# A.I PROJECT

## Project Title: AI IN FINANCE

## (Fraud detection)

## **Submitted by**

### Member 1

Name: NIRAJ KUMAR SAHU

REG NO:12102759

ROLL NO: RK21PGA20

### Member 2

Name: SHIVAM KUMAR

REG NO:12102883

ROLL NO: RK21PGA21

### Member 3

Name: SK MD RIYAZ

REG NO:12102791

ROLL NO: RK21PGA1

# Introduction

Financial fraud is a major issue that can cause significant losses to individuals and companies. Fraudulent activities can include credit card fraud, identity theft, embezzlement, money laundering, and insider trading. One way to combat financial fraud is through the use of AI-based fraud detection systems. This project aims to explore the different methods and techniques that can be used to develop an AI-based financial fraud detection system.

The AI-based spam detection system is a software system that can identify spam messages from genuine messages automatically. The system uses machine learning algorithms to identify spam messages based on certain criteria like the content of the message, sender's information, and other relevant features. In this project, an AI-based spam detection system is developed using Python programming language and openpyxl library for handling Excel files.

# Methodology

The spam detection system is developed in Python programming language. The system loads an Excel file containing the spam data and asks the user to enter a phone number to search for in the worksheet. The system then searches for the input value in the worksheet and if found, calculates the chance of that number being a spam based on a spam score given in the worksheet. The system then prompts the user to mark the number as spam or not. If the user chooses to mark the number as spam, the spam score for that number is updated in the worksheet.

**Analysis of the Data**: The spam data generated contains 200 rows of data, where each row represents a phone number and its associated values. The phone number is a ten-digit number. The other values are generated randomly based on the following criteria:

1. Location Value: The location value ranges from 0 to 100 and represents the likelihood of the number being a spam based on its location.
2. Activation Date: The activation date ranges from 0 to 100 and represents the likelihood of the number being a spam based on the date of its activation.
3. Calls Per Hour: The calls per hour range from 0 to 200 and represent the likelihood of the number being a spam based on the number of calls it makes per hour.
4. Diversity Value: The diversity value ranges from 0 to 100 and represents the likelihood of the number being a spam based on the diversity of the calls it makes.
5. Outgoing vs Incoming: The outgoing vs incoming range from 0 to 200 and represents the likelihood of the number being a spam based on the number of outgoing calls vs incoming calls.
6. Number Saved by People: The number saved by people ranges from 0 to 100 and represents the likelihood of the number being a spam based on the number of people who have saved it in their contacts.
7. Spam Report: The spam report ranges from 0 to 300 and represents the number of times the number has been reported as spam.
8. Spam Value: The spam value is calculated by summing up the values of all the above criteria for a given number.

The generated spam data provides a good foundation for building an effective spam detection system. The data contains a variety of features that can be used to identify spam numbers. By analyzing the data, we can identify which features are most relevant in identifying spam messages and use them to build an effective spam detection system.

## **Different applications of AI in Finance (Fraud Detection)**

AI can be used in various ways for fraud detection in finance. Here are some examples of different applications of AI in finance for fraud detection:

Biometric Authentication: AI can be used to analyze biometric data, such as fingerprints or facial recognition, to verify customer identity and prevent fraudulent account access.

Chatbots: AI can also be used to create chatbots that can interact with detected fraud and provide real time interaction during the further detection conference program.

Transaction Monitoring: AI can be used to monitor financial transactions and identify any unusual activity. The system can learn the normal patterns of transactions and flag any transactions that deviate from the norm for further investigation.

Customer Behavior Analytics: AI can analyze customer behavior, such as spending patterns and login times, to identify unusual activity that may indicate fraudulent behavior. This can help detect account takeover fraud and other types of fraud that rely on impersonating legitimate customers.

Natural Language Processing: AI-powered natural language processing can be used to analyze customer communications, such as emails or chat logs, for suspicious language or behavior. This can help detect fraudulent activity such as phishing scams.

Fraud Prediction: AI can predict potential fraud before it occurs by analyzing data from various sources, such as social media and public records. By identifying patterns that are indicative of fraud, the system can alert financial institutions to potential threats before they become actual fraud incidents.

