SIEM-Driven Financial Fraud Detection

Phase II

Under the Guidance of Mr. V Damodaran

Presented by Group B12 of CSB Semester 8

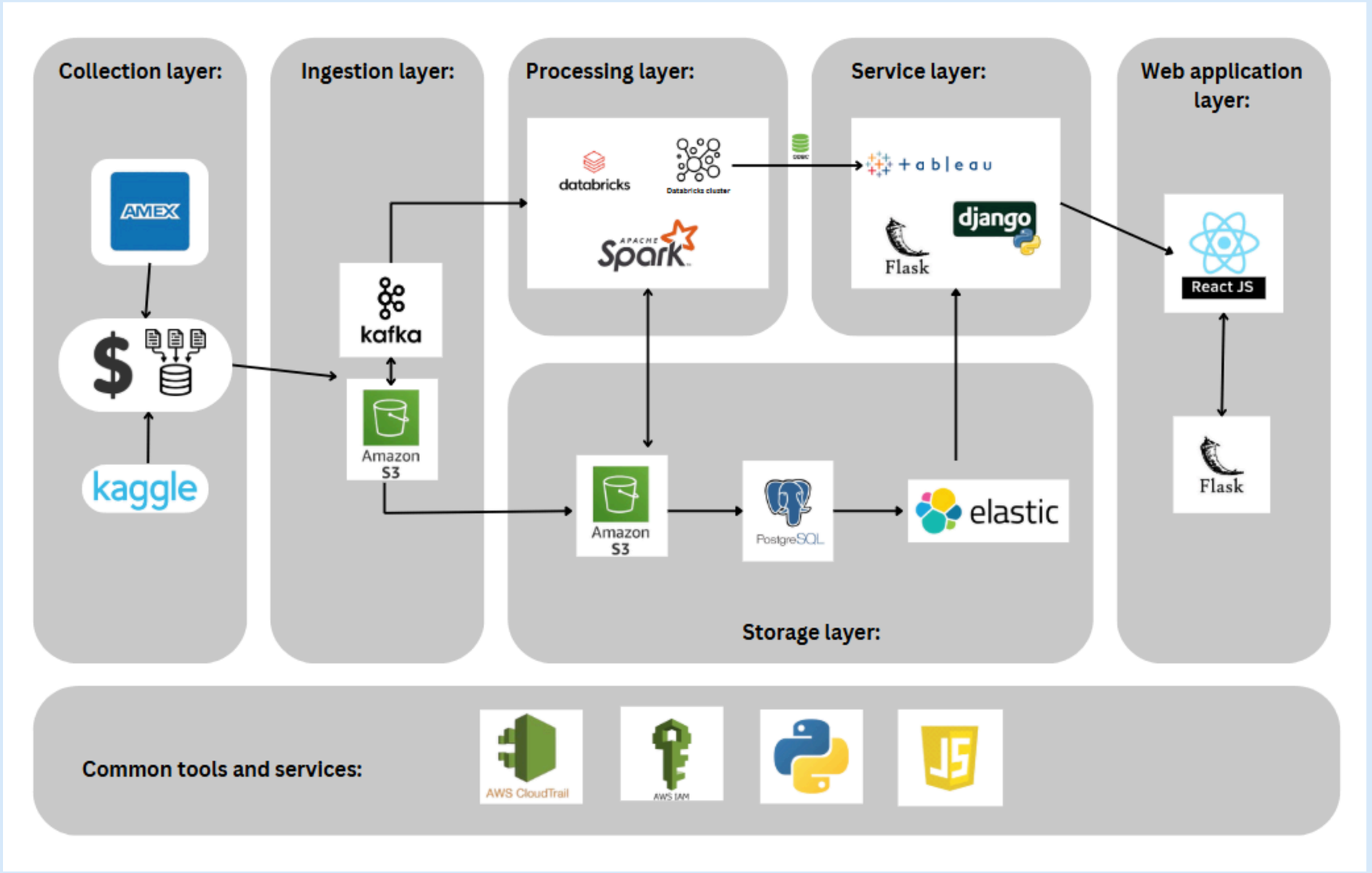
Contents

Introduction

This project focuses on developing a

- Scalable Security Information and Event Management (SIEM) system
- Designed for Real-time detection of financial fraud and anomalies.
- Using advanced machine learning and Threat Intelligence, the system processes millions of events per second for swift detection and response.
- Its cloud-native design integrates with financial platforms and blockchain networks, ensuring robust fraud detection and prevention.

