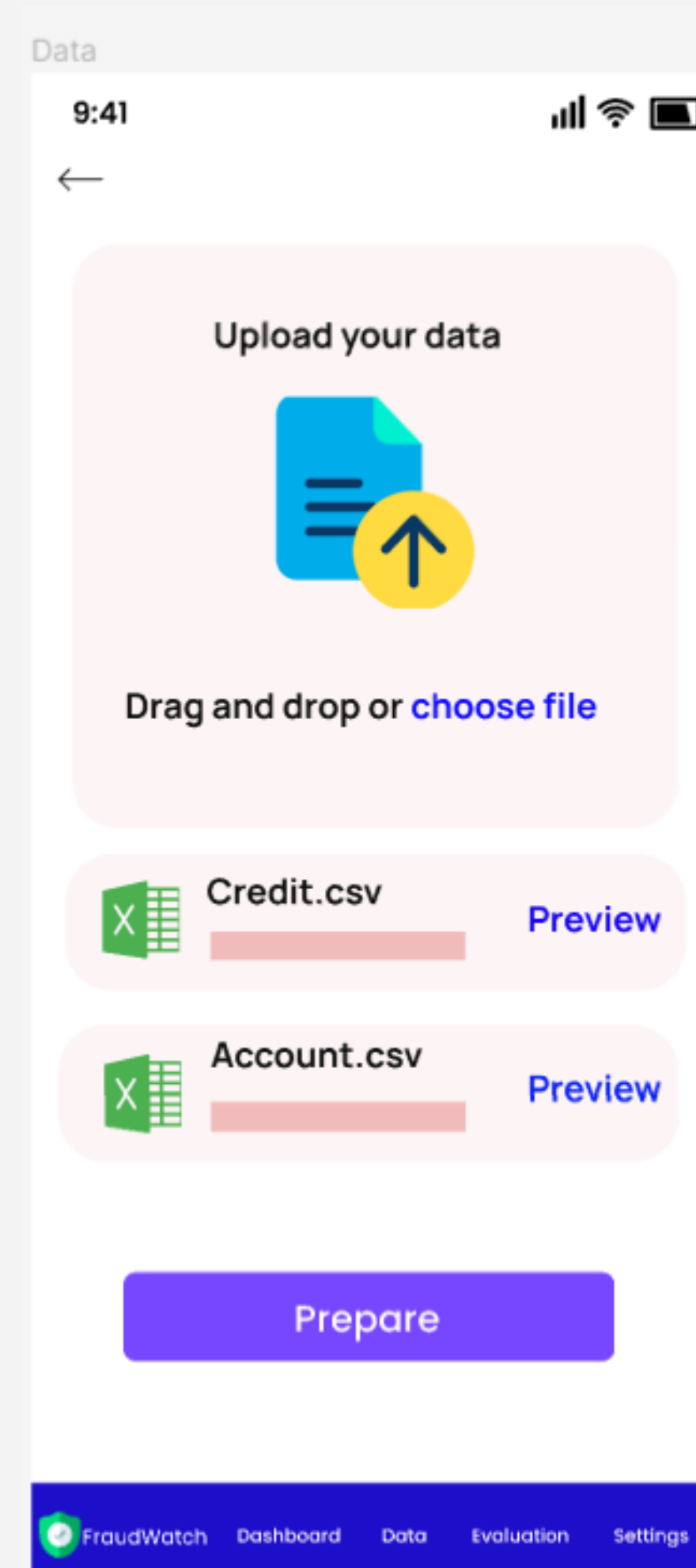


WIREFRAME

4. Data:

The data page can be accessed from the taskbar below the dashboard. This page contains the following operations-

1. Data Collection: The screen will allow users to collect data for the model. Users will be able to upload data in various formats, including CSV files and database queries. Users will also be able to preview the uploaded data.
2. Data Preparation: Once the data is uploaded the users can click on Prepare and they can select features to include or exclude, convert data types, and handle missing data.
3. Imbalanced Data Handling: The screen will also enable users to handle imbalanced data while training the model. Users can choose to oversample, undersample, or use other techniques to balance the data.