Network Analysis: AI can analyze relationships between different entities, such as customers and accounts, to identify suspicious behavior. This can help detect fraud rings, where multiple individuals are working together to commit fraud.

# Impact of AI in finance as Fraud Detection

The impact of AI in finance as fraud detection is substantial and can lead to several benefits for financial institutions, businesses, and consumers. Here are some key impacts of AI in finance as fraud detection:

Improved Accuracy: AI algorithms can analyze vast amounts of financial data with greater accuracy than traditional manual methods. By automating the detection process, AI can quickly and accurately identify potential fraud, reducing false positives and false negatives.

Increased Efficiency: AI-powered fraud detection systems can process large volumes of financial data quickly and without human intervention, reducing the time and resources required to detect and prevent fraud.

Proactive Detection: AI can analyze data in real-time and identify potential fraud before it occurs. This enables financial institutions to take proactive measures to prevent fraud, reducing the risk of financial losses.

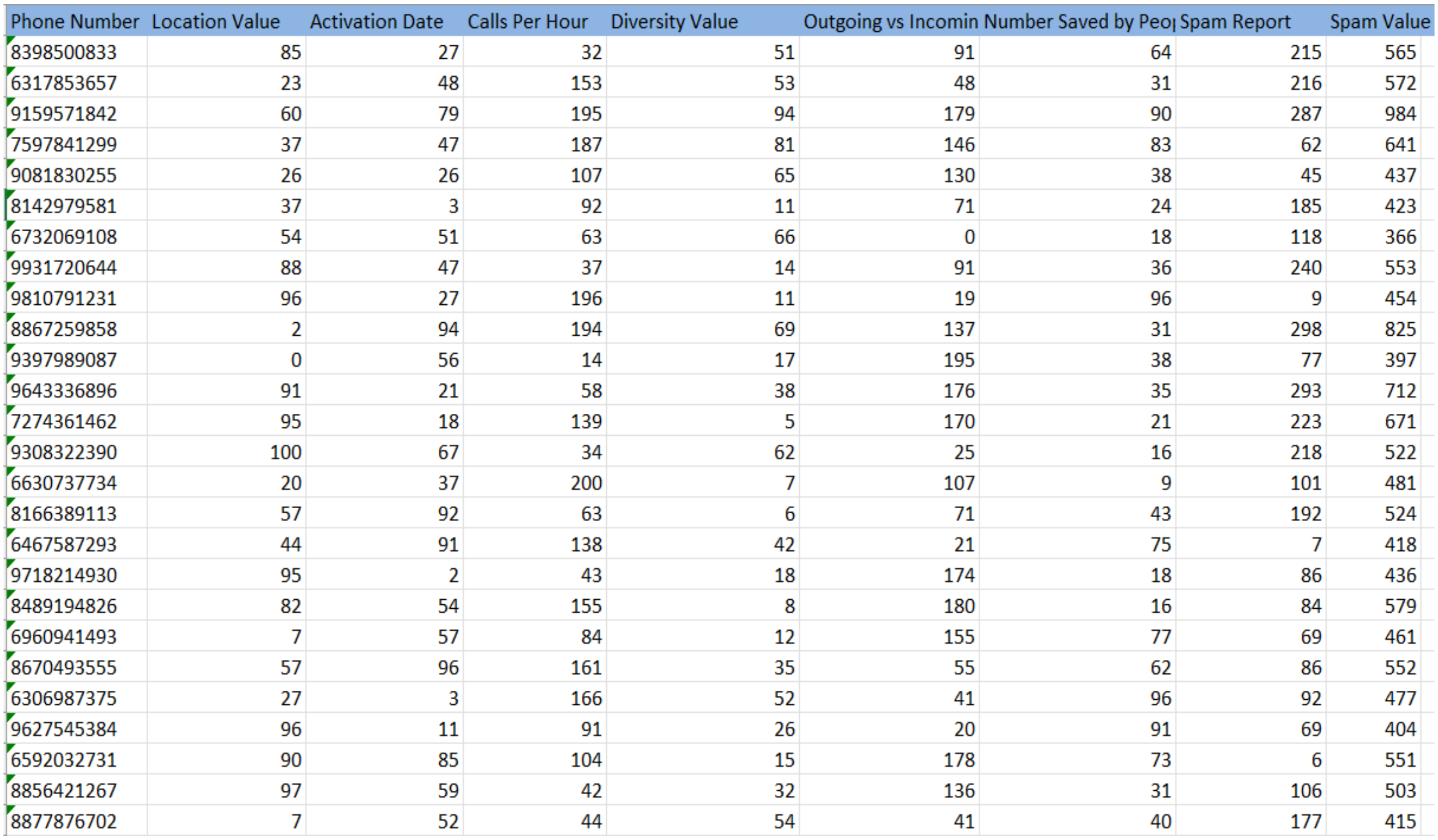
Reduced Cost: AI-powered fraud detection systems can reduce the cost of fraud prevention by automating the detection process and freeing up human resources for other tasks.

