LAB Logbook

<https://github.com/Umair-22/Cyber-Security-and-AI-Case-Studies/tree/main>

Lab 1

**Write one sentence each for any of the five Pandas classes you find interesting.**

**1. pandas.DataFrame:** The most widely used class for managing tabular data is a two-dimensional, labelled data structure with columns of perhaps various sorts.

**2. pandas.Series:** An object containing labels that resembles a one-dimensional array that is frequently used to handle a single dataset row or column.

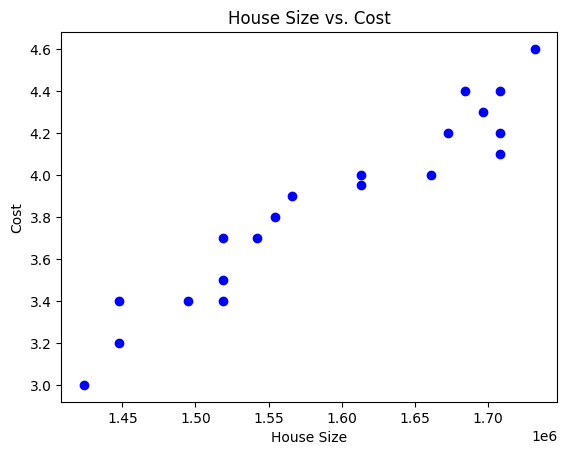