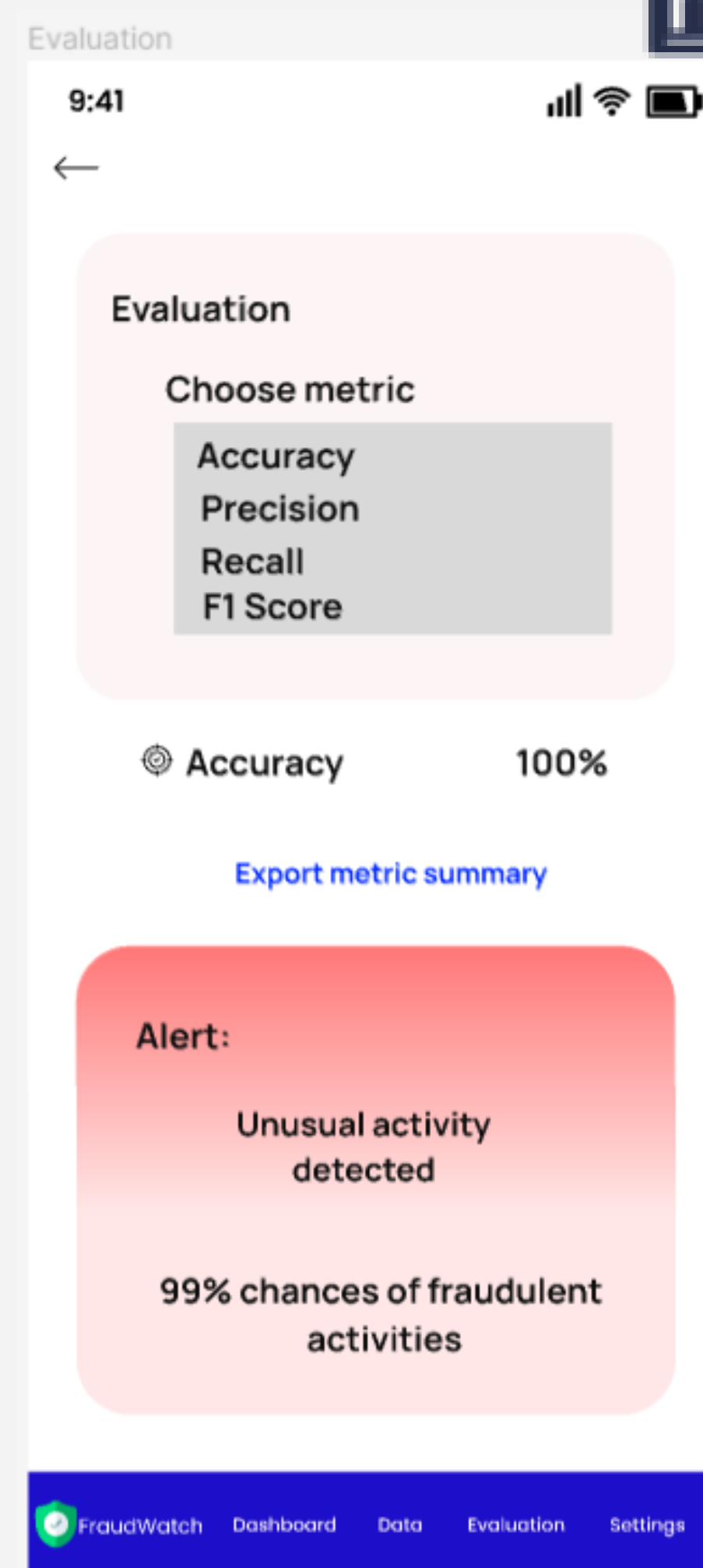
WIREFRAME

5. Evaluation:

This screen will provide users with metrics to evaluate the model's performance. Users can view metrics such as accuracy, precision, recall, F1 score, and confusion matrix. When the model detects fraud, it should generate an alert to notify users. Users can receive alerts via email, SMS, or other communication channels.