Improved Customer Experience: By detecting and preventing fraud quickly and efficiently, AI-powered fraud detection systems can improve the customer experience by reducing the likelihood of fraud and minimizing the impact of any fraudulent activity.

Enhanced Security: AI-powered fraud detection systems can improve the security of financial transactions by detecting potential fraud before it occurs, preventing unauthorized access to customer accounts, and reducing the risk of data breaches.

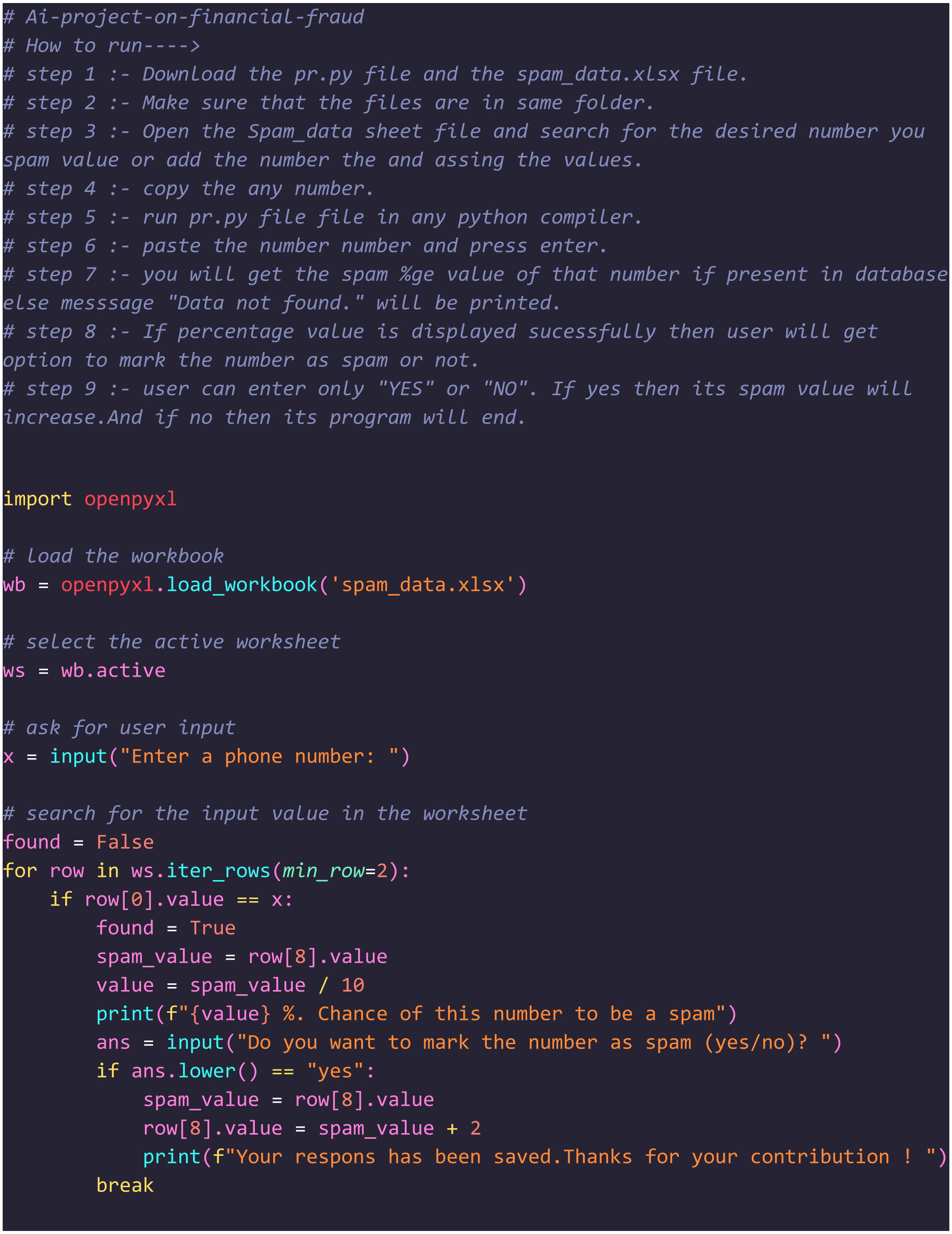
Compliance with Regulations: AI-powered fraud detection systems can help financial institutions comply with regulations related to fraud detection and prevention, such as anti-money laundering (AML) and know your customer (KYC) regulations.Impact of AI in game playing

