Janardan Bhagat Shikshan Prasarak Sanstha's

Changu Kana Thakur Arts, Commerce and Science College, New Panvel (Autonomous) Plot No.-1, Sector-11, Khanda Colony, New Panvel (W), Dist.-Raigad, State- Maharashtra, India, PIN.-410206

PROJECT REPORT ON

"MOBILE BANKING RISK ANALYSIS"

DEVELOPED BY

MR. KSHITIJ BABAN BAGAL

(M.Sc.-II (SEM-IV) COMPUTER SCIENCE)

UNDER THE GUIDANCE

OF

Dr. ANJALI KULKARNI

2022-2023

॥ विद्या विनयेन शोभते ॥
Janardan Bhagat Shikshan Prasarak Sanstha's
CHANGU KANA THAKUR
ARTS, COMMERCE AND SCIENCE COLLEGE, NEW PANVEL
(AUTONOMOUS)
Re-accredited 'A+' Grade by NAAC (3rd Cycle - CGPA 3.61)
'College with Potential for Excellence' Status Awarded by UGC
'Best College Award' by University of Mumbai

Prof. (Dr.) Sanjay K. Patil
Principal
M.Sc., SET, M.Phil., Ph.D.
Tel: (022) 2746 7599 (D)

Ref. No.: CKTACS/ Date :

Department of Computer Science

CERTIFICATE

This is to certify that the Project Report entitled

"MOBILE BANKING RISK ANALYSIS"

Is successfully completed by **Mr. Kshitij Baban Bagal** Examination Seat Number **3004** under the guidance of **Dr. Anjali Kulkarni** during the academic year **2022-2023** as per the Syllabus, and the fulfillment for the completion of the M.Sc.-II (Semester-IV) in the Computer Science of **University of Mumbai**. It is also to certify that this is original work of the candidate done during academic

Place: Panvel

Date:

Internal Examiner **Head of Department**

External Examiner

Plot No.-1, Sector-11, Khanda Colony, New Panvel (W), Dist.-Raigad, Maharashtra, India - 410 206. ☎ :(022)2745 5760, 2746 4193,
Super Fax : 9022933585 • E-mail : principalckthakurcollege@rediffmail.com / principal@ckthakurcollege.net • URL : www.ckthakurcollege.net

MOBILE BANKING RISK ANALYSIS

KSHITIJ BABAN BAGAL
EXAM ROLL NO- MSCS3004

ACKNOWLEDGMENT

I am very thankful to the **Changu Kuna Thakur (CKT)college**, University of Mumbai, who gave us the opportunity to develop the project based on our Specialization titled "**MOBILE BANKING RISK ANALYSIS**".

I would also like to express our deep regards and gratitude to the principal **Dr. Prof. S.K.Patil**. I would also like to tender our sincere thanks to the **H.O.D. Mrs. P.M.Jadhav** and my project guide **Dr. Anjali Kulkarni** and all teachers for their co-operation. I will wish to thank the non-teaching staff and my friends who have helped me all time in one way or the other.

We are also very much thankful to the "**University of Mumbai**" for including the project work as part of syllabus, without which we would not gained the experience of using the analytical software as this.

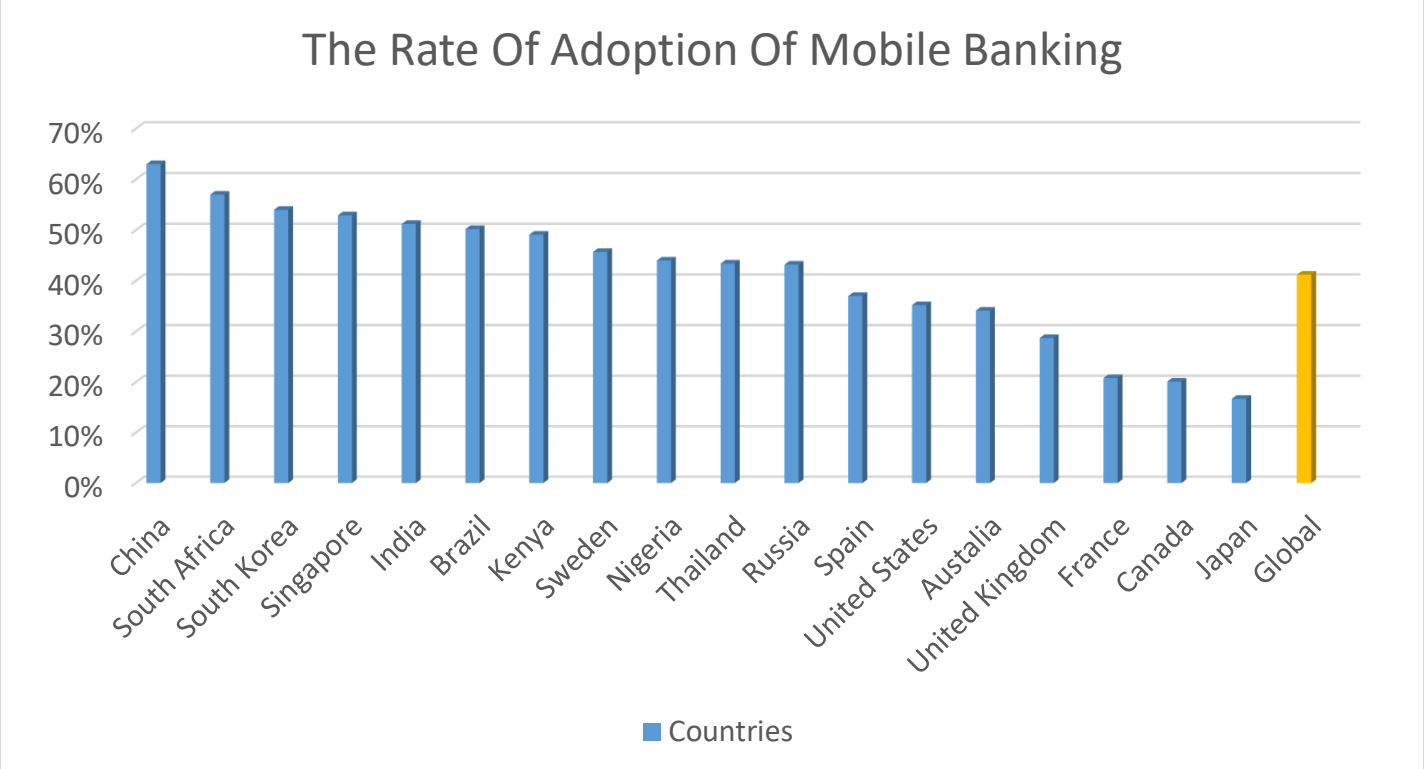
INDEX

INTRODUCTION

"Mobile banking is a service provided by a bank or other financial institution that allows its customers to conduct financial transactions remotely using a mobile device such as a smartphone or tablet"

Mobile banking allows customers of an insured depository institution to conduct banking activities, such as checking balances, receiving account alerts, or making bill payments, through a smartphone or tablet. Mobile financial services, of which mobile banking is a subset, involve nonbank third parties.

The rate of the Adoptions is utmost in so-called developing countries, reaching 60-70% in China and India in comparison to developed one, such as the US, Canada and the UK. [3]



. **Risk Definitions**

1. Systemic: A risk that could cause collapse of, or significant damage to, the financial system or a risk which results in adverse public perception, possibly leading to lack of confidence and worst case scenario, a "run" on the system

2. Operational: A risk which damages the ability of one of the stakeholders to effectively operate their business or a risk which results in a direct or indirect loss from failed internal processes, people, systems or external events

3. Reputation: A risk that damages the image of one of the stakeholders, the mobile system, the financial system, or of a specific product

4. Legal: A risk which could result in unforeseeable lawsuits, judgment or contracts that could disrupt or affect MFS business practices

5. Liquidity: A risk that lessens the ability of a bank or MFS provider/agent to meet cash obligations upon demand

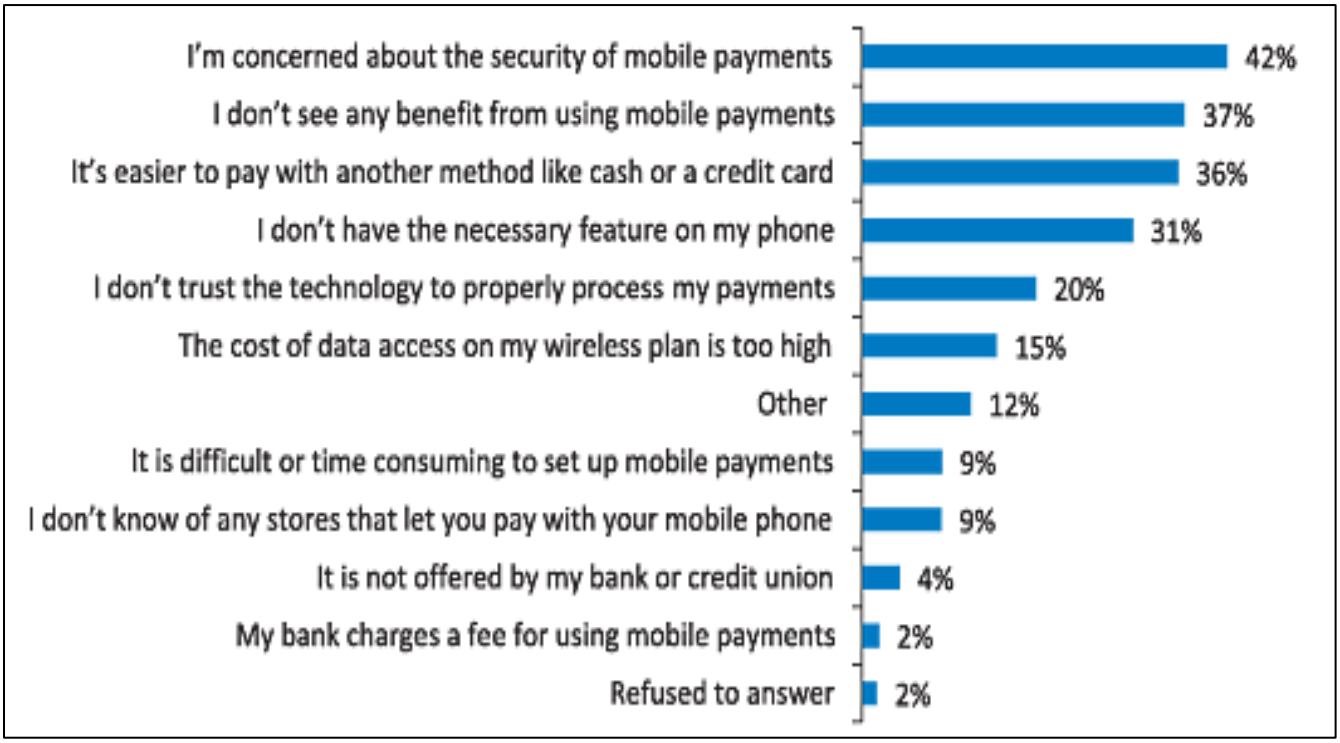
6. International: A systemic risk (as defined above) that could have cross-border contagion effect