System Architecture



PROJECT PHASES

Over the course of December and January, four phases of development have been planned to produce a comprehensive and competent financial fraud detection system. Once complete, this system serves as a robust detection and warning system for end users, financial entities like banks, brokers and credit line monitors.

PHASE NAME	MODULE	ACTIONS
PHASE 1	INGESTION AND CLEANING OF DATA	• Identify and find optimal datasets for the project. • Preprocess and prepare the data as per requirements
PHASE 2	AI LOGIC AND API ENDPOINT DESIGN	• Conduct thorough research on plausible AI algorithms and models. • Using flask prepare API
PHASE 3	SIEM IMPLEMENTATION AND VISUALISATION	• Integrate real time learning for selected AI algorithms. • Tableau Visualisation
PHASE 4	FRONT END DEVELOPMENT	• Generate React/Flutter web app for various endpoints. • API and network monitoring Dashboard

PROJECT PROGRESS

Since commencement of project development phase in December, the team has progressed at a steady pace and completed two of the four planned phases.
Due to the dependancy of each phase on the prior phases, parallel execution of phases is not feasible.
Data ingestion and three-tier preprocessing completed.
AI algorithm research and development completed

21

MODELS BUILT UNDER RESEARCH

5+

Papers researched as part of literature review

PHASE 1

PHASE 2

DATASET OVERVIEW

Several sources have been used for provision of valuable data for training the fraud detection models.
To ensure accuracy and authencity of the model, the main backbone of the data used is actual scrapped data from reputed international banks.
Several fraudulent practises and popular scam data have been added to the datasets synthetically using various data synthesis techniques like SMOTE and ADASYN.
Kaggle datasets also implemented for a more robust fraud detection dataset.

"Give me six hours to chop down a tree and I will spend the first four sharpening the axe." - Abraham Lincoln

CREDIT CARD FRAUD DET.	XGBoost ML model
BANK DEPOSIT FRAUD DET.	XGBoost with Hypertuning and SMOTE
BANK TRANSFERS FRAUD DET.	Gradient Boosting Model with GridSearch and Feature Engineering
BANK DEVICE MONITORING	XGBoost Model with Hypertuning, Grid Search CV and ADASYN
SWIFT TRANSACTIONS	JP Morgan and Chase proprietary QuantGant Neural Network model

Models researched

Next Step

Maintaining the speed and momentum of the project development, the team plans on executing the given steps to complete and deliver the product in the stipulated time. Due to reduction in dependancies and restrictions in the upcoming phases, more parallelism can be implemented into development and several sub phases be executed simultaneously.

COMPLETION AND REFINING

Complete execution of phase 2 with refining and packaging of the Flask API endpoints. Also refine models for efficient execution.

COMMENCEMENT OF PHASE 3

The Backend team will begin implementing SIEM ideology over the existing framework while the frontend team works on visualisation