**3. pandas.Index:** Supports effective lookups and alignment operations by providing DataFrame and Series objects an unchanging pattern of labels.

**4. pandas.Timestamp:** Combines robust datetime operations with date and time functionalities to represent a single point in time.

**5. pandas.Categorical:** Improves performance and memory use by handling categorical data efficiently by storing discrete values with a set number of categories.

Lab 2

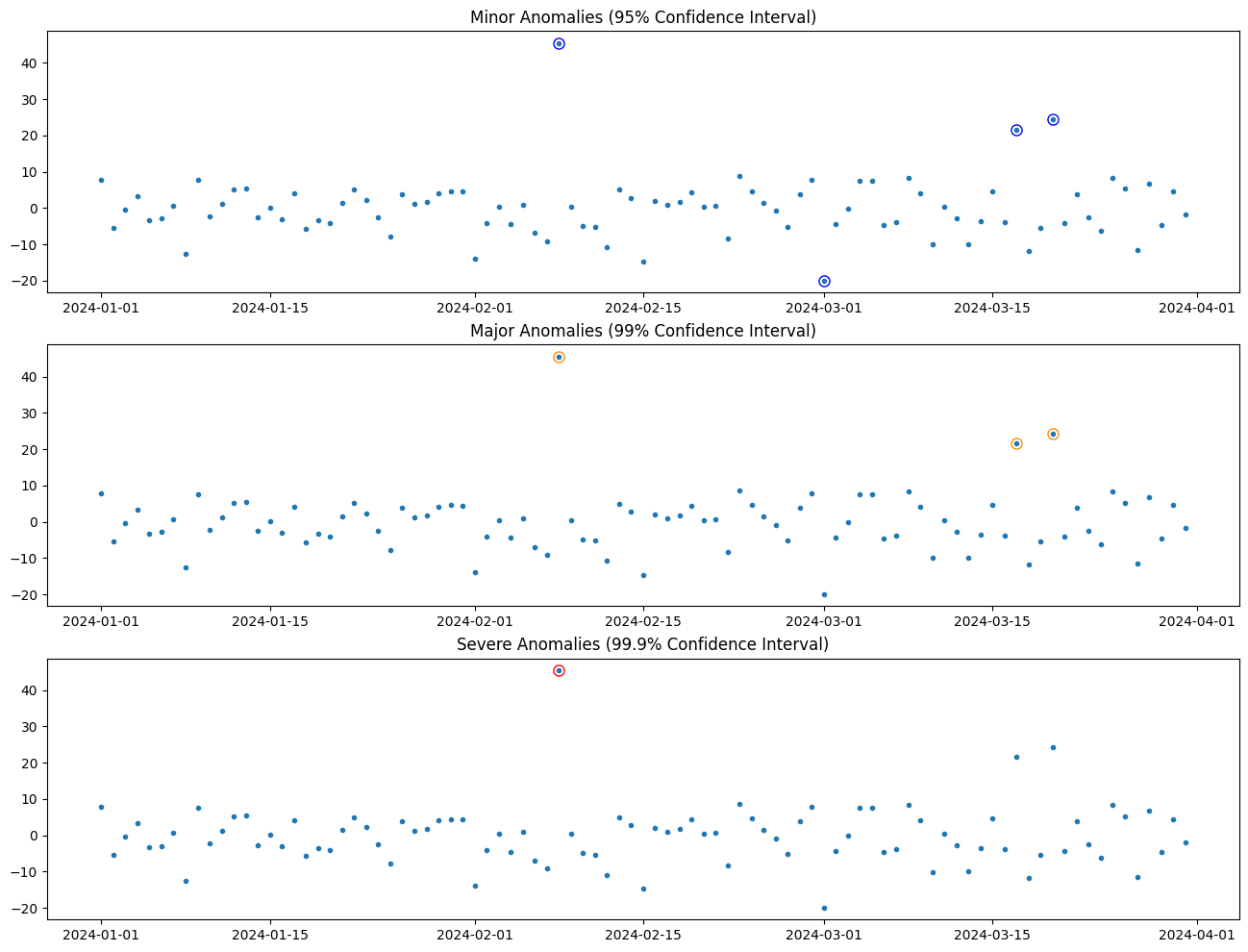
**Record the guess you made for the cost of a slightly larger house with a size of SID\*0.75. Don't worry if your guess is incorrect.**