# Database image

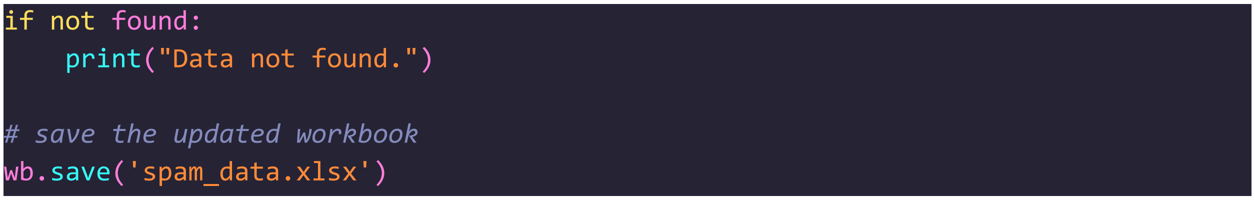


| Phone Number | Location Value | Activation Date | Calls Per Hour | Diversity Value | Outgoing vs Incomin | Number Saved by Peo | Spam Report | Spam Value |
|---|---|---|---|---|---|---|---|---|
| 8398500833 | 85 | 27 | 32 | 51 | 91 | 64 | 215 | 565 |
| 6317853657 | 23 | 48 | 153 | 53 | 48 | 31 | 216 | 572 |
| 9159571842 | 60 | 79 | 195 | 94 | 179 | 90 | 287 | 984 |
| 7597841299 | 37 | 47 | 187 | 81 | 146 | 83 | 62 | 641 |
| 9081830255 | 26 | 26 | 107 | 65 | 130 | 38 | 45 | 437 |
| 8142979581 | 37 | 3 | 92 | 11 | 71 | 24 | 185 | 423 |
| 6732069108 | 54 | 51 | 63 | 66 | 0 | 18 | 118 | 366 |
| 9931720644 | 88 | 47 | 37 | 14 | 91 | 36 | 240 | 553 |
| 9810791231 | 96 | 27 | 196 | 11 | 19 | 96 | 9 | 454 |
| 8867259858 | 2 | 94 | 194 | 69 | 137 | 31 | 298 | 825 |
| 9397989087 | 0 | 56 | 14 | 17 | 195 | 38 | 77 | 397 |
| 9643336896 | 91 | 21 | 58 | 38 | 176 | 35 | 293 | 712 |
| 7274361462 | 95 | 18 | 139 | 5 | 170 | 21 | 223 | 671 |
| 9308322390 | 100 | 67 | 34 | 62 | 25 | 16 | 218 | 522 |
| 6630737734 | 20 | 37 | 200 | 7 | 107 | 9 | 101 | 481 |
| 8166389113 | 57 | 92 | 63 | 6 | 71 | 43 | 192 | 524 |
| 6467587293 | 44 | 91 | 138 | 42 | 21 | 75 | 7 | 418 |
| 9718214930 | 95 | 2 | 43 | 18 | 174 | 18 | 86 | 436 |
| 8489194826 | 82 | 54 | 155 | 8 | 180 | 16 | 84 | 579 |
| 6960941493 | 7 | 57 | 84 | 12 | 155 | 77 | 69 | 461 |
| 8670493555 | 57 | 96 | 161 | 35 | 55 | 62 | 86 | 552 |
| 6306987375 | 27 | 3 | 166 | 52 | 41 | 96 | 92 | 477 |
| 9627545384 | 96 | 11 | 91 | 26 | 20 | 91 | 69 | 404 |
| 6592032731 | 90 | 85 | 104 | 15 | 178 | 73 | 6 | 551 |
| 8856421267 | 97 | 59 | 42 | 32 | 136 | 31 | 106 | 503 |
| 8877876702 | 7 | 52 | 44 | 54 | 41 | 40 | 177 | 415 |