To understand mobile banking risk, it is important to understand the three most common delivery channels (many institutions offer all three channels to reach the greatest number of customers):

1. Text messaging/short message service (SMS)
2. Mobile-enabled Internet browser
3. Mobile applications

A major challenge for the adoption of mobile banking technology and services is the perception of insecurity. In the survey conducted by the Federal Reserve, **48%** of respondents cited their main reason for not using mobile banking was "I'm concerned about the security of mobile banking". In the same study, respondents were asked to rate the security of mobile banking for protecting their personal information and **32%** rated it as somewhat unsafe and very unsafe, while **34%** were not sure of the security. These statistics represent a significant barrier to the use of mobile banking products and services. [1]

The number of frauds in the year 2016-17 was more than 3870, involving an insane amount of 17,750 crores including both commercial and private banks. If we Compare this with 2013-17, we seen that the number of frauds was almost doubled as a total of 17,501 frauds were reported in this period. Out of these, 2,084 had insider involvement. [4]



IMPLEMENTATION DETAILS

OBJECTIVES

There are few objectives for this project

General Objective: -

- To identify various Mobile Banking Risks Factors.
- To suggest some prevention measures against Mobile Banking Risks from general populations opinion.
- To create awareness in peoples About Mobile Banking Risks.

Specific Objective: -

- To Better Understand How Mobile Banking Risks Affect Us.
- To Analyze Mobile Banking Risks with Predictive Analysis to Identify Future Trends.
- Using Various Analysis Method to Find Out Which Is Better Suited for Mobile Banking Risk Analysis

RELATED WORK

[1] In this study there is explained what is Risk, what are its Key Security Risks (Mobile Device and application vulnerabilities, Privacy, Wireless Carrier, Payments Technology), Risk Mitigation. When we think of risk we can easily understand the main concept from this article. The details are very accurate which give simple insights to concepts.

[2] This study is centered to customer's perspective. here by conducting analysis on customer's remark authors have gotten to know the perception of individuals towards mobile banking, how to find out the satisfaction levels of users towards mobile banking and how to identify the growth and scope of mobile banking as well as significant factor of mobile banking.

[3] In this article author is giving the overview of how with increasing rate of Mobile Banking acceptance and usage how the risks and loss of privacy in security system are of concerning. Here author introduces a concept of AHP (Analytical Hierarchy Process) based on MCDM (Multi-Criteria Decision Making) to evaluate and rank the different factors that contribute to impact the adoption of M-Banking.

[4] The main focus on this study is on What are banking frauds? With increasing growth of mobile banking and digitalization we face many risks and frauds. Here we have a list of banking frauds which shows increment by years. With list of fraud factor we can take proper precaution.

[5] With increasing popularity of Mobile banking many people are starting to adapt to trend of digitalization here we can see study is conducted to understand populations Roll and their impact on mobile banking.

[6] With quantitative research approach authors has conducted through analysis. They have found that Mobile banking players must focus on conformation, accuracy and monitoring tools in order to win the confidence of customers and break all the global and political hurdles in order to achieve the efficient, well regulated open architecture.

[7] Author with basic objective is to identify the advantages and limitations of mobile banking and the problems faced by customers in mobile banking has given proper two-sided arguments. This is explained with proper example and explanation

[8] authors have given a through explanation about how M-Banking is currently implemented? what challenges we must face to? And what are the security issues? All with proper details. Authors also have explained how mobile bank transaction services model works.

SYSTEM CONFIGURATION

Hardware Requirement:

Processor	Intel
RAM	8 GB or above cache memory
Hard Disk	60 GB or above
Input Device	Keyboard, Mouse
Output Device	Monitor

Software Requirement:

Operating System	Windows 2007 and above
Programming Language	C#
Development application	Unity Engine, Google Colab
Storage application	Google drive,

Dataset

For Project implementation purpose we needed minimum 50+ records which were collected with use of Google Form with which we have collected sufficient data to perform our analysis. The data which is received from google form is stored in Google Spread-sheets and then the spreadsheet is stored in Goggle Drive. Which will make retrieving data for analysis much easier.

Link o dataset is as follow: -

https://docs.google.com/spreadsheets/d/1bQBFcZreho8Oo0-XZ8b2OTIplJ0R7rP_a16w5bQXOk0/edit#gid=0

This Dataset is used for analysis purpose only. Here all unnecessary values and Sentences (Noisy, Incomplete Data, different language) are removed and only necessary data is stored

ANALYSIS

METHODOLOGY

➢ Defining the question

First we need to discuss about what is our purpose of this project/ research which is to analyze the data about Mobile Banking Risk to find way to alert the population about these risks.

➢ Collecting the data

Now with objective conformed we need a strategy for data collection and aggregate the appropriate data. Here we can use both quantitative (numeric) or qualitative (descriptive) data.

Here we will use Surveys & Questionnaires. Primary medium will be Google Form which will take peoples responses about how they have face any Mobile Banking Risk in any banking platform such as G-pay, Paytm, etc. or any mobile banking services over SMS or mobile banking over USSD.

In Questionnaires primary goal is to get data about users and their experience about M-Banking but we will also be asking about any suggestion they can think of to avoid falling into this risks.

The link to Google Form Which is used for collecting data is as follow: -

https://docs.google.com/forms/d/e/1FAIpQLSfXL8U92pDPI2Th17DmlL5NMYV2uqzpEqrP9O0ehk1GAPfQeQ/viewform

➢ Data Mining

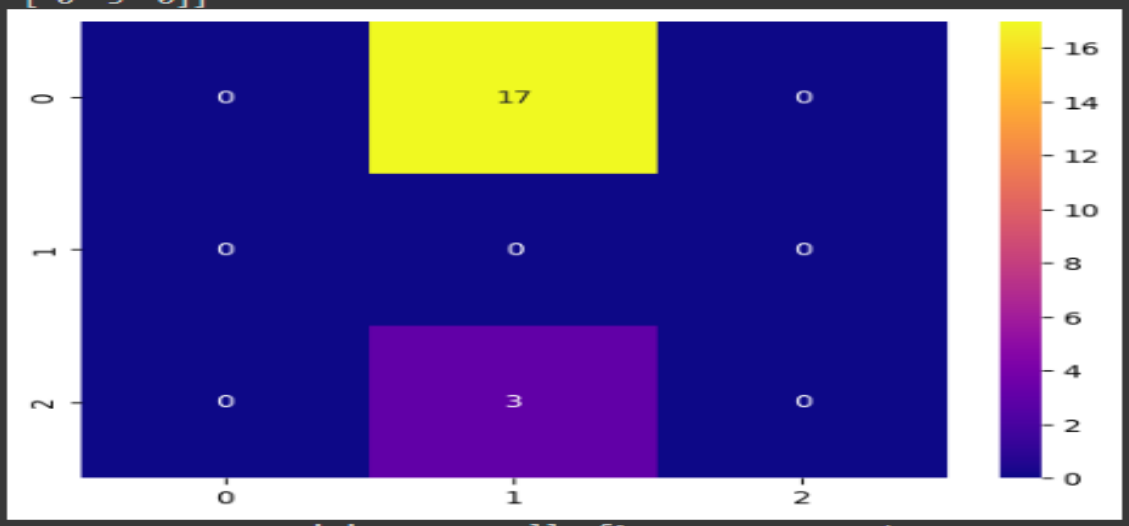
Now we can use Data Mining to identify patterns and relationships so that we can have easy and sorted data sets. Data mining have many techniques to use such as classification, clustering, regression, etc.

