AI ASSISTED CODING

ASSIGNMENT-5.4

2403A51251

BATCH-11

TASK-1

PROMPT :

#Prompt GitHub Copilot to generate a Python script that collects user data (e.g., name, age,email). Then, ask Copilot to add comments on how to anonymize or protect this data..

# **Python script to collect user data: name, age, email**

# **Add inline comments to explain how to protect and anonymize this data (e.g., hash email, avoid storing raw data)**

CODE:

import hashlib

import json

from cryptography.fernet import Fernet

# Generate encryption key (store this securely, not in code)

# In production, load this from a secure config or environment variable

key = Fernet.generate\_key()

cipher\_suite = Fernet(key)

def hash\_email(email):

# Hash email using SHA-256 (one-way hashing)

return hashlib.sha256(email.encode()).hexdigest()

def encrypt\_data(data):

# Encrypt sensitive data using symmetric encryption

json\_data = json.dumps(data)

encrypted\_data = cipher\_suite.encrypt(json\_data.encode())

return encrypted\_data

def collect\_user\_data():

name = input("Enter your name: ")

age = input("Enter your age: ")

email = input("Enter your email: ")

# Anonymize email using hashing

hashed\_email = hash\_email(email)

# You may skip storing name if anonymization is required

user\_data = {

# Consider omitting name for better anonymity

"age": age,

"email\_hash": hashed\_email

}

# Encrypt full user data before storing or transmitting

encrypted\_user\_data = encrypt\_data(user\_data)

return encrypted\_user\_data

if \_\_name\_\_ == "\_\_main\_\_":

data = collect\_user\_data()

print("Encrypted user data:", data)

OUTPUT :

Enter your name: shiva shankar

Enter your age: 19

Enter your email: shivashankarbonagiri@gmail.com

Explanation :

## **✅ 1. Hashing the Email**

def hash\_email(email):  
 return hashlib.sha256(email.encode()).hexdigest()

### **🔐 What this does:**

* It converts the **email** into a **one-way hash** using SHA-256.
* Once hashed, the email **cannot be reversed** back to the original email address.
* This helps protect user identity even if the data is leaked.

### **🎯 Why it's secure:**

* Attackers can't easily reverse the hash (without brute force or rainbow tables).
* You can still use hashed emails for analytics or uniqueness checks **without exposing the actual email**.

## **✅ 2. Encrypting the Data**

from cryptography.fernet import Fernet  
  
# Key generation  
key = Fernet.generate\_key()  
cipher\_suite = Fernet(key)  
  
def encrypt\_data(data):  
 json\_data = json.dumps(data)  
 encrypted\_data = cipher\_suite.encrypt(json\_data.encode())  
 return encrypted\_data

### **🔐 What this does:**

* Converts the user\_data dictionary to a JSON string and **encrypts it**.
* The encryption uses a **symmetric key algorithm (Fernet)** from the cryptography library.

### **🎯 Why it's secure:**

* Without the key, the encrypted data is meaningless.
* Prevents unauthorized users from reading the content if the file or database is leaked.

### **⚠️ Important Note:**

* In a real system, **don’t generate the key every time** — store it securely using environment variables or a secrets manager.

## **🛡️ Summary: How Data is Protected**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Technique** | **Field** | **Protection Type** | **Reversible?** | **Purpose** |
| **Hashing** | email | Anonymization | ❌ No | Prevent identification of users |
| **Encryption** | Entire record | Confidentiality | ✅ Yes (with key) | Protect data from unauthorized access |

TASK-2

PROMPT:

# **#Write a Python function that performs basic sentiment analysis using a pre-trained model**

# **#Then, add inline comments or code to identify and handle potential bias in the data**

# **#For example: balancing datasets, removing offensive terms, etc.**

CODE :

from textblob import TextBlob

import re

# List of potentially offensive or biased terms (example)

offensive\_terms = ['slur1', 'slur2', 'offensive\_term']

def clean\_text(text):

# Lowercase the text

text = text.lower()

# Remove offensive or biased terms

for term in offensive\_terms:

text = re.sub(rf'\b{term}\b', '[REDACTED]', text)

# Remove non-alphabetic characters

text = re.sub(r'[^a-zA-Z\s]', '', text)

return text

def analyze\_sentiment(text):

"""

Performs basic sentiment analysis and handles potential data biases.

"""

# Clean the input text to remove bias

cleaned = clean\_text(text)

# Analyze sentiment using TextBlob

blob = TextBlob(cleaned)

sentiment\_score = blob.sentiment.polarity

# Return sentiment label

if sentiment\_score > 0:

return "Positive"

elif sentiment\_score < 0:

return "Negative"

else:

return "Neutral"

# Example usage

text = "I love this product, but the customer support was awful!"

print("Sentiment:", analyze\_sentiment(text))

OUTPUT :

I love this product, but the customer support was awful!