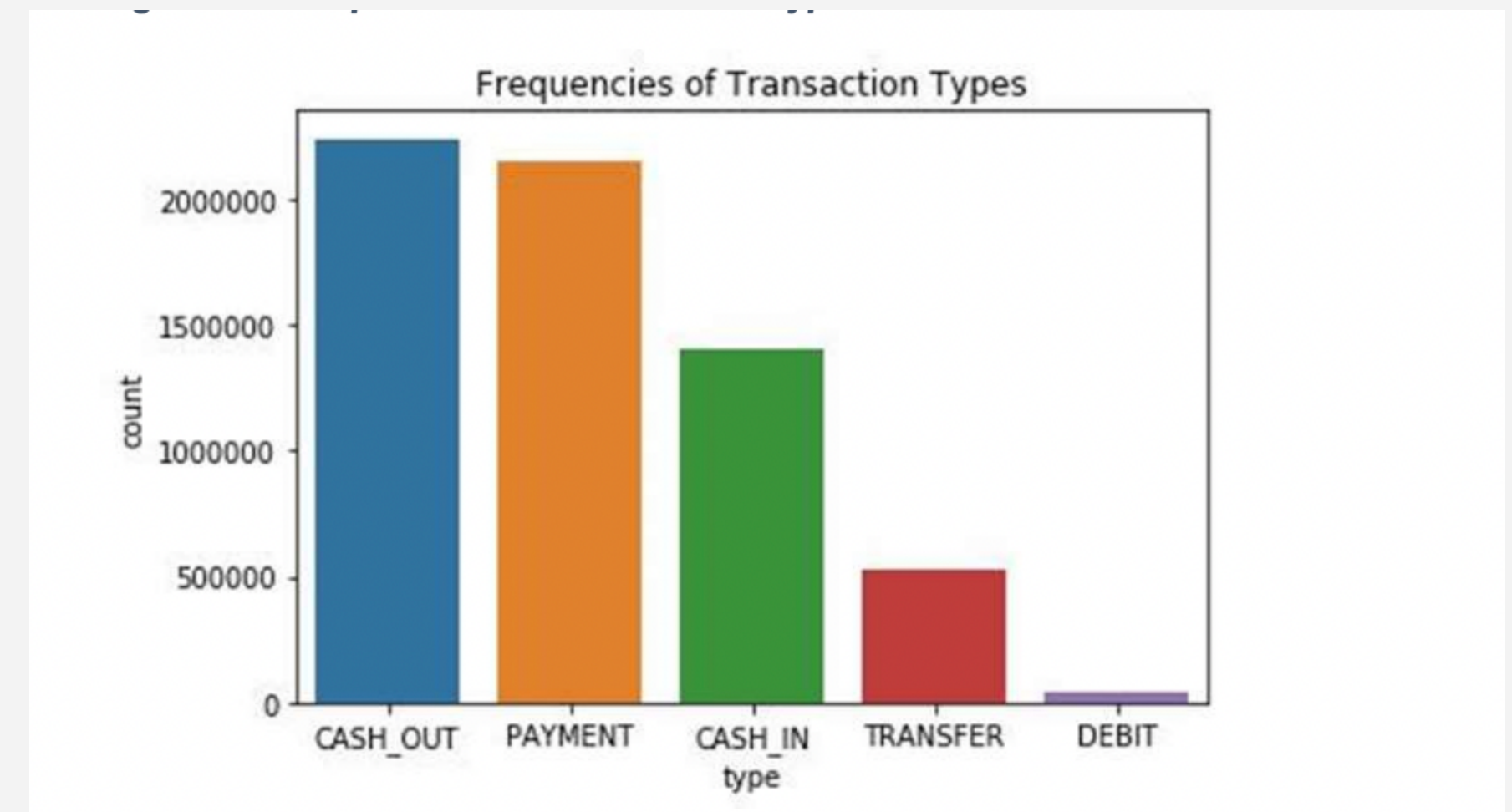