[1] Classification

Here we classify the data based on its data structure/type or source, which kind of KDD is obtained. Classification divides data in to multiple gropes per requirement based on varies rules. this classified data is categories into different sets is easy to use and store.

```
[ ]  from sklearn.metrics import confusion_matrix
     import seaborn as sns
     from sklearn.metrics import classification_report
     cm = confusion_matrix(y_pred, z_test)
     print(cm)
     sns.heatmap(cm, cmap="plasma", annot=True)
     plt.show()
     print(classification_report(y_pred, z_test))
```

```
[[ 0 17  0]
 [ 0  0  0]
 [ 0  3  0]]
```

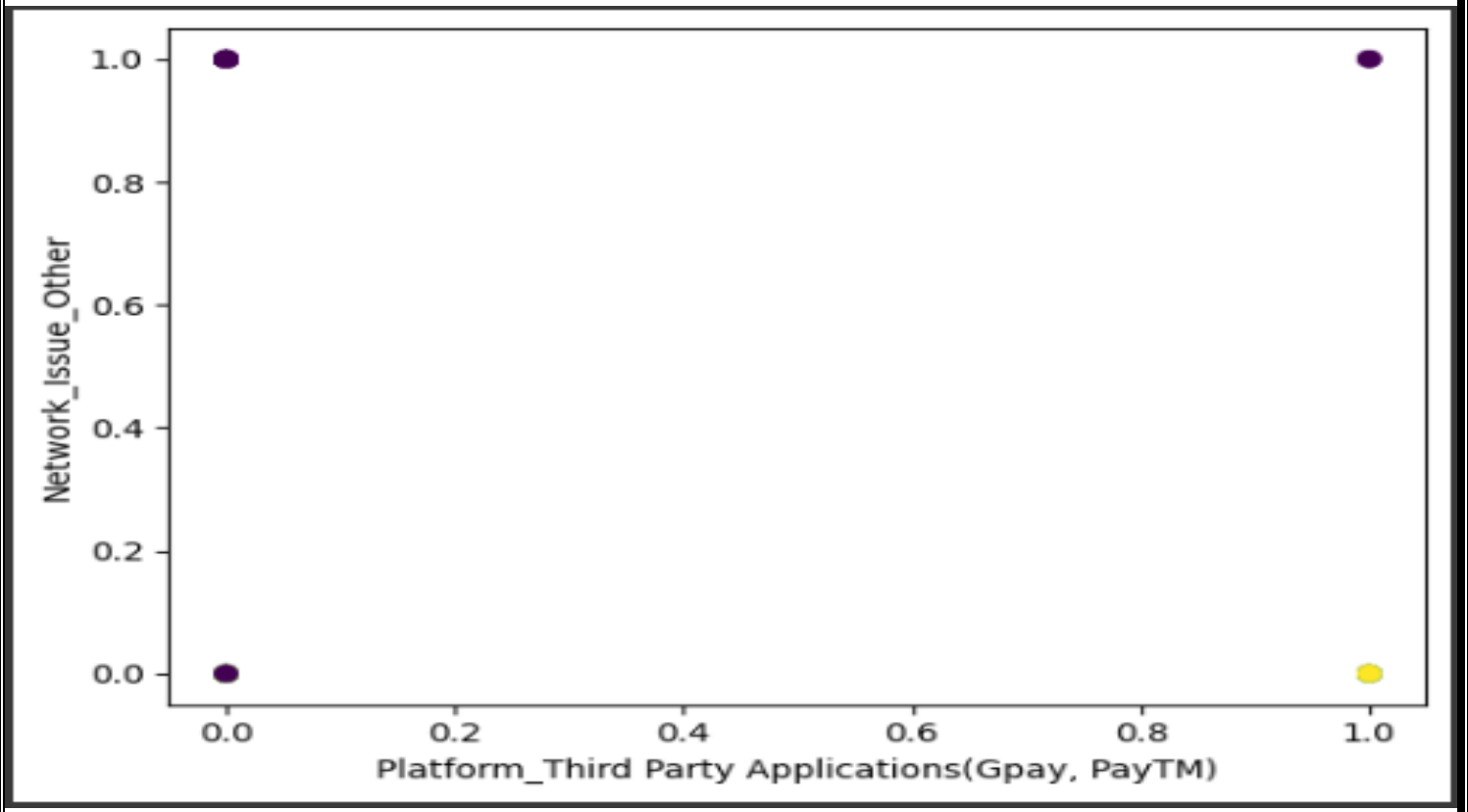


	precision	recall	f1-score	support
-1	0.00	0.00	0.00	17.0
0	0.00	0.00	0.00	0.0
1	0.00	0.00	0.00	3.0
accuracy			0.00	20.0
macro avg	0.00	0.00	0.00	20.0
weighted avg	0.00	0.00	0.00	20.0

[2] Clustering

Clustering is very similar to the classification, but it involves grouping chunks of data together based on their similarities.

```
import pandas as pd
import matplotlib.pyplot as plt
from sklearn.cluster import KMeans

# Load the dataset
dfa = pd.read_excel('MBR.xlsx')

# Encode categorical variables
dfa = pd.get_dummies(dfa)

# Scale the data if required

# Perform clustering using KMeans
kmeans = KMeans(n_clusters=3, random_state=42)
kmeans.fit(dfa)

# Add the cluster labels to the dataframe
dfa['Cluster'] = kmeans.labels_

# Visualize the clusters
plt.scatter(dfa['Platform_Third Party Applications(Gpay, PayTM)'], dfa['Network_Issue_Other'], c=dfa['Cluster'])
plt.xlabel('Platform_Third Party Applications(Gpay, PayTM)')
plt.ylabel('Network_Issue_Other')
plt.show()
```


1.0
0.8
0.6
0.4
0.2
0.0
Network_Issue_Other
0.0
0.2
0.4
0.6
0.8
1.0
Platform_Third Party Applications(Gpay, PayTM)

[3] Regression

Here we can use to give exact relationship between risks and their solution's provide by peoples or to shoe show relation between certain platform and their frequent risks (problems)

```
import pandas as pd
from sklearn.linear_model import LinearRegression
from sklearn.model_selection import train_test_split
from sklearn.metrics import r2_score
from sklearn.linear_model import LinearRegression
#Load the dataset
df = pd.read_excel('MBR.xlsx')
# Check for missing values
print(df.isnull().sum())
#Encode categorical variables
df = pd.get_dummies (df)
#Split the dataset into training and testing sets
X = df.drop(columns=['Other_Issue_Privacy Protection'])
y=df['Other_Issue_Privacy Protection']
X_train, X_test, y_train, y_test = train_test_split(X, y, test_size=0.4, random_state=42)
#Perform feature scaling if required
#Build and train the regression model reg = LinearRegression().fit(X_train, y_train)
#Evaluate the model performance on the testing set
# Define and train the regression model
reg = LinearRegression().fit(X_train, y_train)
y_pred = reg.predict(X_test)
print('R^2 Score:', r2_score (y_test, y_pred))
```

```
Platform            0
Network_Issue       0
Application_Issue   0
Other_Issue         0
dtype: int64
R^2 Score: 1.0
```

➢ Cleaning The Data

Now that we have Data mined. But we can't use this data sets as they are because they contain many unnecessary data which can be any type of noisy data or any incomplete or wrong and unreverent data which have to be filtered out. This step is done manual because of lack of expertise in automated data filtering skills

➢ Analyzing the data

Now that we've finished cleaning the data, we have to analyze the data set.to come to the conclusions for which we can use any analyzing technique such as **Descriptive analysis**, **Diagnostic analysis**, **Predictive analysis**, **Prescriptive analysis.**

here we will be using Predictive analysis on the data set. In predictive analysis we predict future trends using training set of past data. There are many ways/methods to use Predictive analysis from which we will use following methods

- Here we have used **Association Rule**

  Association rule mining is a data mining technique used to identify frequent patterns, associations, and correlations among items in a dataset. It can be used for prediction by identifying the likelihood of certain items being purchased together

```
import pandas as pd
from mlxtend.frequent_patterns import apriori
from mlxtend.frequent_patterns import association_rules

# Load the dataset
df = pd.read_excel('MBR.xlsx')

# Convert the data to a one-hot encoded format
one_hot = pd.get_dummies(df).astype('int')

# Generate frequent itemsets using the Apriori algorithm
frequent_itemsets = apriori(one_hot, min_support=0.2, use_colnames=True)

# Generate association rules from the frequent itemsets
rules = association_rules(frequent_itemsets, metric="lift", min_threshold=1)

# Print the association rules
print(rules)
```

```
                                antecedents  \
0                    (Network_Issue_Other)
1  (Other_Issue_Unsatisfactory Reward/Coupon System)

                                consequents  antecedent support  \
0  (Other_Issue_Unsatisfactory Reward/Coupon System)                0.26
1                    (Network_Issue_Other)                0.34

   consequent support  support  confidence      lift  leverage  conviction
0                0.34      0.2    0.769231  2.262443    0.1116    2.860000
1                0.26      0.2    0.588235  2.262443    0.1116    1.797143
```

The result suggests that there is a strong association between the two issues. Specifically, it indicates that customers who experience "Network_Issue_Other" are highly likely to also experience "Other_Issue_Unsatisfactory Reward/Coupon System", and vice versa.

The confidence value of 0.769 suggests that when a customer has experienced "Network_Issue_Other", there is a 76.9% chance that they will also experience "Other_Issue_Unsatisfactory Reward/Coupon System".

The lift value of 2.262 suggests that these two issues are more likely to occur together than would be expected if they were independent of each other.

The leverage value of 0.1116 indicates that the presence of these two issues together is responsible for increasing the total number of complaints by 11.16%

Finally, the conviction value of 2.86 suggests that customers who have experienced both of these issues are about 2.86 times more likely to report both issues together than if the two issues were independent of each other.

- Here we have used **Isolation Forest Analysis**

  The main idea behind Isolation Forest is to isolate outliers by using binary trees. The algorithm randomly selects a feature and a split value to divide the data set into two parts at each step of building the tree. It continues recursively partitioning the data until it isolates the outlier data points into their own leaf nodes, which requires fewer steps than for normal data points

```
from sklearn.ensemble import IsolationForest
from sklearn.model_selection import train_test_split
from sklearn.metrics import precision_score
import numpy as np

X_train, X_test, z_train, z_test = train_test_split(X, z, test_size=0.2, random_state=42)
# Create an instance of the Isolation Forest model with desired parameters
isoforest = IsolationForest(n_estimators=100, contamination='auto', random_state=42)

# Fit the model on the training data
isoforest.fit(X_train)

# Predict the anomalies in the test set
y_pred = isoforest.predict(X_test)
z_pred = isoforest.predict(X_train)

# Anomaly scores (the higher, the more anomalous)
scores = isoforest.decision_function(X_test)

# Evaluate the model using appropriate metrics (e.g., precision, recall, F1-score)
# based on the ground truth labels (if available)
# Evaluate the model
accuracy = np.mean(y_pred == z_test)
print(y_pred)
precision = precision_score(z_test, y_pred, average='weighted')
recall = recall_score(z_test, y_pred, average='weighted')
f1 = f1_score(z_test, y_pred, average='weighted')

# Print the accuracy score
print("Accuracy:", accuracy)
print("Precision:", precision)
print("Recall:", recall)
print("F1-score:", f1)
```

```
[ 1  1 -1 -1  1  1 -1  1  1 -1 -1 -1 -1 -1 -1 -1  1  1 -1 -1]
Accuracy: 0.0
Precision: 0.0
Recall: 0.0
F1-score: 0.0
```

Isolation Forest model is evaluates using the accuracy score, which is calculated by taking the mean of the predicted labels (y_pred and z_pred) and comparing them with the true labels (z_test and z_train). In this case, the accuracy scores for both the training and testing data are 0.0, which suggests that the model is not performing well in detecting anomalies in the data.

result suggests that the Isolation Forest model is predicting the anomalies in the test set. The predicted anomalies are represented by the array of 1s and -1s. In this case, the accuracy of the model is 0.0, which means that none of the predicted anomalies match the actual anomalies in the test set.