****

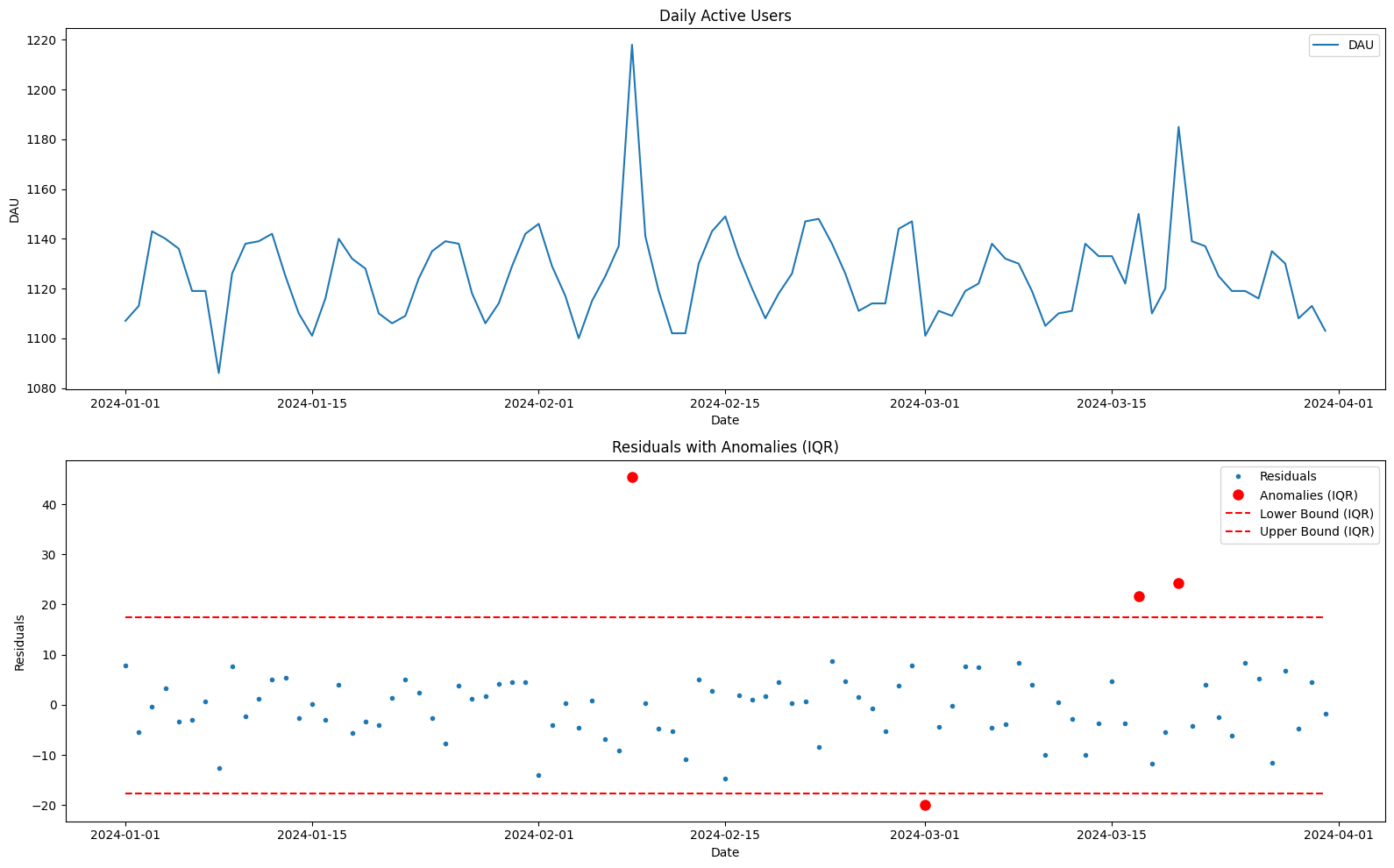
Lab 3

**Plot of anomalies using Z-score and IQR methods.**

**Z-Score:**

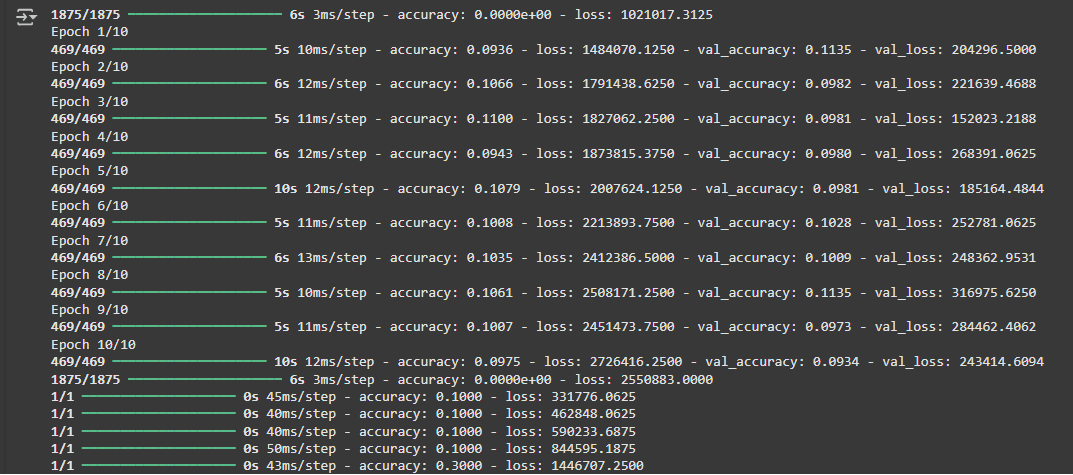
****

**IQR:**

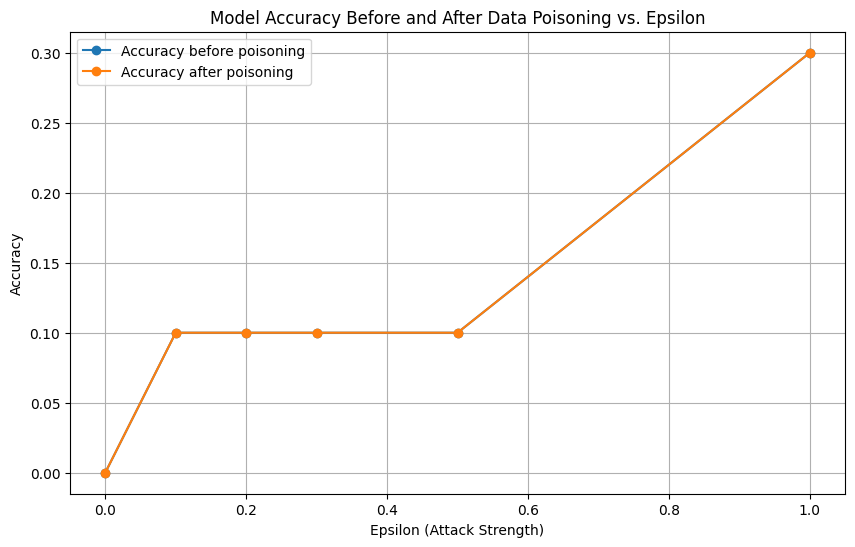
****

Lab 4

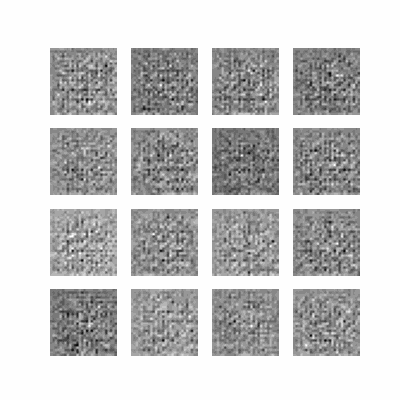
**Plot a graph showing the model's accuracy for each epsilon value. The model accuracy before and after data poisoning.**