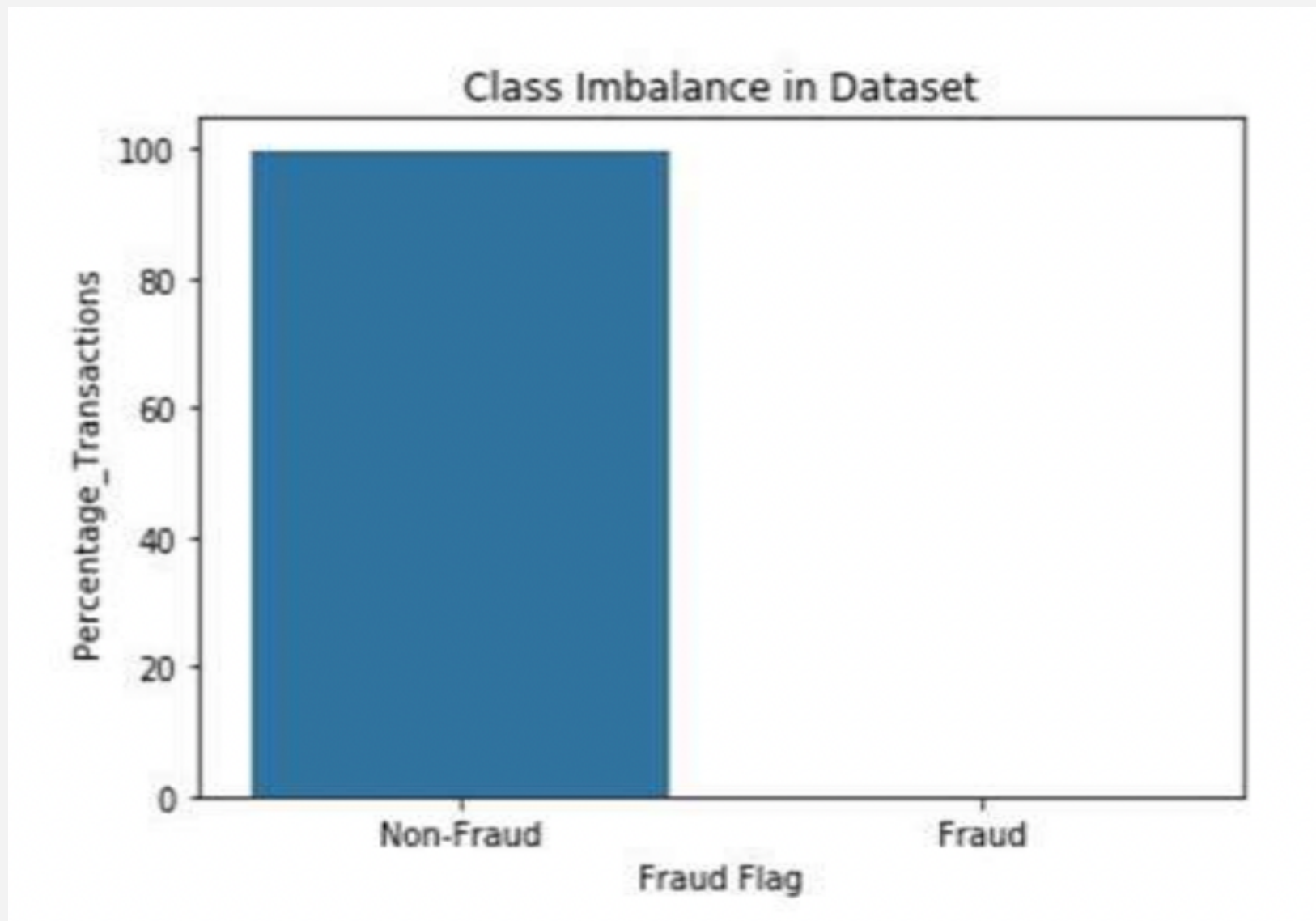
6. Settings:

The settings screen will allow users to customize the system's configuration, such as selecting notification channels, changing model parameters, and setting up user permissions.

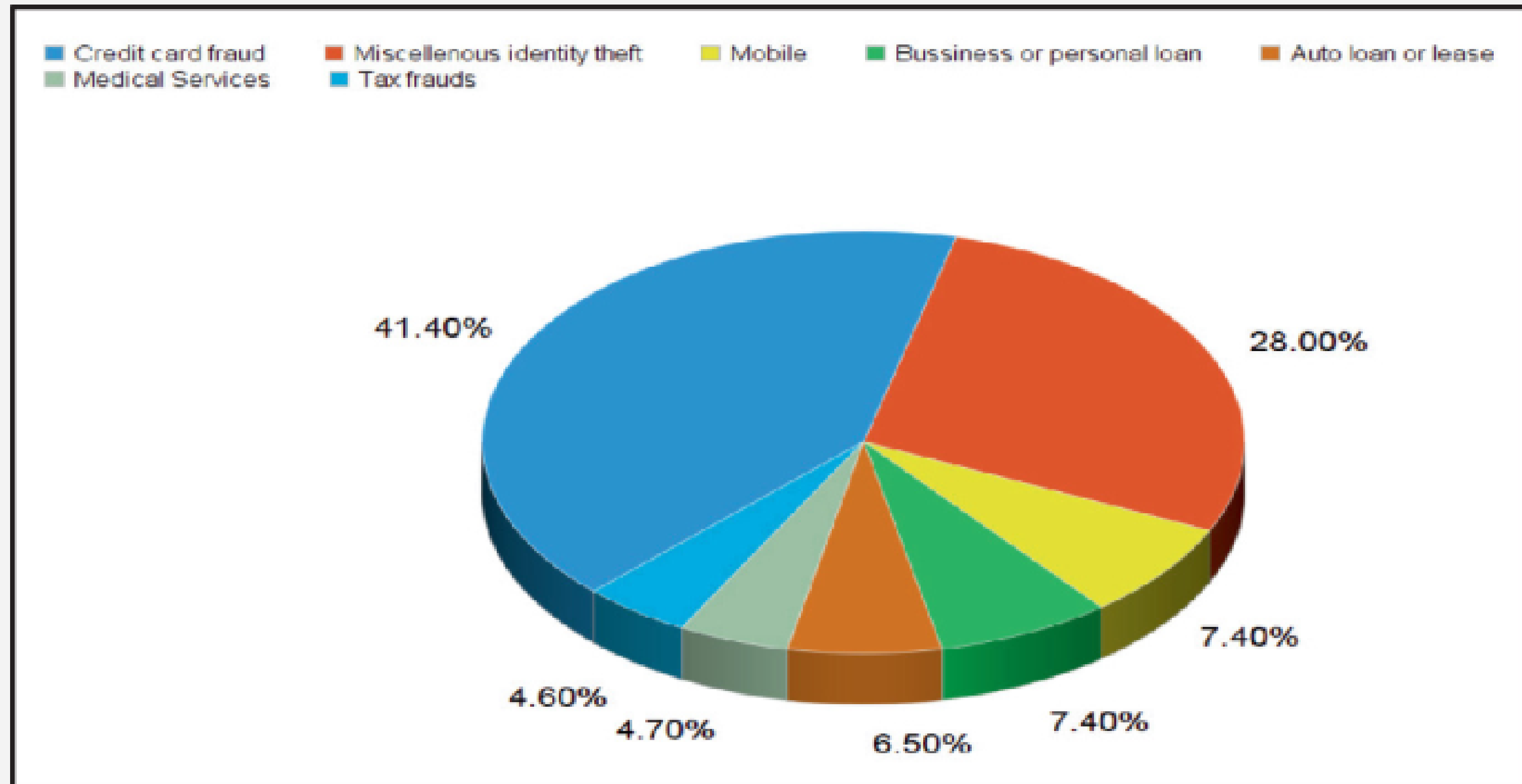


GRAPHICAL REPRESENTATION

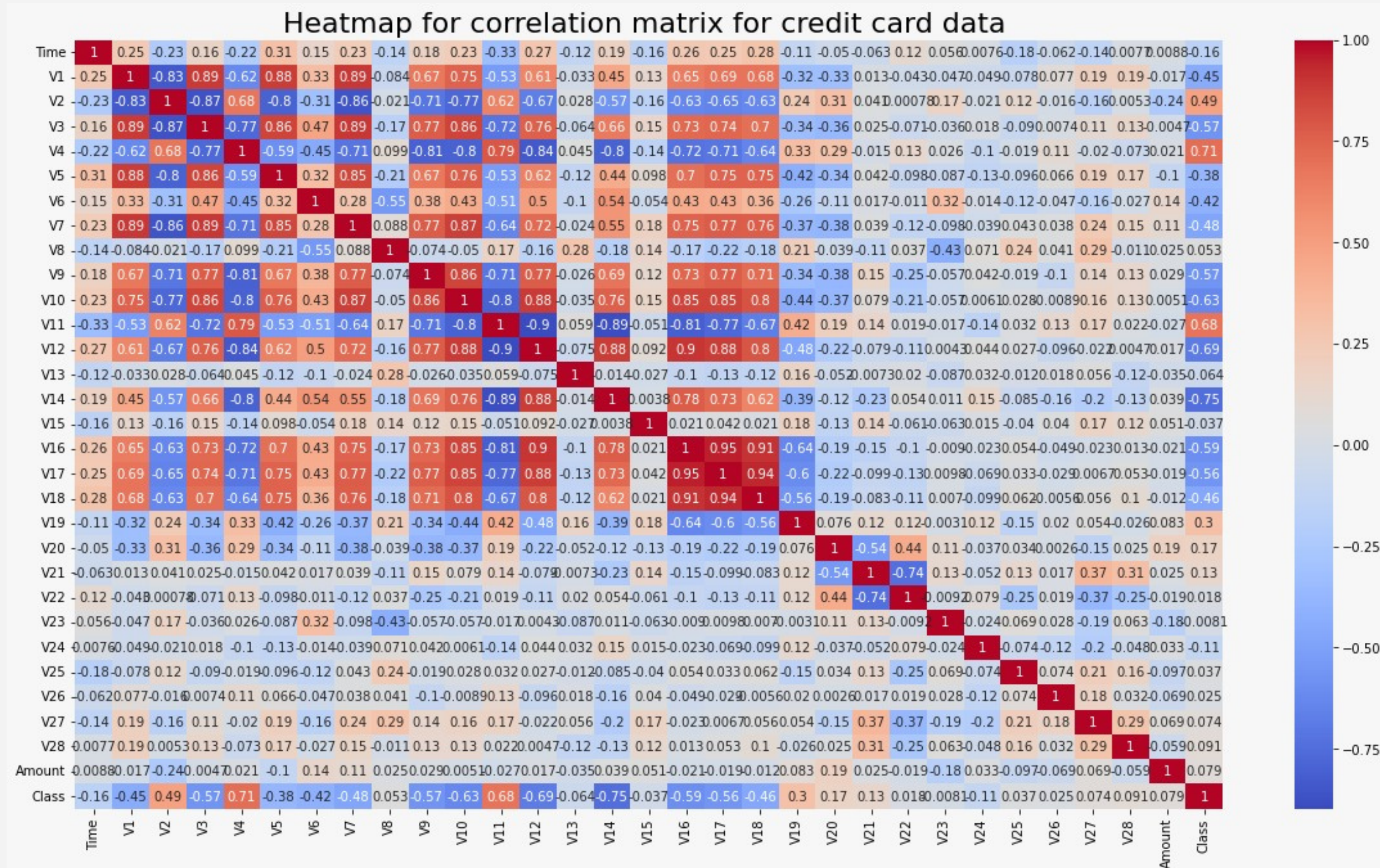