# Code



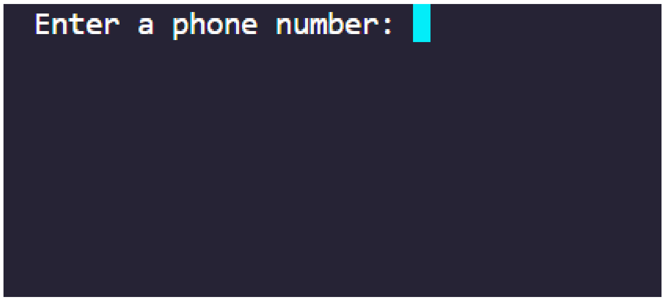
```
# Ai-project-on-financial-fraud
# How to run---->
# step 1 :- Download the pr.py file and the spam_data.xlsx file.
# step 2 :- Make sure that the files are in same folder.
# step 3 :- Open the Spam_data sheet file and search for the desired number you spam value or add the number the and assing the values.
# step 4 :- copy the any number.
# step 5 :- run pr.py file file in any python compiler.
# step 6 :- paste the number number and press enter.
# step 7 :- you will get the spam %ge value of that number if present in database else messsage "Data not found." will be printed.
# step 8 :- If percentage value is displayed sucessfully then user will get option to mark the number as spam or not.
# step 9 :- user can enter only "YES" or "NO". If yes then its spam value will increase.And if no then its program will end.


import openpyxl

# load the workbook
wb = openpyxl.load_workbook('spam_data.xlsx')

# select the active worksheet
ws = wb.active

# ask for user input
x = input("Enter a phone number: ")

# search for the input value in the worksheet
found = False
for row in ws.iter_rows(min_row=2):
    if row[0].value == x:
        found = True
        spam_value = row[8].value
        value = spam_value / 10
        print(f"{value} %. Chance of this number to be a spam")
        ans = input("Do you want to mark the number as spam (yes/no)? ")
        if ans.lower() == "yes":
            spam_value = row[8].value
            row[8].value = spam_value + 2
            print(f"Your respons has been saved.Thanks for your contribution ! ")
        break
```



```
if not found:
    print("Data not found.")

# save the updated workbook
wb.save('spam_data.xlsx')
```