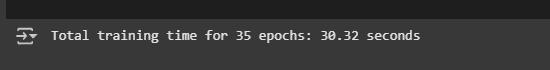


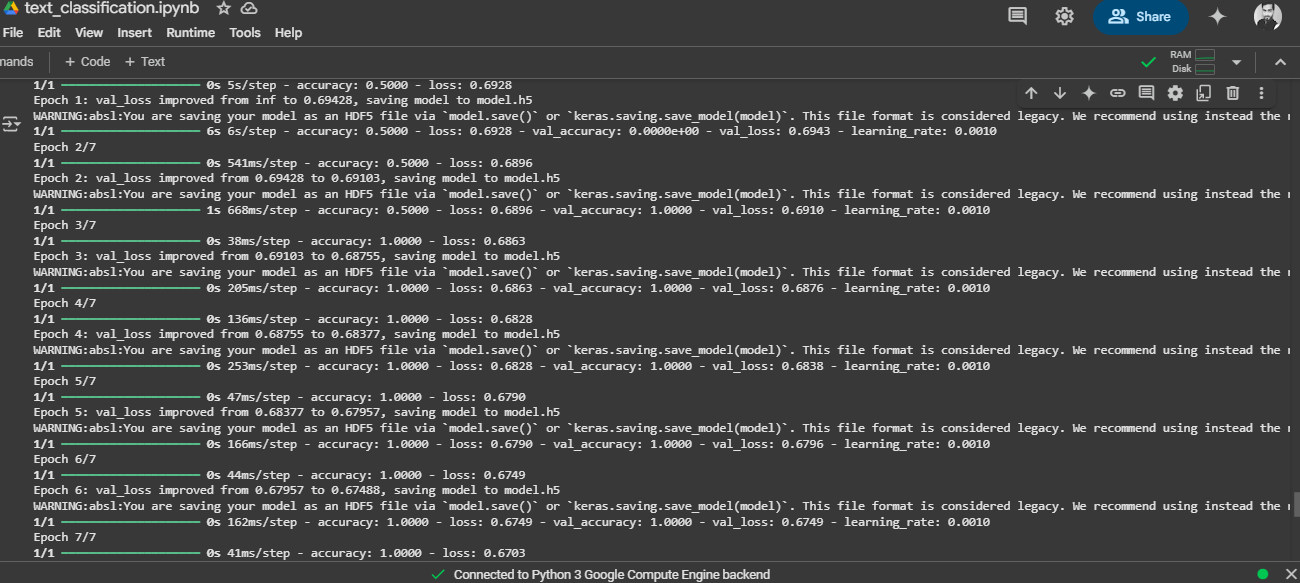
**Model accuracy Plot:**



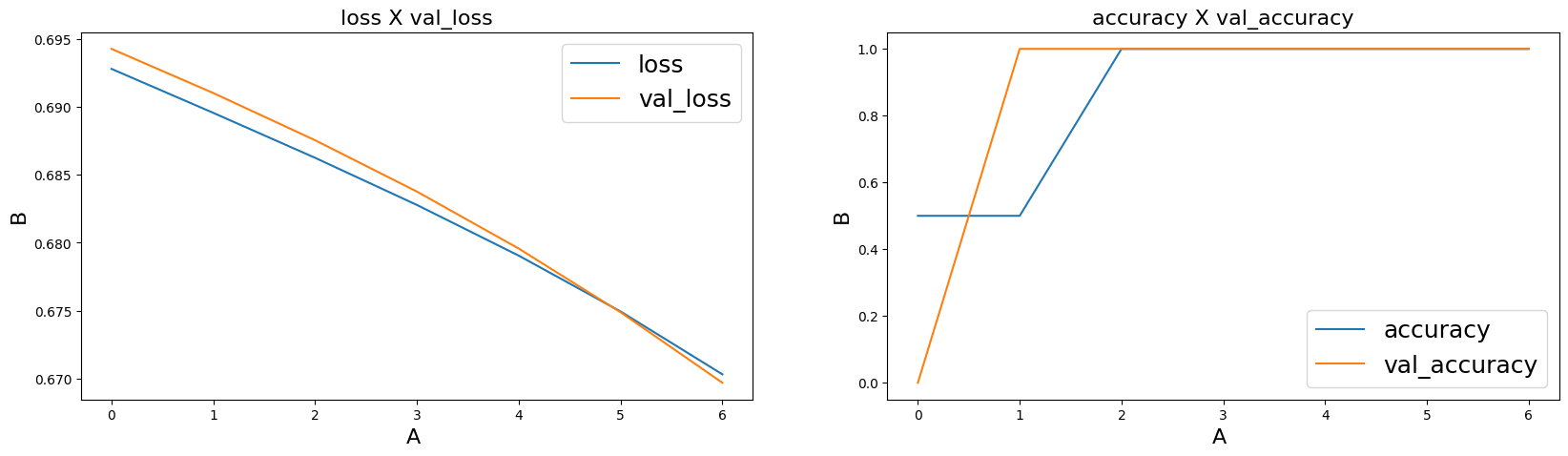
Lab 5

SID is 2372735. SO, EPOCHS = 35

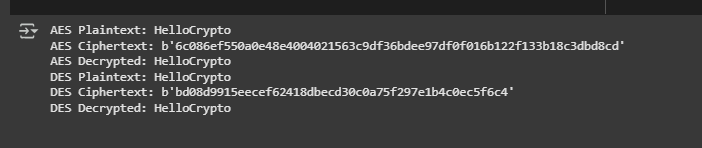


Lab 6

Provide a graph showing the history of training and validation loss based on your code. You should enhance the style of the plot to make it more visually appealing and presentable.