Additionally, the precision, recall, and F1-score are also 0.0. Precision is the proportion of true positives among the predicted positives, while recall is the proportion of true positives among the actual positives. F1-score is the harmonic mean of precision and recall, and it is used to evaluate the trade-off between precision and recall. Since there are no true positives or actual positives in this case, the precision, recall, and F1-score are all ill-defined and set to 0.0.

- Here We have used **Random Forest Analysis**

  a supervised machine learning algorithm used for classification and regression tasks. It is an ensemble method that combines multiple decision trees to make predictions. Each decision tree is trained on a random subset of the training data and a random subset of the features. This random selection of both data and features helps to reduce the variance and overfitting in the model, making it more robust and generalizable.

```
from sklearn.ensemble import RandomForestClassifier
from sklearn.metrics import accuracy_score, precision_score, recall_score, f1_score
from sklearn.model_selection import train_test_split
import pandas as pd

# Load the MBR dataset
data = pd.read_excel('MBR.xlsx')
data['Platform'] = data['Platform'].astype('category')
data['Network_Issue'] = data['Network_Issue'].astype('category')
data['Application_Issue'] = data['Application_Issue'].astype('category')
data['Other_Issue'] = data['Other_Issue'].astype('category')

data = pd.get_dummies(data, columns=['Platform', 'Network_Issue', 'Application_Issue', 'Other_Issue'])
# Separate the features (X) and target variable (y)
X = data.drop('Network_Issue_Other', axis=1)
y = data['Network_Issue_Other']

# Split the data into training and testing sets (80% for training, 20% for testing)
X_train, X_test, y_train, y_test = train_test_split(X, y, test_size=0.2, random_state=42)

# Train a Random Forest classifier with 100 trees
clf = RandomForestClassifier(n_estimators=100, random_state=42)
clf.fit(X_train, y_train)

# Make predictions on the test set
y_pred = clf.predict(X_test)

# Evaluate the model using accuracy, precision, recall, and F1-score
accuracy = accuracy_score(y_test, y_pred)
precision = precision_score(y_test, y_pred, average='binary')
recall = recall_score(y_test, y_pred, average='binary')
f1 = f1_score(y_test, y_pred, average='binary')

print(f"Accuracy: {accuracy:.2f}")
print(f"Precision: {precision:.2f}")
print(f"Recall: {recall:.2f}")
print(f"F1-score: {f1:.2f}")
```

```
Accuracy: 0.95
Precision: 0.80
Recall: 1.00
F1-score: 0.89
```

The results suggest that the Random Forest classifier performed well in predicting the target variable ('Network_Issue_Other') on the MBR dataset, with an overall accuracy of 95%.

The precision score of 0.80 indicates that among the predictions made by the model for the positive class, 80% of them were correct. The recall score of 1.00 indicates that the model correctly identified all the positive samples in the test set. The F1-score of 0.89 is the harmonic mean of precision and recall, indicating a good balance between the two metrics.

Overall, these results suggest that the Random Forest classifier is a suitable algorithm for predicting network issues in the MBR dataset, and it could be used in practical applications for this purpose.

As we have observed above between **Association Rule**, **Isolation Forest** and **random Forest** methods the Random Forest **Analysis Method is Most Suited to be Used on our data set to predict future Trends**

➢ Visualizing Results

Now that analysis is completed we can now form conclusion/ result based on it. But these result will only have their meaning if people can understand them so we can use Data Visualization to convert data into many type of charts or diagrams so that results can be easy to understand.

For Data Visualization purpose I have decided to create an Application which will visualize the dataset that we have gathered as well as the results and finding of our analysis

This application will also play important role for connecting general populations problems and their suggestions to people in-charge of mobile banking

The application will be called “MBRA” which was developed using UNITY Engine. Unity provides us with multiple library and assets which are available for free use and unity make all things for networking and GUI very easy to Create and handle.

Algorithm

The most important algorithm is shown below.

```
// Load the MBR dataset
DataTable data = new DataTable();
data.ReadXml("MBR.xml");

// Create a matrix with the issue data
double[][] issueData = new double[data.Rows.Count][];
for (int i = 0; i < data.Rows.Count; i++)
{
   issueData[i] = new double[data.Columns.Count - 1];
   for (int j = 0; j < data.Columns.Count - 1; j++)
   {
      if (data.Columns[j].ColumnName.Contains("Issue"))
      {
         string issue = data.Rows[i][j].ToString().Trim();
         if (string.IsNullOrEmpty(issue))
         {
            issueData[i][j] = 0;
         }
         else
         {
            issueData[i][j] = 1;
         }
      }
   }
}
```

```
// Perform K-means clustering on the issue data
int numClusters = 10;
KMeans kmeans = new KMeans(numClusters);
int[] clustering = kmeans.Compute(issueData);

// Group the issues by cluster
Dictionary<int, List<string>> clusterIssues = new Dictionary<int, List<string>>();
for (int i = 0; i < clustering.Length; i++)
{
   if (!clusterIssues.ContainsKey(clustering[i]))
   {
      clusterIssues.Add(clustering[i], new List<string>());
   }
   for (int j = 0; j < data.Columns.Count - 1; j++)
   {
      if (data.Columns[j].ColumnName.Contains("Issue"))
      {
         string issue = data.Rows[i][j].ToString().Trim();
         if (!string.IsNullOrEmpty(issue))
         {
            clusterIssues[clustering[i]].Add(issue);
         }
      }
   }
}

// Select the most common issue in each cluster
Console.WriteLine("Most Common Issues by Cluster:");
foreach (var cluster in clusterIssues)
{
   var mostCommonIssue = cluster.Value.GroupBy(x => x)
```

```
            .OrderByDescending(x => x.Count())
            .Select(x => x.Key)
            .FirstOrDefault();
        Console.WriteLine($"Cluster {cluster.Key}: {mostCommonIssue}");
    }
```

APPLICATION

SCENE

In application we have used various scene to handle and show particular parts of Application and they are shown below