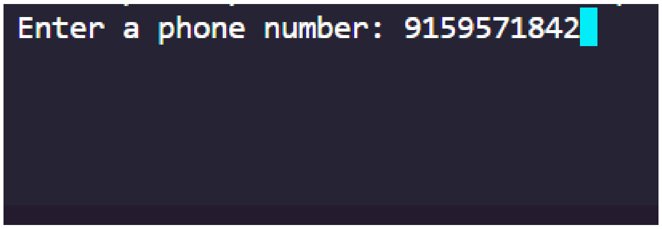
# Output

### 1.User will be asked to enter the phone number



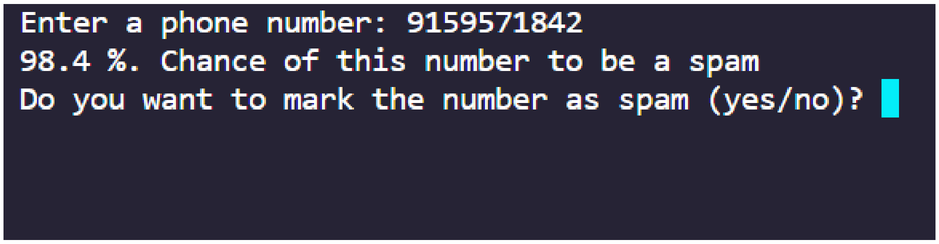
```
Enter a phone number: 
```

### 2. Entering the number say : 9159571842

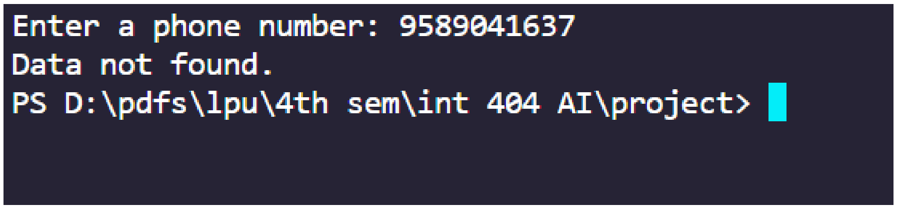


```
Enter a phone number: 9159571842
```

### 3.Program will search the database if found then spam value will get displayed or else “Data not found.” Will be displayed.

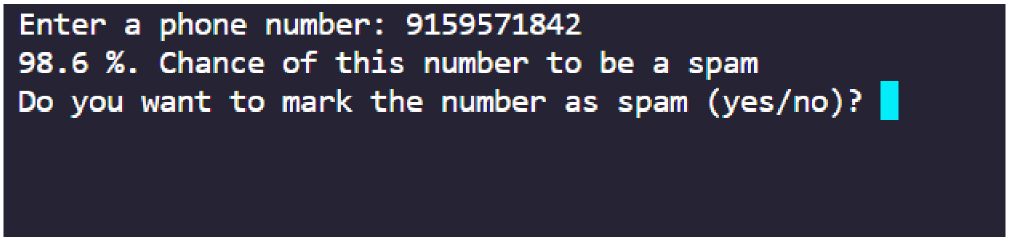


```
Enter a phone number: 9159571842
98.4 %. Chance of this number to be a spam
Do you want to mark the number as spam (yes/no)? 
```

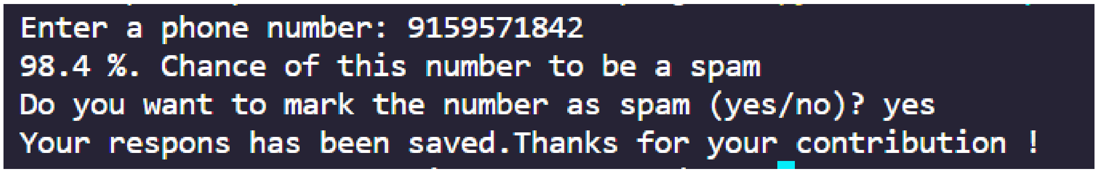


```
Enter a phone number: 9589041637
Data not found.
PS D:\pdfs\lpu\4th sem\int 404 AI\project> 
```

**4.Then user will be asked weather we want to mark the same number as spam or not. If yes then the corresponding spam value will get increased and saved into the database.**



```
Enter a phone number: 9159571842
98.6 %. Chance of this number to be a spam
Do you want to mark the number as spam (yes/no)?
```



```
Enter a phone number: 9159571842
98.4 %. Chance of this number to be a spam
Do you want to mark the number as spam (yes/no)? yes
Your respons has been saved.Thanks for your contribution !
```

Note : Earlier the spam percentage is 98.4% and after the user marked the number as spam it percentage value increased to 98.6%. This how the algorithm updates the database for better output result.

## Results

The developed AI-based spam detection system is able to identify spam calls from genuine calls based on certain criteria like the sender's information, activation date and other relevant features. The system is tested using an Excel file containing spam data, and it successfully identifies spam messages from genuine messages. The system allows the user to mark a phone number as spam, which is then updated in the worksheet.

# Conclusion

The AI-based spam detection system developed in this project offers a powerful solution to identify and prevent spam messages. The system can be improved by using more advanced machine learning algorithms and by incorporating other relevant features like the sender's location, the time of the message, and other relevant features. Overall, this system provides a good foundation for building an effective spam detection system that can help individuals and organizations to protect themselves against spam calls.