On a given set of data



GRAPHICAL REPRESENTATION



GRAPHICAL REPRESENTATION

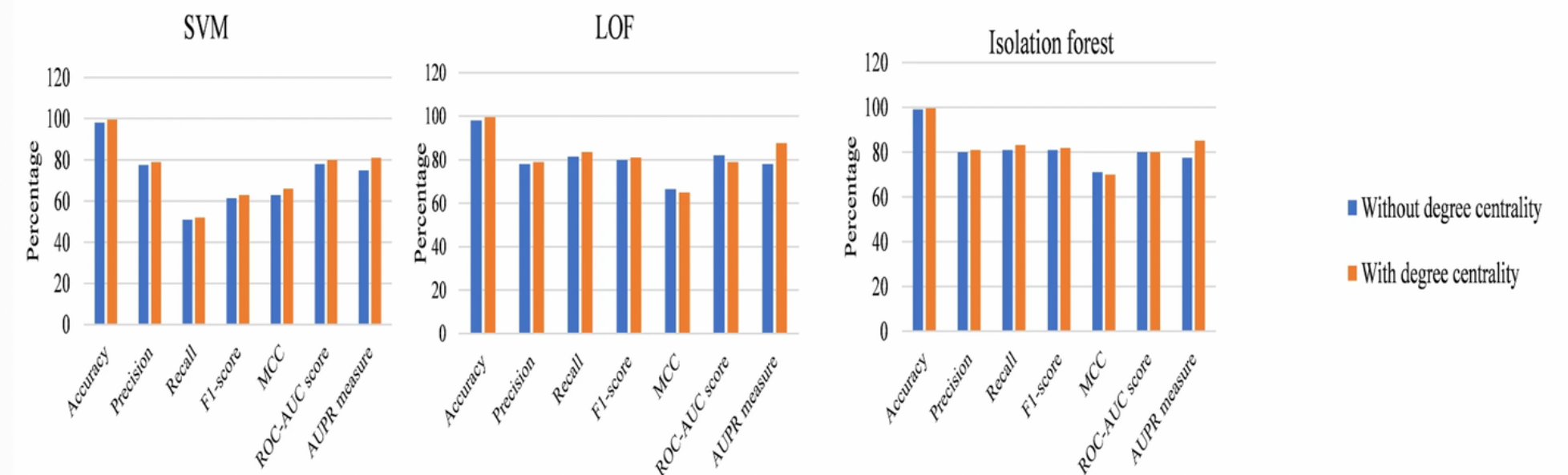
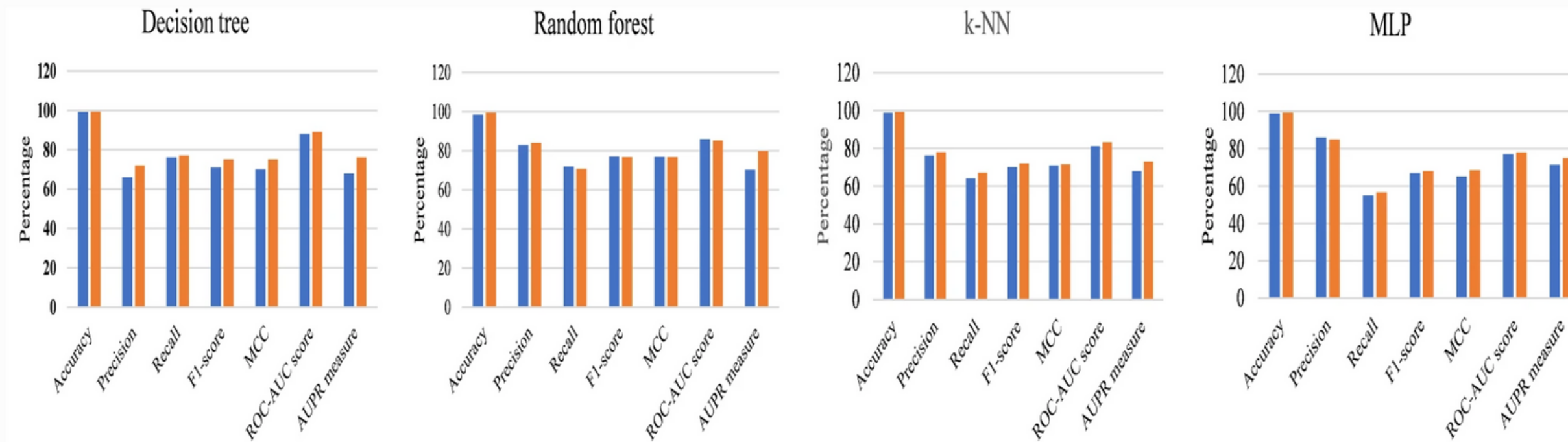


