SQA ASSIGNMENT-1

EMAIL SPAM DETECTION ASSISTANT

DONE BY

CHANDRU N P

III YEAR IT-B

113222071012

INTRODUCTION

I hope this message finds you well. I am excited to share with you an overview of our recent project on email spam detection using machine learning (ML). In today's digital age, where email remains a primary mode of communication, ensuring inbox security and efficiency is paramount. Our project focuses on leveraging advanced ML techniques to enhance the accuracy and effectiveness of spam detection.

Steps and Quality Assurance(SQA)

1. **Define Objectives and Use Cases:**
    - Gathering a comprehensive dataset of labeled emails (spam and non-spam) to train our ML models.
    - Identify the target audience and their needs.

2.Data Collection and Preparation:

- Extracting relevant features from email content, metadata, and sender information to enhance classification accuracy.
- Clean and preprocess data to ensure it is accurate and suitable for training models.

3.Natural Language Understanding (NLU):

- Develop algorithms and models for speech recognition and text understanding.
- Implement techniques such as machine learning and NLP to interpret user queries accurately.

4.Task Execution and Integration:

Evaluating and selecting appropriate ML algorithms(such as Naive Bayes, Support Vector Machines, or Neural Networks) for training robust spam detection.

5.User Interface and Experience Design:

- Improving our ability to detect and filter out spam emails, thereby reducing potential security threats such as phishing and malware.
- Ensure usability and accessibility for different user demographics.

6.Testing and Evaluation:

- Integrating the developed models into our existing email systems and conducting rigorous testing to ensure reliability and performance.
- Perform stress testing to evaluate performance under high load or unusual conditions.

7.Deployment and Monitoring:

- Monitor performance and user feedback to identify areas for improvement.

CODE:

```python
# importing require Libraries
from sklearn.feature_extraction.text import CountVectorizer
from sklearn.model_selection import train_test_split
from sklearn.naive_bayes import MultinomialNB
from sklearn.metrics import accuracy_score, classification_report

# In this example, we create a small dataset of email text and Labels ( for not spam, 1 for spam)
emails = {
"Get rich Quick! Click here to win a million dollars!",
"Hello, could you please review this document for me",
"Discounts on luxuray watches and handbages!",
"Meeting scheduled for tommorow, please confirm your attendance.",
"Congratulations, you've won a free gift card!",
}

labels=[1,0,1,0,1]

# convert text dato into numerical features using Count vectorization
vectorizer =CountVectorizer()
x=vectorizer.fit_transform(emails)

# split the data into training and testing sets
x_train,x_test,y_train,y_test=train_test_split(x,labels,test_size=0.2)

# create a multinomial noive bayes classifier
model =MultinomialNB()
```

✓ 1s completed at 10:56 PM

```python
# train the model on training data
model.fit(x_train,y_train)

# make prediction on test data
y_pred=model.predict(x_test)

# evaluate the model
accuracy=accuracy_score(y_test,y_pred)
report=classification_report(y_test,y_pred)

print("Accuracy:",accuracy)
print("classification Report:\n",report)

# predict whether a new email is spam or not
new_email=["you've won a free cruise vacation"]
new_email_vectorized=vectorizer.transform(new_email)
predicted_label=model.predict(new_email_vectorized)

if predicted_label[0]==0:
    print("predicted as not spam")
else:
    print("predicted as spam")
```

OUTPUT:

```
Accuracy: 1.0
classification Report:
              precision    recall  f1-score   support

           1       1.00      1.00      1.00         1

    accuracy                           1.00         1
   macro avg       1.00      1.00      1.00         1
weighted avg       1.00      1.00      1.00         1

predicted as spam
```

CONCLUTION:

In our ongoing efforts to implement and refine our email spam detection system mark a significant step forward in enhancing the security and efficiency of our communication channels. By leveraging advanced machine learning algorithms and robust data preprocessing techniques, we have successfully developed a system capable of effectively filtering out spam while minimizing false positives.