Round 2

Phase 2 – Proof Of Concept

Defined Deliverables	Sample
Detailed Use Case selected for POC	We aim to analyze the data of transactions (Cash-In, Cash-Out etcetera) which comprises both normal as well as fraud customer behavior. With the help of machine learning techniques the classification model shall accurately classify transactions as genuine or fraud.
Solution Design and Architecture  Use_Case_Architecture	The transactions are monitored for types which cause major frauds. Based on the obtained categories, we monitor the zero balance accounts specifically as they showed more frauds even after transactions between senders' and receivers'. Feature engineering is applied to record errors in the senders' and receivers' accounts for each transaction. Visualization of frauds are made based on factors like time and amount and even separating out genuine and fraudulent transactions. Techniques like AUPRC, Confusion matrix and Precision and Recall are used to make the model predict more accurately. Bias-variance tradeoff technique is used to avoid the model from becoming underfit.
Logical Data Model  Logical Data Model	Sample Data Model
Test Data Set Availability with Test Result  Test_Case.xlsx	The test dataset consists of over 6.3 million rows in csv. It gives details about according to the account type how much is the balance amount. Later it gives specific details about the current and after transaction balance of the source and destination accounts. Then it gives a binary classification of whether fraud exists or not and accordingly flags it.
Installation & Execution Guide	Step by step guide to run the submitted proof of concept.

Detailed Business Case

- Frauds in online transactions are seen in abundance.
- Studies suggest 93% of the merchants perform manual review.
- We aim to analyze the data of transactions, which comprises both normal as well as fraud customer behavior.
- Classification model shall accurately classify transactions as genuine or fraud.
- Businesses using the solution will in turn endup saving a lot of resources.

Detailed Business Model

Key Partners

Key Partners
> Financial Service providers
> Ministry of finance
> Small and Large scale organisations
> Banks

Key Supplier
> Employees
> Customers
> Companies using online transaction methods

Key Activities

> Real time notification against fraud
> Deriving insights from past incidences
> Identifying fraud / unusual activities
> Analysing customer behavior

Key Resources

> Past data of general and fraud transactions
> User activity analysis
> Feedback

Value Propositions

> Real time notification against fraud
> Notification of unusual activity
> Reduction of false negatives through feedback
> Better insights to activity

Customer Relationships

> Bank activity
> Wallet activity
> Identifying false negatives
> Unusual activity / Fraud detection

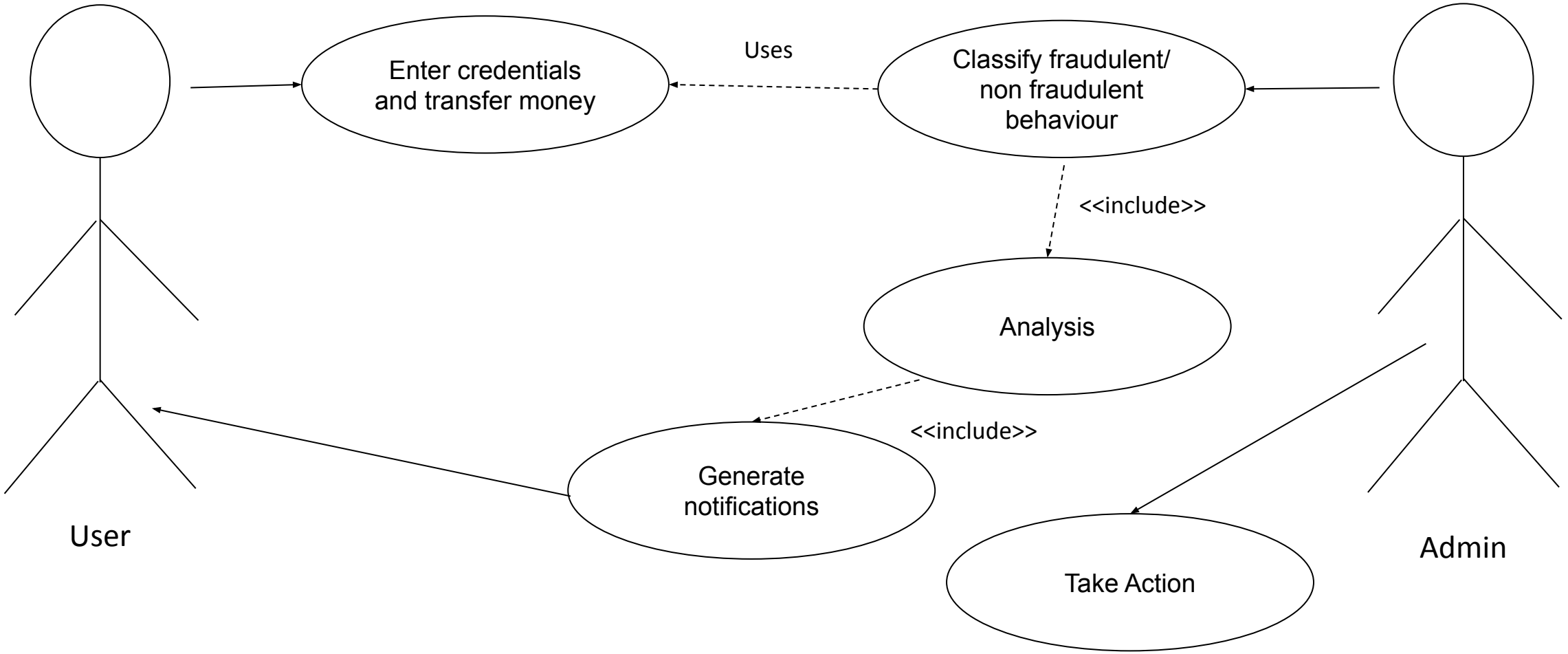
Channels

All online transaction portals including wallet and other transactions

Customer Segments

Banks
Financial Institution
Users / Customers

Detailed Use Case



Solution, Design and Architecture