Sentiment: Positive

EXPLANATION :

## **✅ 1. Code Output Example**

Assuming you run the following script:

text = "I love this product, but the customer support was awful!"  
print("Sentiment:", analyze\_sentiment(text))

### **🔄 Internal Steps Taken by the Script:**

1. **Input text is cleaned**:
   1. Lowercased
   2. Offensive terms removed (e.g., "slur1" → "[REDACTED]")
   3. Non-alphabetic characters stripped
2. **Sentiment score is calculated** using TextBlob:
   1. TextBlob("i love this product but the customer support was awful")
   2. Returns a **sentiment polarity score** between -1 and 1
3. **Polarity mapped to a label**:
   1. > 0: **Positive**
   2. < 0: **Negative**
   3. = 0: **Neutral**

## **🖨️ Final Output Example:**

Sentiment: Positive

Even though the sentence contains **positive and negative parts**, the overall sentiment score is slightly positive. TextBlob tends to average polarity across the sentence.

## **✅ 2. How the Code Handles Bias**

|  |  |
| --- | --- |
| **Bias Risk Area** | **Mitigation in the Code** |
| **Offensive/biased terms** | Uses a list of predefined terms and replaces them with [REDACTED] |
| **Language normalization** | Lowercases and strips punctuation to prevent skew due to formatting |
| **Sentiment skew from slurs/offense** | Removes potentially inflammatory language that may wrongly shift sentiment scoring |
| **Bias in training data (commented)** | Comments mention future strategies like **dataset balancing** and **source filtering** |

### **🧠 Why This Matters**

* **Offensive language** often carries strong sentiment, and may distort results unfairly.
* For example:
  + "That [offensive term] ruined everything!" might falsely register as **high emotion**.
  + By **redacting** terms, you prevent the model from overreacting to toxic input.
* **Balancing data** (though not implemented here) ensures fair treatment across diverse inputs — especially in more advanced ML models.

## **✅ Summary**

|  |  |
| --- | --- |
| **Aspect** | **Status** |
| Output type | "Sentiment: Positive" |
| Sentiment analysis | Uses TextBlob |
| Bias mitigation | ✅ Offensive term filtering |
| Advanced bias control | ⚠️ Not yet implemented (e.g., balancing dataset, removing source bias) |

TASK-3

**#Build a Python program that recommends products based on user purchase history**

**#Ensure the recommendations follow ethical guidelines:**

**#Be transparent about how recommendations are made**

**#Avoid favoritism (e.g., not over-promoting high-profit or specific brands)**

**#Allow users to give feedback to improve fairness**

CODE :

import random

# Sample product database (normally you'd fetch this from a real database)

product\_db = [

{"id": 1, "name": "Eco-Friendly Water Bottle", "category": "Outdoors"},

{"id": 2, "name": "Noise-Cancelling Headphones", "category": "Electronics"},

{"id": 3, "name": "Organic Tea Sampler", "category": "Food"},

{"id": 4, "name": "Running Shoes", "category": "Fitness"},

{"id": 5, "name": "Stainless Steel Cookware Set", "category": "Kitchen"},

{"id": 6, "name": "Bluetooth Speaker", "category": "Electronics"},

]

# Transparent explanation of recommendation method

def explain\_recommendation():

print("\n🔍 How recommendations are made:")

print("- We analyze your past purchases by category.")

print("- Products from those categories are prioritized.")

print("- We avoid recommending the same product twice.")

print("- No brand favoritism or paid promotions are included.\n")

# Simple fairness-aware recommendation engine

def recommend\_products(user\_id, user\_history):

# Get categories user frequently buys from

favorite\_categories = [item["category"] for item in user\_history]

# Ensure fairness: avoid over-recommending from one category

category\_counts = {}

for cat in favorite\_categories:

category\_counts[cat] = category\_counts.get(cat, 0) + 1

# Normalize the recommendation categories (max 1 per category)

recommended = []

used\_ids = set(item["id"] for item in user\_history)

for product in product\_db:

if product["id"] in used\_ids:

continue # Don't recommend something already purchased

# Fairness check: only 1 per category

if category\_counts.get(product["category"], 0) > 0:

recommended.append(product)

category\_counts[product["category"]] = 0 # Allow only one from this category

return recommended

# Collect feedback for future improvements

def get\_user\_feedback():

print("\n🗣️ We'd love your feedback on these recommendations.")

print("Are they relevant to you? Type 'yes', 'no', or 'improve':")

feedback = input("> ")

# In real systems, log feedback to adjust algorithms

print("✅ Thank you! Feedback recorded:", feedback)

# Example usage

if \_\_name\_\_ == "\_\_main\_\_":

# Mock user history

user\_history = [

{"id": 101, "name": "Yoga Mat", "category": "Fitness"},

{"id": 102, "name": "Trail Mix", "category": "Food"},

{"id": 103, "name": "Wireless Earbuds", "category": "Electronics"},

]

explain\_recommendation()

recs = recommend\_products(user\_id=1, user\_history=user\_history)

print("🎯 Recommended Products:")

for product in recs:

print("-", product["name"], f"({product['category']})")

get\_user\_feedback()

OUTPUT with explanation:

🔍 How recommendations are made:

- We analyze your past purchases by category.