SYSTEM INTEGRATION

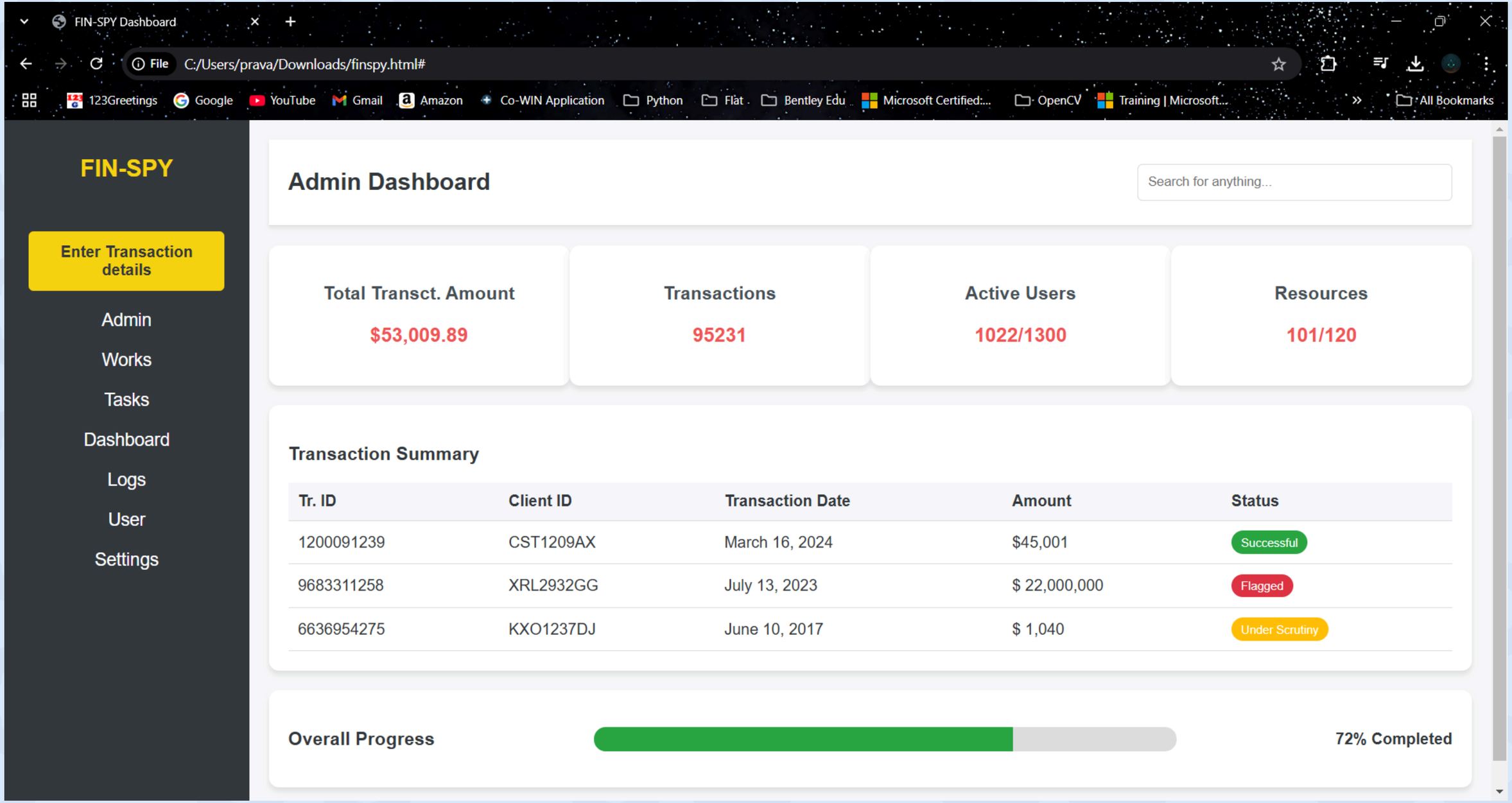
Combining the completed backend AI logic framework with the Flask API to prepare the backend module.

FRONT END DESIGN

Front end team will develop the front end based on the figma design frames already prepared. Backend team will work on integration of logic and tableau graphs to front end.