Records.unity


Responces.unity


Analysis.unity


Complaint.unity

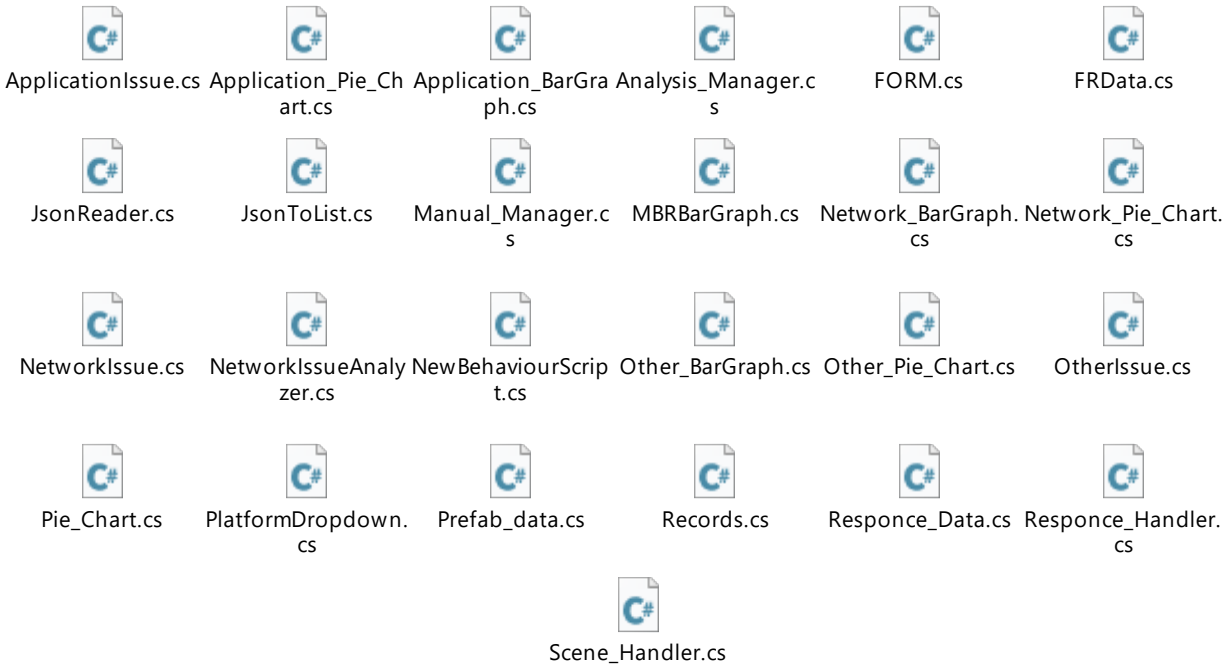

Form.unity


Manual.unity


Menu.unity

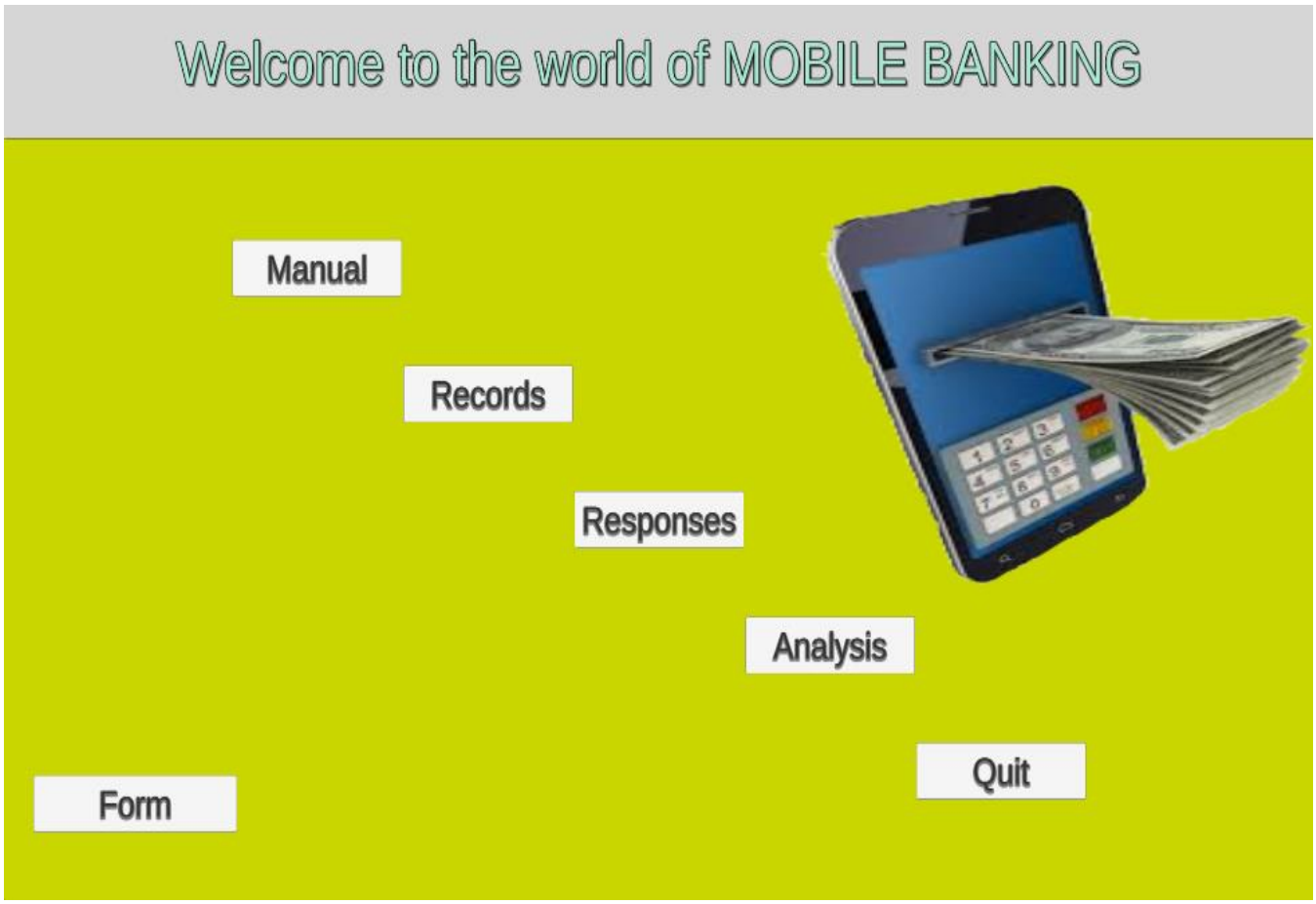
CODE

In application we have used 25 C# Scripts and they are shown below

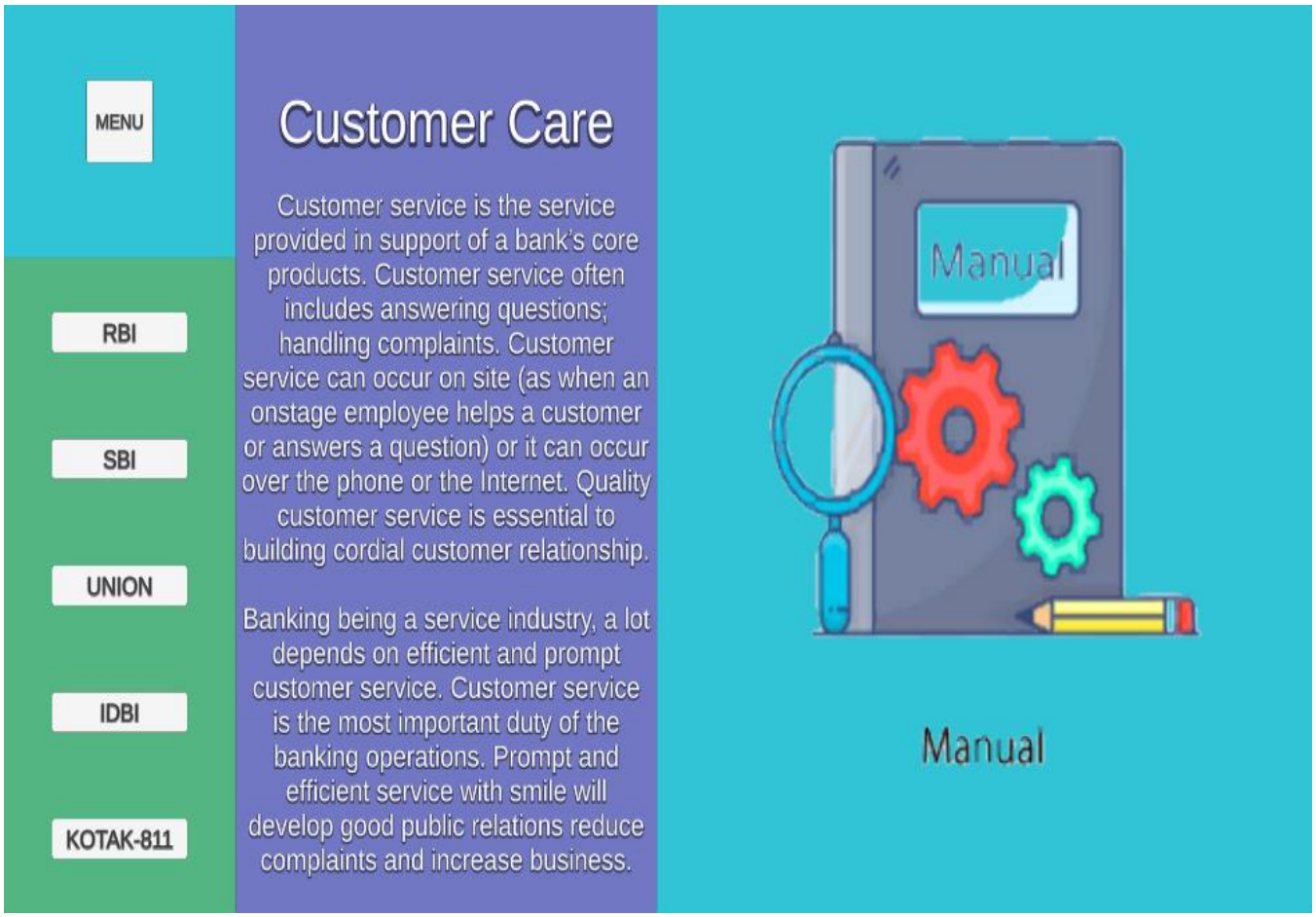


Result

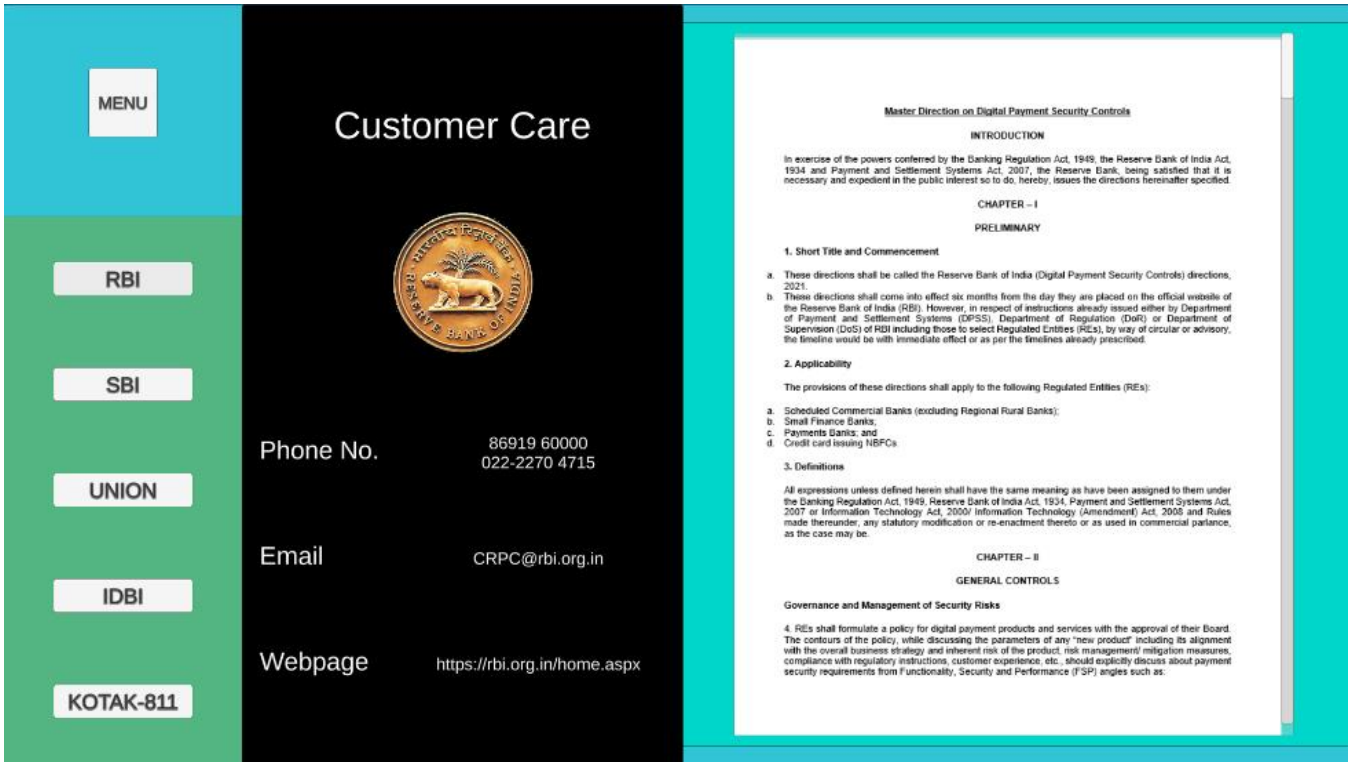
MENU: - Main menu where we can assess all scene