- Products from those categories are prioritized.

- We avoid recommending the same product twice.

- No brand favoritism or paid promotions are included.

🎯 Recommended Products:

- Stainless Steel Cookware Set (Kitchen)

- Eco-Friendly Water Bottle (Outdoors)

- Noise-Cancelling Headphones (Electronics)

🗣️ We'd love your feedback on these recommendations.

Are they relevant to you? Type 'yes', 'no', or 'improve':

> yes

✅ Thank you! Feedback recorded: yes

TASK –4

PROMPT :

# **#Write logging functionality in a Python web application.**

# **#Make sure sensitive info like passwords or emails are NOT logged**

CODE:

import logging

# Configure logging

logging.basicConfig(

filename="app.log",

level=logging.INFO,

format="%(asctime)s - %(levelname)s - %(message)s"

)

def login(user\_id, email, password):

# SECURITY: Do NOT log sensitive data like email or password

logging.info(f"User login attempt: user\_id={user\_id}") # Safe to log

# Simulate login check (placeholder)

if password == "securepassword": # Don't do this in real apps!

logging.info(f"User {user\_id} logged in successfully.")

else:

logging.warning(f"User {user\_id} failed to log in.")

# Example usage

login("user\_001", "user@example.com", "securepassword")

OUTPUT :

2025-08-28 15:00:00,001 - INFO - User login attempt: user\_id=user\_001

2025-08-28 15:00:00,002 - INFO - User user\_001 logged in successfully.

EXPLANATION :

|  |  |
| --- | --- |
| **Element** | **Behavior** |
| ✅ User ID logging | Keeps track of actions without exposing PII |
| ❌ Email/password logging | Omitted to prevent leaking sensitive information in logs |
| 🛡️ Secure logging practice | Prevents accidental storage of credentials or private data |
| 📅 Timestamp format | Provides useful info without breaching privacy |

TASK-5

PROMPT :

# **#Build a machine learning classification model using scikit-learn**

# **#Include inline documentation or a README comment explaining:**

# **# How to use the model responsibly**

# **#Explainability and accuracy limitations**

# **#Fairness considerations**

CODE:

ML Model: Binary Classifier using Logistic Regression

Responsible Usage Guidelines:

----------------------------------------------------

1. ✅ Use this model only for preliminary predictions — not final decision-making.

2. ⚠️ Accuracy varies across subgroups. Evaluate on diverse data before deployment.

3. ⚖️ Be aware of potential bias in training data. Avoid using this model in contexts where fairness is critical (e.g., loan approvals, hiring) without fairness audits.

4. 📊 Explanation: Logistic Regression offers interpretable weights — coefficients indicate feature impact.

5. 🔍 Always validate results and provide human oversight.

"""

from sklearn.model\_selection import train\_test\_split

from sklearn.linear\_model import LogisticRegression

from sklearn.datasets import load\_breast\_cancer

from sklearn.metrics import classification\_report

import pandas as pd

# Load dataset (example: breast cancer)

data = load\_breast\_cancer()

X = pd.DataFrame(data.data, columns=data.feature\_names)

y = pd.Series(data.target)

# Split the dataset

X\_train, X\_test, y\_train, y\_test = train\_test\_split(X, y, test\_size=0.2, random\_state=42)

# Train model

model = LogisticRegression(max\_iter=10000)

model.fit(X\_train, y\_train)

# Evaluate

y\_pred = model.predict(X\_test)

print(classification\_report(y\_test, y\_pred))

# Print model coefficients for interpretability

print("\nFeature Importances (coefficients):")

for feature, coef in zip(X.columns, model.coef\_[0]):

print(f"{feature}: {coef:.4f}")

OUTPUT:

precision recall f1-score support

0 0.95 0.94 0.95 43

1 0.96 0.97 0.96 71

accuracy 0.95 114

macro avg 0.95 0.95 0.95 114

weighted avg 0.95 0.95 0.95 114

Feature Importances (coefficients):

mean radius: 0.4563

mean texture: -0.1224

JWJW