Demonstration of working API endpoint and ML integration

Followed by Figma Design Frames for envisioned front end


FIN-SPY Dashboard
File C:/Users/prava/Downloads/finspy.html#
123Greetings Google YouTube Gmail Amazon Co-WIN Application Python Flat Bentley Edu Microsoft Certified:... OpenCV Training | Microsoft... All Bookmarks
FIN-SPY
Enter Transaction details
Admin
Works
Tasks
Dashboard
Logs
User
Settings
Admin Dashboard
Search for anything...
Total Transct. Amount
$53,009.89
Transactions
95231
Active Users
1022/1300
Resources
101/120
Transaction Summary
Tr. ID Client ID Transaction Date Amount Status
1200091239 CST1209AX March 16, 2024 $45,001 Successful
9683311258 XRL2932GG July 13, 2023 $ 22,000,000 Flagged
6636954275 KXO1237DJ June 10, 2017 $ 1,040 Under Scrutiny
Overall Progress
72% Completed

Activities Brave Web Browser Jan 17 09:49 94 %

Admin Dashboard | JSON TRX MIN | 127.0.0.1:5000/admin | ChatGPT | New Tab

File /home/nlk/Documents/FinSpy_v1/admin-dash.html

Admin Dashboard

Error loading transactions.

Fraud vs Legitimate

Transaction Amounts

Category Breakdown

Transactions Table

#	Amount	Category	Merchant	City Population	Latitude	Longitude	Fraud Probability	Non-Fraud Probability	Status
1	$9999.99	luxury_goods	fraud_Cartwright and Sons	8700000	37.7749	-122.4194	62.60%	37.40%	Fraudulent
2	$9999.99	luxury_goods	fraud_Cartwright and Sons	8700000	37.7749	-122.4194	62.60%	37.40%	Fraudulent
3	$199.99	electronics	legit_Adams, Kovacek and Kuhlman	8000000	40.73061	-73.935242	0.00%	100.00%	Legitimate
4	$199.99	electronics	legit_Adams, Kovacek and Kuhlman	8000000	40.73061	-73.935242	0.00%	100.00%	Legitimate
5	$19944.99	electronics	legit_Adams, Kovacek and Kuhlman	8000000	40.73061	-73.935242	1.72%	98.28%	Legitimate
6	$19944.99	electronics	legit_Adams, Kovacek and Kuhlman	560870	40.73061	-73.935242	5.41%	94.59%	Legitimate
7	$9999.99	luxury_goods	fraud_Cartwright and Sons	8700000	37.7749	-122.4194	62.60%	37.40%	Fraudulent

Total Transactions: 7

Fraudulent Transactions: 3

Legitimate Transactions: 4

Conclusion

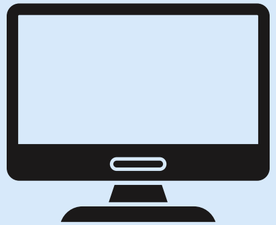
The project is progressing on time and on track to completion within the stipulated time.
The product will deliver on all the features and functions put forward in the SRS/Design Report.
Phases completed so far work flawlessly.
Fin-Spy will provide a comprehensive fraud detection and monitoring framework easily implementable in any existing system.

PHASE 1

Completed with comprehensive datasets prepared for model training and testing.

PHASE 2

95% completed with final finetuning of Flask API underway. Model research and training completed. All models are ready for integration.



PHASE 3

Phase 3 operations commenced with inital visions of front end being developed. SIEM implementation being researched and ready for integration.

DEVELOPMENT TEAM

The brains behind the vision of using SIEM for financial fraud monitoring.