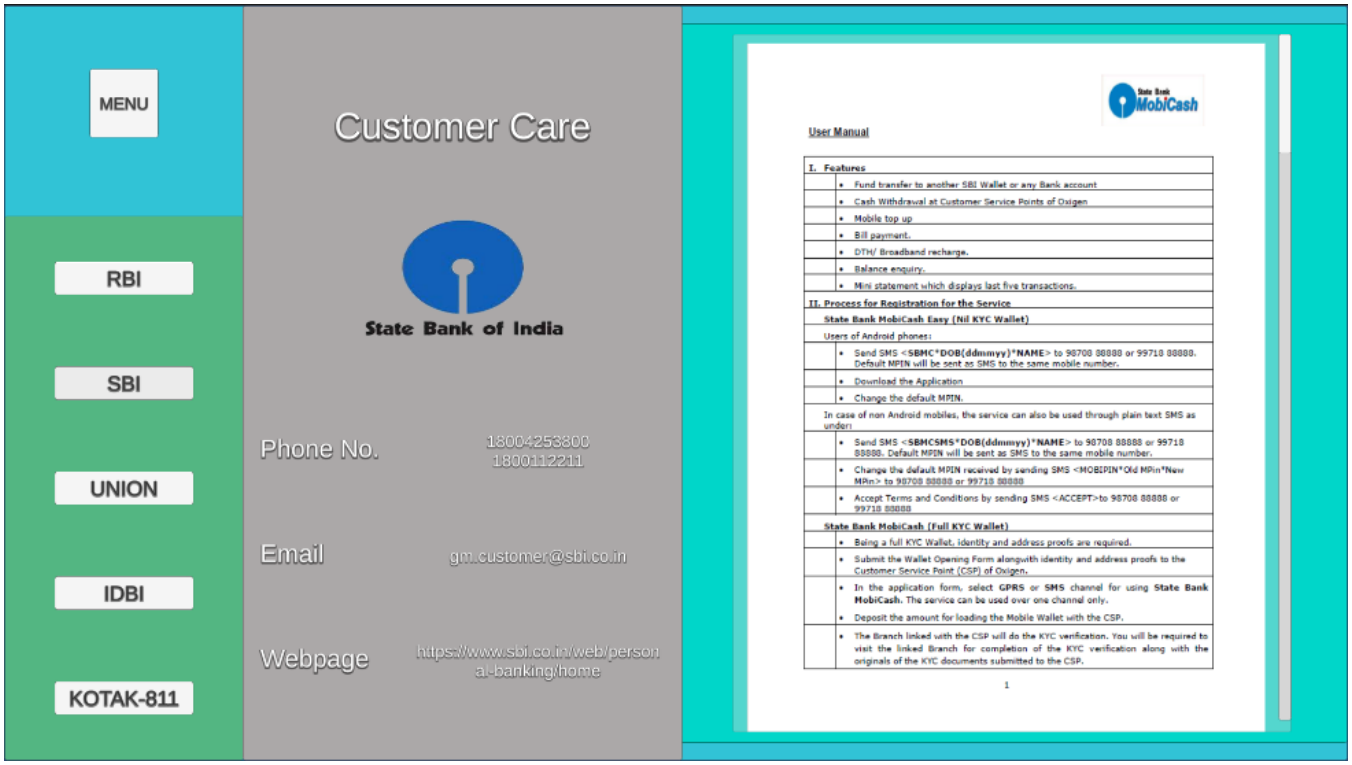
MANUAL:- Here we can see manual and customer care info for vaieous banks



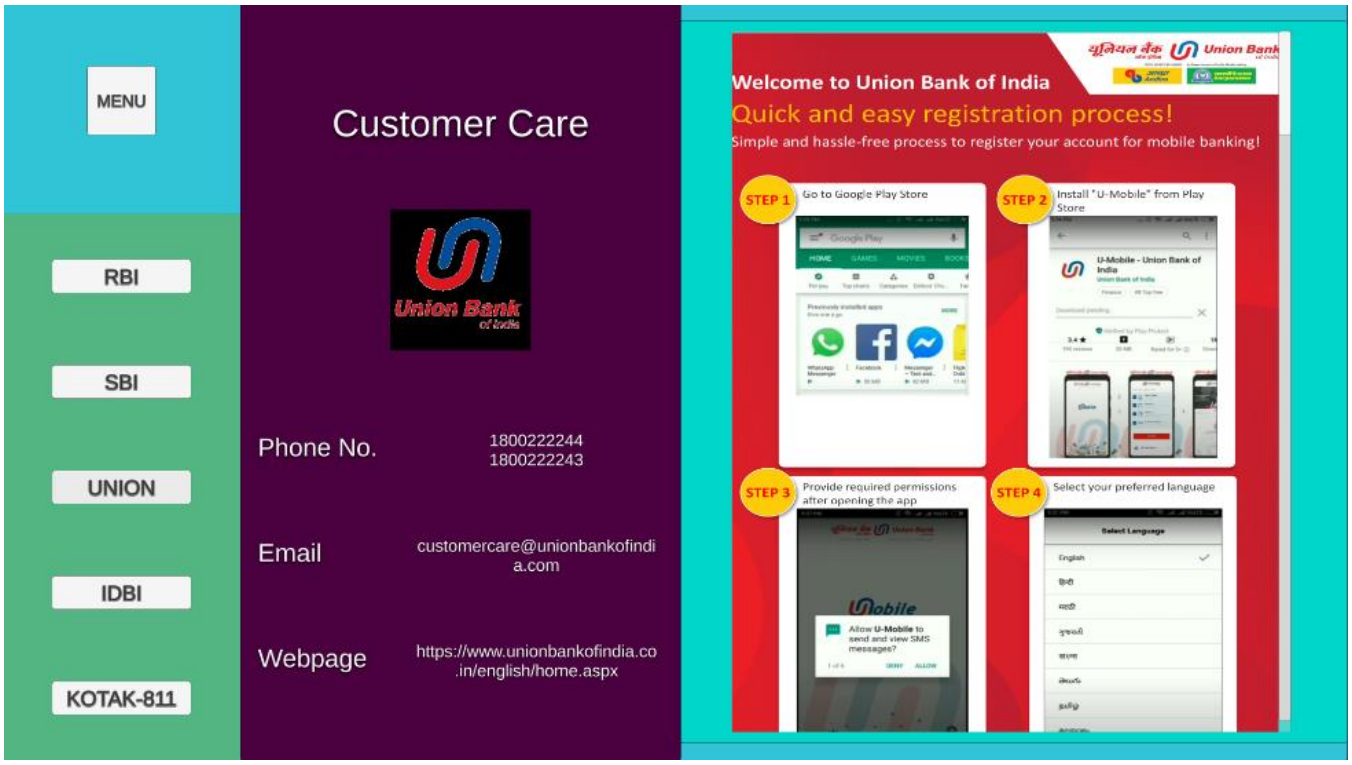
RBI manual


MENU
RBI
SBI
UNION
IDBI
KOTAK-811
Customer Care
Phone No.
86919 60000
022-2270 4715
Email
CRPC@rbi.org.in
Webpage
https://rbi.org.in/home.aspx
Master Direction on Digital Payment Security Controls
INTRODUCTION
In exercise of the powers conferred by the Banking Regulation Act, 1949, the Reserve Bank of India Act, 1934 and Payment and Settlement Systems Act, 2007, the Reserve Bank, being satisfied that it is necessary and expedient in the public interest so to do, hereby, issues the directions hereinafter specified.
CHAPTER – I
PRELIMINARY
1. Short Title and Commencement
a. These directions shall be called the Reserve Bank of India (Digital Payment Security Controls) directions, 2021.
b. These directions shall come into effect six months from the day they are placed on the official website of the Reserve Bank of India (RBI). However, in respect of instructions already issued either by Department of Payment and Settlement Systems (DPSS), Department of Regulation (DoR) or Department of Supervision (DoS) of RBI including those to select Regulated Entities (REs), by way of circular or advisory, the timeline would be with immediate effect or as per the timelines already prescribed.
2. Applicability
The provisions of these directions shall apply to the following Regulated Entities (REs):
a. Scheduled Commercial Banks (excluding Regional Rural Banks);
b. Small Finance Banks;
c. Payments Banks; and
d. Credit card issuing NBFCs
3. Definitions
All expressions unless defined herein shall have the same meaning as have been assigned to them under the Banking Regulation Act, 1949, Reserve Bank of India Act, 1934, Payment and Settlement Systems Act, 2007 or Information Technology Act, 2000/ Information Technology (Amendment) Act, 2008 and Rules made thereunder, any statutory modification or re-enactment thereto or as used in commercial parlance, as the case may be.
CHAPTER – II
GENERAL CONTROLS
Governance and Management of Security Risks
4. REs shall formulate a policy for digital payment products and services with the approval of their Board. The contours of the policy, while discussing the parameters of any "new product" including its alignment with the overall business strategy and inherent risk of the product, risk management/ mitigation measures, compliance with regulatory instructions, customer experience, etc., should explicitly discuss about payment security requirements from Functionality, Security and Performance (FSP) angles such as:

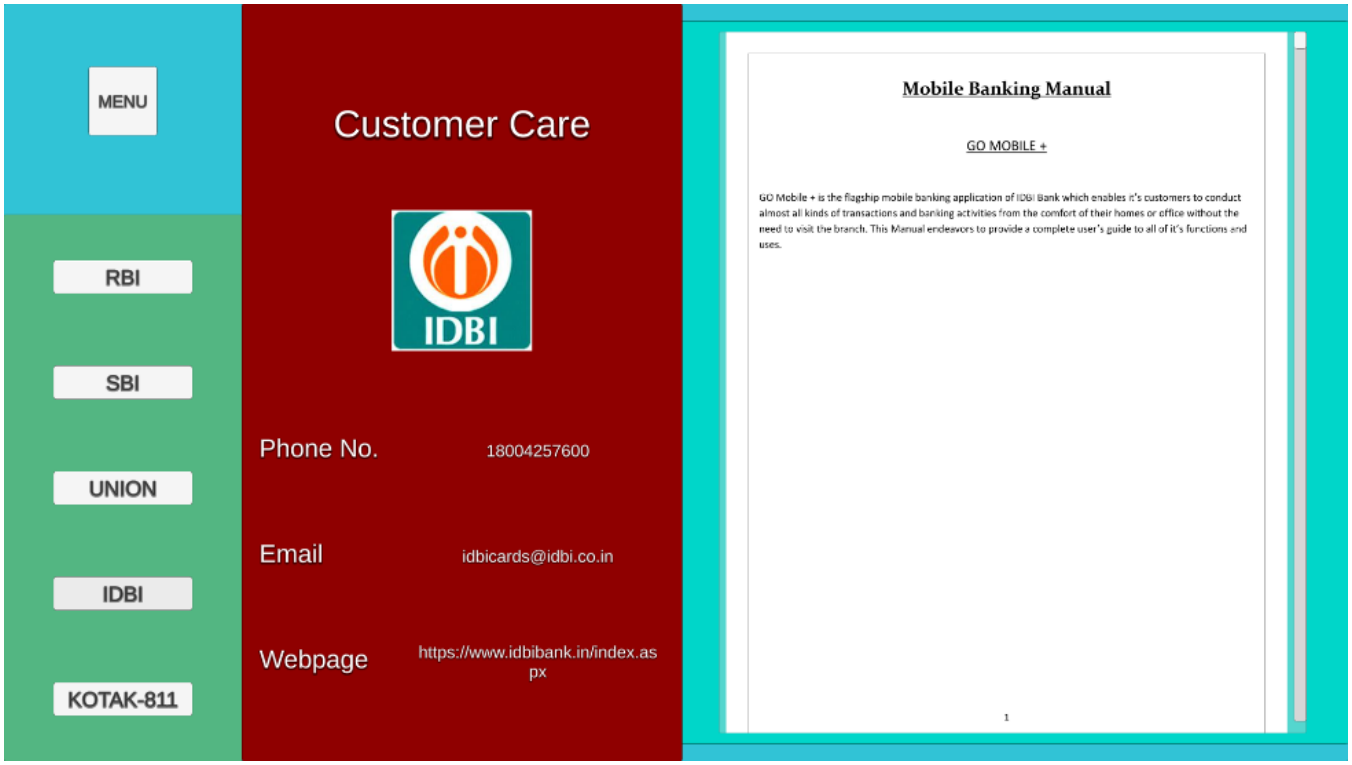
SBI Manual


MENU
RBI
SBI
UNION
IDBI
KOTAK-811
Customer Care
State Bank of India
Phone No.
18004253800
1800112211
Email
gm.customer@sbi.co.in
Webpage
https://www.sbi.co.in/web/personal-banking/home
MobiCash
User Manual
I. Features
Fund transfer to another SBI Wallet or any Bank account
Cash Withdrawal at Customer Service Points of Oxigen
Mobile top up
Bill payment.
DTH/ Broadband recharge.
Balance enquiry.
Mini statement which displays last five transactions.
II. Process for Registration for the Service
State Bank MobiCash Easy (Nil KYC Wallet)
Users of Android phones:
Send SMS <SBMC*DOB(ddmmyy)*NAME> to 98708 88888 or 99718 88888. Default MPIN will be sent as SMS to the same mobile number.
Download the Application
Change the default MPIN.
In case of non Android mobiles, the service can also be used through plain text SMS as under:
Send SMS <SBMCSMS*DOB(ddmmyy)*NAME> to 98708 88888 or 99718 88888. Default MPIN will be sent as SMS to the same mobile number.
Change the default MPIN received by sending SMS <MOBIPIN*Old MPin*New MPin> to 98708 88888 or 99718 88888
Accept Terms and Conditions by sending SMS <ACCEPT>to 98708 88888 or 99718 88888
State Bank MobiCash (Full KYC Wallet)
Being a full KYC Wallet, identity and address proofs are required.
Submit the Wallet Opening Form alongwith identity and address proofs to the Customer Service Point (CSP) of Oxigen.
In the application form, select GPRS or SMS channel for using State Bank MobiCash. The service can be used over one channel only.
Deposit the amount for loading the Mobile Wallet with the CSP.
The Branch linked with the CSP will do the KYC verification. You will be required to visit the linked Branch for completion of the KYC verification along with the originals of the KYC documents submitted to the CSP.
1

UNION Manual

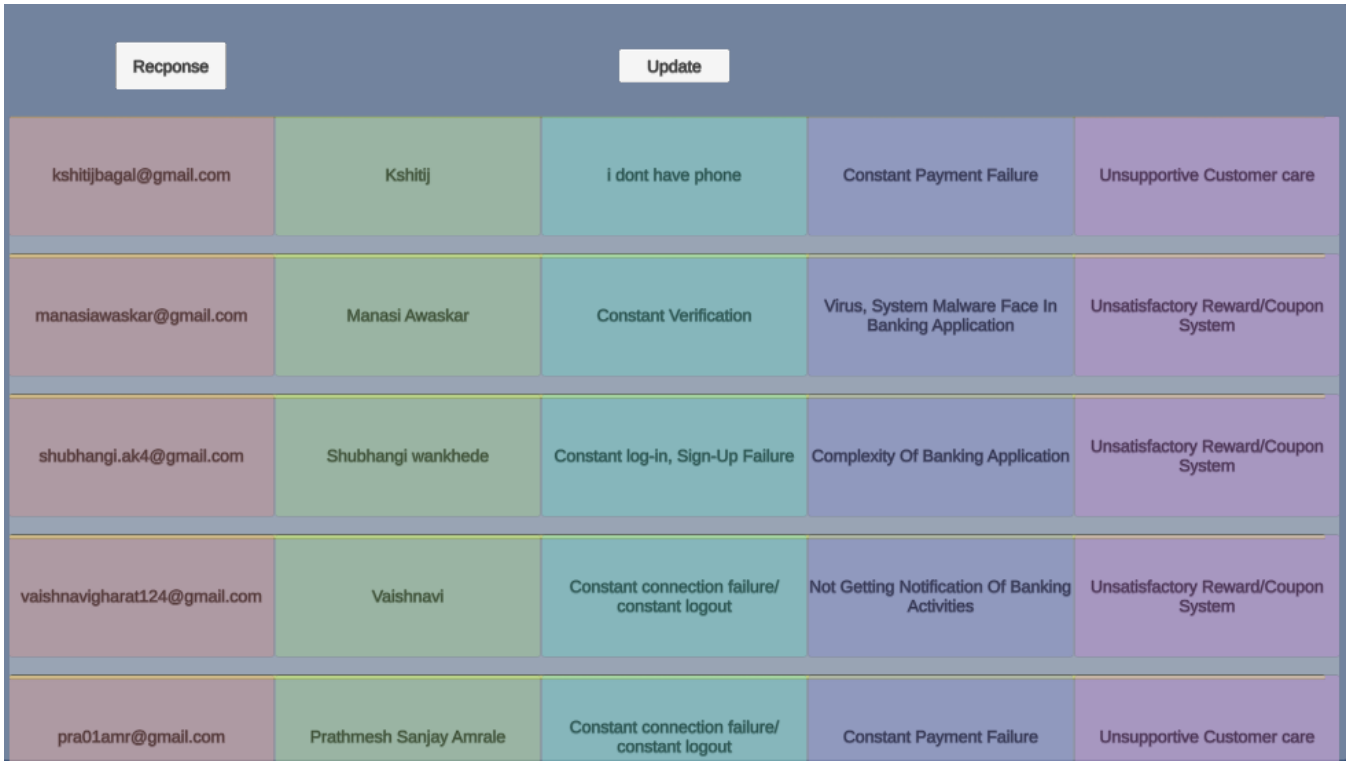


IDBI Manual


MENU
RBI
SBI
UNION
IDBI
KOTAK-811
Customer Care
IDBI
Phone No.
18004257600
Email
idbicards@idbi.co.in
Webpage
https://www.idbibank.in/index.aspx
Mobile Banking Manual
GO MOBILE +
GO Mobile + is the flagship mobile banking application of IDBI Bank which enables it's customers to conduct almost all kinds of transactions and banking activities from the comfort of their homes or office without the need to visit the branch. This Manual endeavors to provide a complete user's guide to all of it's functions and uses.
1