GRAPHICAL REPRESENTATION

From here we can conclude that the accuracy of the random forest classifier is more than other ML algorithms.

Machine learning	Methods	Accuracy	Precision	Recall	usage frequency	References	advantages	disadvantages
Supervised Learning	Neural Network	98.69	98.41	98.98	17	[4,17,19,20,32,36,38,52,53,54,55,56,57,72,75,78,82]	Highly accurate and reliable	Need to understand and label the input More computation time required for the training phase
	Support Vector Machine	93.96	93.22	93.00	20	[21,33,38,39,53,59,61,62,63,64,65,66,67,68,69,70,71,74,75,78]		
	Bayesian Network Classifiers	91.62	97.09	84.82	21	[20,21,35,39,42,47,55,56,58,59,61,64,66,67,73,74,78,80,82,87,93]		
	K-Nearest Neighbor	94.99	94.58	92.00	6	[39,64,67,73,81,82]		
	Logistic Regression	94.84	97.58	92.00	21	[21,33,36,39,42,52,53,55,59,61,63,64,66,71,73,74,75,82,83,84,85]		
	Decision Tree	92.88	99.48	86.34	21	[20,21,33,35,39,51,52,53,55,59,63,64,66,69,73,74,75,82,83,84,85]		
Unsupervised Learning	Expectation-Maximization				1	[58]	Easy to find unknown patterns	Computationally complex Less accurate
	K-Means				3	[14,58,64]		
Ensemble Learning	Random Forest	99.96	96.38	81.63	32	[13,18,21,22,23,35,36,37,38,39,42,45,51,52,53,54,59,61,63,65,66,67,69,71,72,78,81,82,84,85,91,93]	Avoid the overfitting problem and gives better predictions when compared with a single model	Computation time is high Reduces model interpretability due to increased complexity
	Boosting				7	[53,65,69,70,71,82,92]		
	Bagging				3	[64,93,64]		
	Voting				1	[10,21]		

GRAPHICAL REPRESENTATION



Comparative analysis of performance metrics of different machine learning classification models with and without consideration of degree centrality graph features

SOCIETAL IMPACT/ NOVELTY

The societal impact of this proposed app is significant, as fraud detection and prevention is a critical issue in today's digital world. By providing a user-friendly and accessible tool for fraud detection, the app can help protect individuals and businesses from financial losses and reputational damage. Additionally, the app's ability to quickly notify authorities can help prevent fraudulent activity from continuing and increase the chances of apprehending perpetrators.

The novelty of this app lies in its use of advanced machine learning algorithms, specifically autoencoders, to identify fraud patterns in real-time. This allows for more efficient and effective detection of fraudulent activity, reducing the need for manual updates to the detection system. Furthermore, the app's user-friendly interface and state-of-the-art encryption and security protocols make it a unique and valuable tool for fraud prevention.

FUTURE SCOPE

Business relevance

- From the business point of view, it can become the relevant model to not only predict the fraud transaction but a one in all platform to carry transactions and detect spam and frauds connecting financial and social accounts.
- For this relatively highly efficient data collection techniques will be required.
- It can be merged with the already giant fintech company American Express.

OPTIMISATION AND MODIFICATION

- The very foremost thing we are thinking of is merging gradient boosting with our forest encoders.
- Generating non-linear loss function and reconstruction error.
- Further segregating the system into individuals and businesses so that frauds can be studied and features can be correlated more effectively.
- Making a few changes in the prototype and giving it First Time User Privilege.
- Incorporating digital wallets in our prototype.



Thank You