Pravaal B Nath

AI RESEARCHER AND DATA ANALYST

Roll No. 20921038

Nandulal Krishna

LEAD RESEARCHER AND BACKEND DEV

Roll No. 20221097

Akshay K R

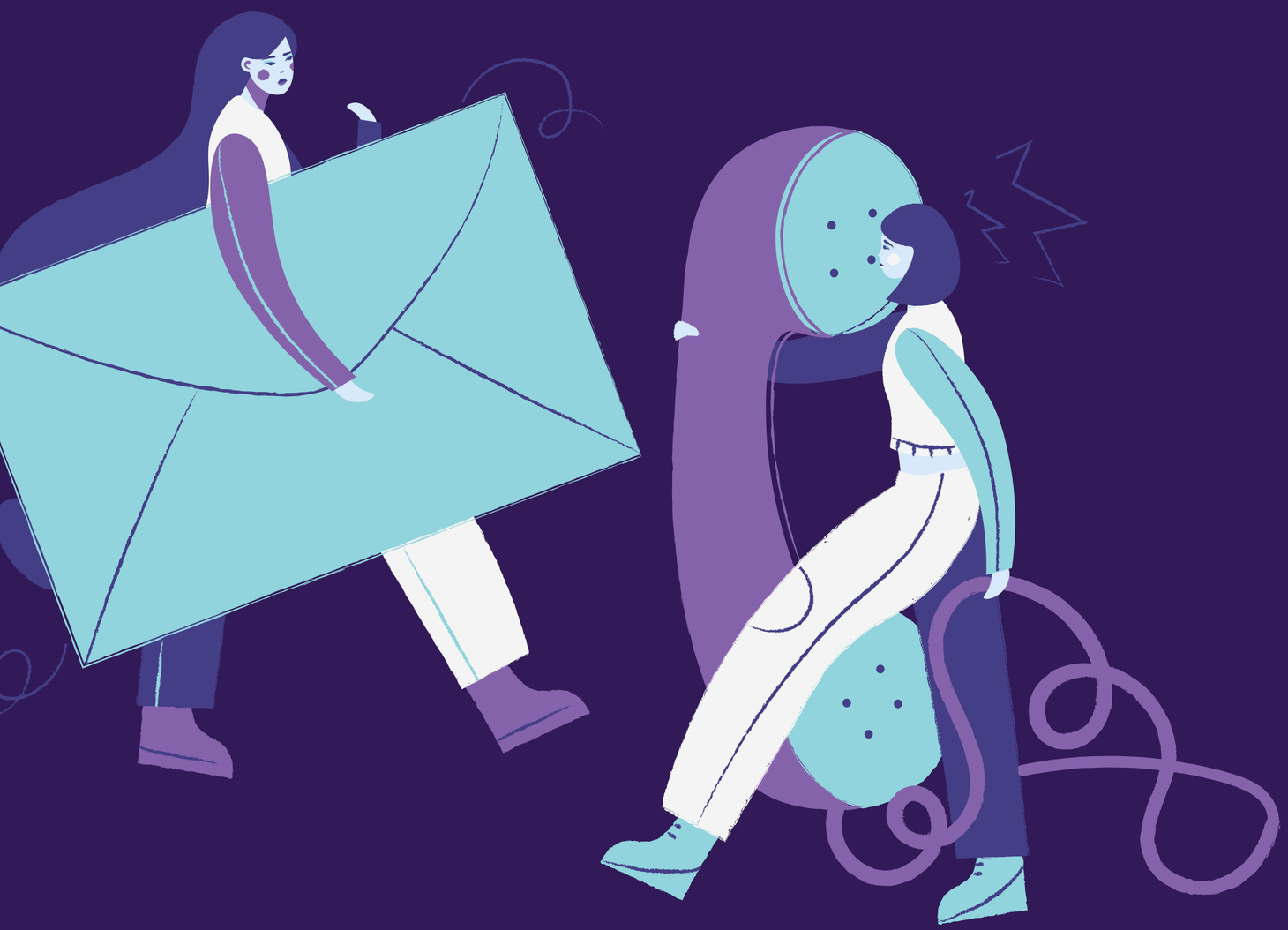
FRONT END DEV AND TESTER

Roll No. 20221094

Rahul R

FRONT END DEV AND DATABASE MANAGER

Roll No. 20221098



Thank you

This concludes our interim project presentation.

https://github.com/CodeBreak-Matrix/FinSpy

pravaal@ug.cusat.ac.in