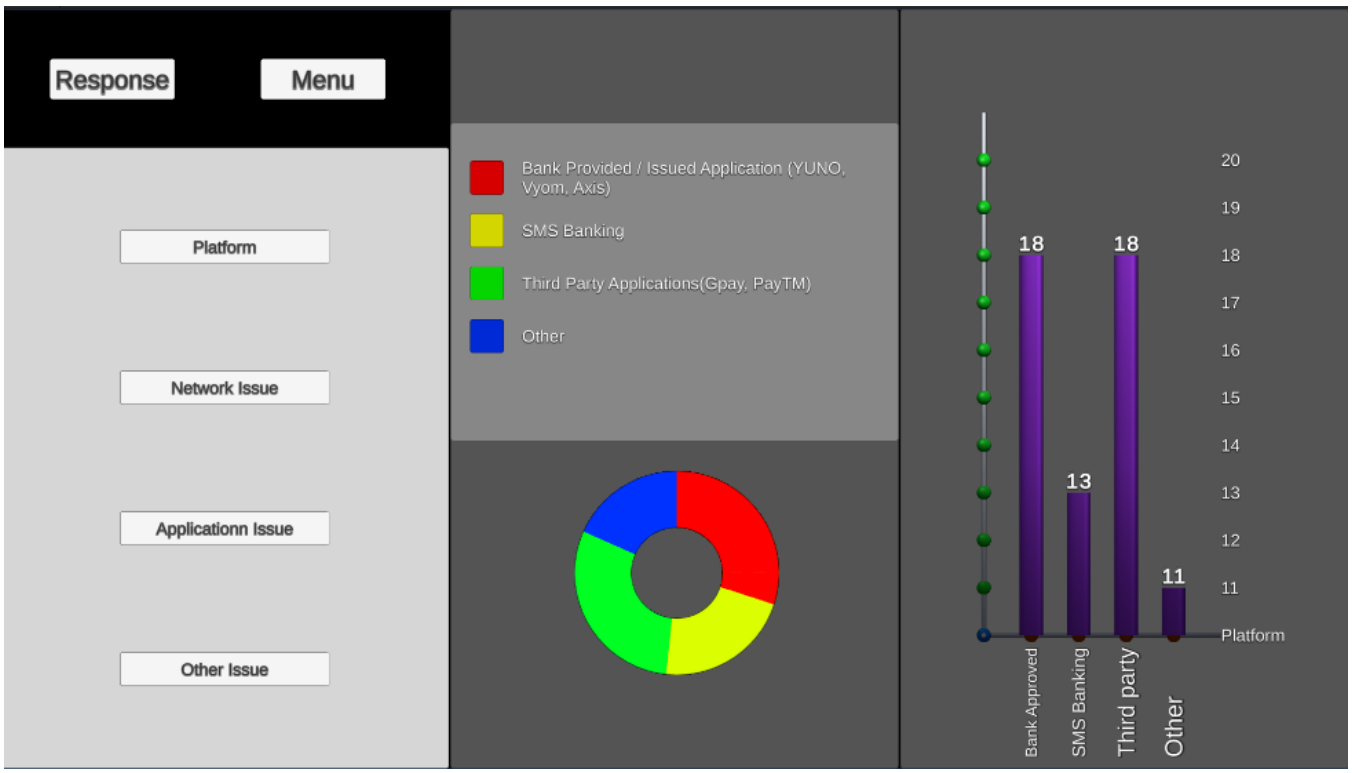
KOTAK-811 Manual

Records: -Here we can see all dataset. after pressing update, we can see latest data entered in dataset.

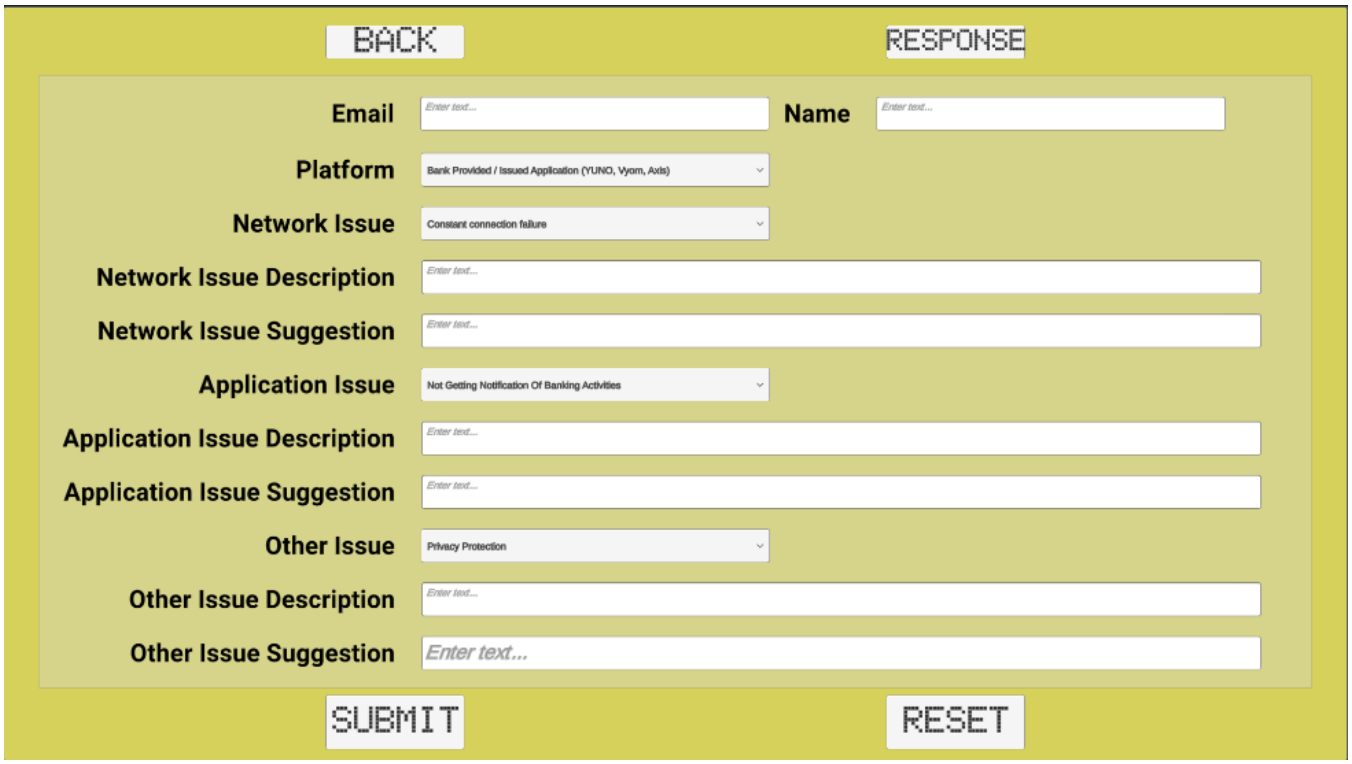


Response: - here we can see all descriptions and suggestions from dataset

ANALYSIS: - Here we can see graphical Visualization of all categorical variable of dataset



FORM: - Here we can enter the new dataset to be added in dataset



CONCLUSION

- This project can offer significant benefits to society by increasing awareness of the risks associated with mobile banking. By highlighting these risks, individuals and businesses can take the necessary precautions to protect their sensitive information and prevent financial loss. Moreover, by proposing counter-measures to address these risks, we can provide practical solutions to mitigate the dangers of mobile banking.

- Through the collection and analysis of statistical data, this project can also contribute to ongoing research efforts to better understand mobile banking risks and develop effective strategies to combat them. Such research can inform future policies and regulations related to mobile banking and enhance the security of financial transactions.

- However, this project does have some limitations. As it is only able to suggest solutions to mobile banking risks, it may not be able to comprehensively address all potential security threats. Additionally, since the project is currently server-based, it cannot directly produce client-based applications, which may limit its effectiveness in some contexts.

- Overall, this project represents an important step towards increasing awareness and promoting best practices in mobile banking security. By working together, we can help safeguard the financial interests of individuals and organizations alike

Future Scope

- Improving the user experience and providing additional features to enhance the functionality of mobile banking. To achieve this, the project team plans to develop a client-server based application, which will enhance the performance and security of the system.
- I have plans about to address some of the basic problems faced with mobile banking, such as ensuring reliable network connectivity and increasing awareness among users about potential security threats.
- To make the mobile banking application more user-friendly and accessible, the team will develop a chat-bot that can assist elderly people in navigating the system. This will help to make the application more inclusive and ensure that everyone can benefit from the convenience of mobile banking.
- I will add basic manual functions to the mobile banking application to provide users with greater control over their finances. These enhancements will ensure that the application remains relevant and useful to users as technology continues to evolve. Overall, the future scope of this project is designed to improve the user experience and meet the changing needs of mobile banking customers.

BIBLIOGRAPHY

[1] Dr. K V D Kiran, M V R Srivatsava, K Gayathri Devi, March – 2014, "Risk Management in Mobile Banking"," International Journal of Engineering Research & Technology (Inert)" Issn: 2278-0181 Vol. 3 Issue 3

[2] Dr. UMESH U, SUBRATA DAS, Dr. RAJIV KUMAR AGARWAL, GOURAB DAS, Dr. D. PAUL DHINAKARAN, Dr. C. VIJAI ,2021," Mobile Banking in India: A Customer Experience Perspective"," Journal of Contemporary Issues in Business and Government", Vol. 27, No. 3

[3] Komlan Gbongli, Yi Peng, Owusu Ackah, January-2016," Selection and Ranking of Perceived Risk Associated with Mobile Banking in West Africa: An AHP Approach from Customers' Perspective."," International Journal of Scientific & Engineering Research,", Volume 7, Issue 1, Issn 2229-5518

[4] Mamta Shah, 1 January-June 2019," A Case Study On Increasing of Banking Frauds in India"," Parichay: Maharaja Surajmal Institute Journal of Applied Research", Vol 2. Issue

[5] Meghna Saikia, 2022," USE OF MOBILE BANKING - A STUDY OF CONSUMER'S PERCEPTION ANALYSIS", "Journal of Positive School Psychology", Vol. 6, No. 2, 5746– 5754

[6] Muhammad Ibrahim, Sayed Fayaz Ahmad, Muhammad Khalil Shahid, Sajjad Akbar, 2015, "Impact of Risk and Ethics On Adoption of Mobile Banking in Pakistan"," Journal of Economics and Sustainable Development Vol.6, No.7," Issn 2222-1700 (Paper) Issn 2222-2855 (Online)

[7] Renju Chandran, October 2014, "Pros and cons of Mobile banking", "International Journal of Scientific and Research Publications", Volume 4, Issue 10

[8] Vishal Goyal, Dr. U. S. Pandey, Sanjay Batra, May – June 2012," Mobile Banking in India: Practices, Challenges and Security Issues"," International Journal of Advanced Trends in Computer Science and Engineering", Volume 1, No.2, ISSN No. 2278 -3091