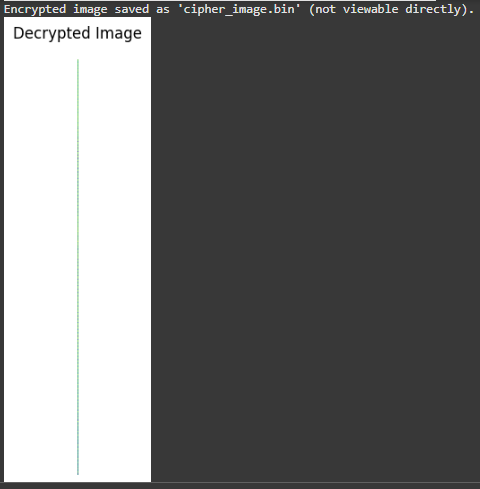


Lab 7

1. Sample of plain and cypher text for AES and DES

2. Real image and cipher image for the image of any choice using AES.





3. Explain in one word - 'YES' or 'NO' whether your encryption method for the images is good.

Yes

Lab 8

1. Your partner's name

Wahid Hussain

1. Values: p, g, s, and your private key (Do not write your partner’s private key)

p = 23 , g = 5, s = 2 , private key(a) = 6, public key (A) = 8

Lab 9

Record the following in your lab logbook:

1. **The attack type you have chosen.**

**Attack Type Chosen:** Log4j Vulnerability Exploit (2021)

A critical flaw in the Log4j logging library (CVE-2021-44228), also known as **Log4Shell**, allowed attackers to execute remote code on affected systems.

1. **Any one key website or research paper link that you found was useful.**

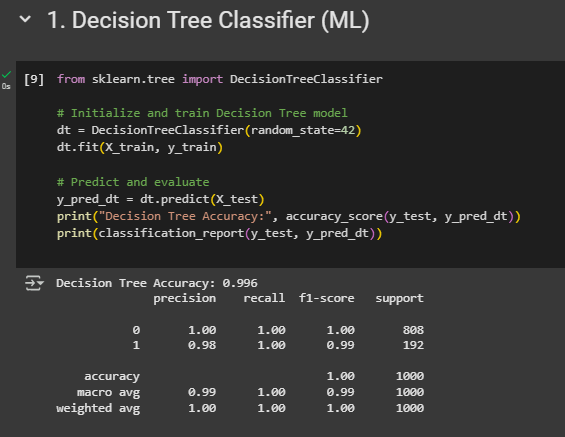
**Useful Resource:**

**Apache Log4j Vulnerability Guidance by CISA (U.S. Cybersecurity & Infrastructure Security Agency):**  
<https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-356a>

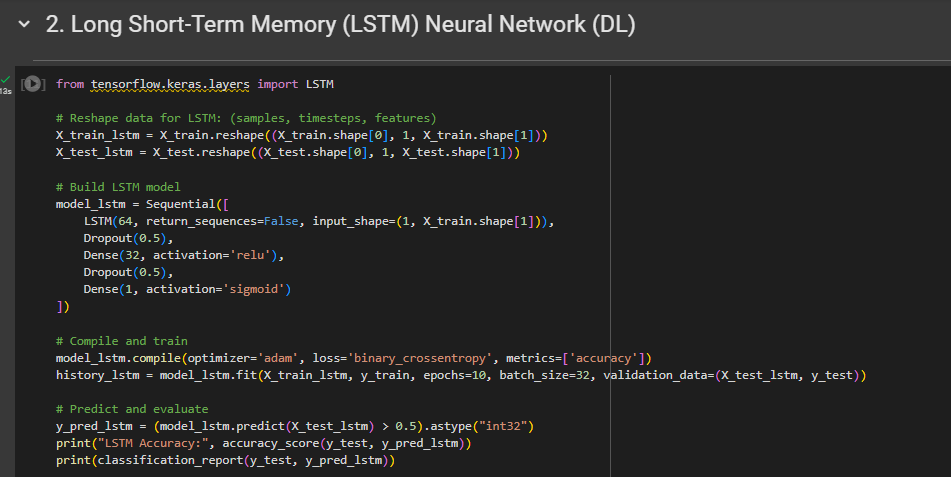
This site includes an official breakdown of the vulnerability, how it was exploited, and recommended mitigations.

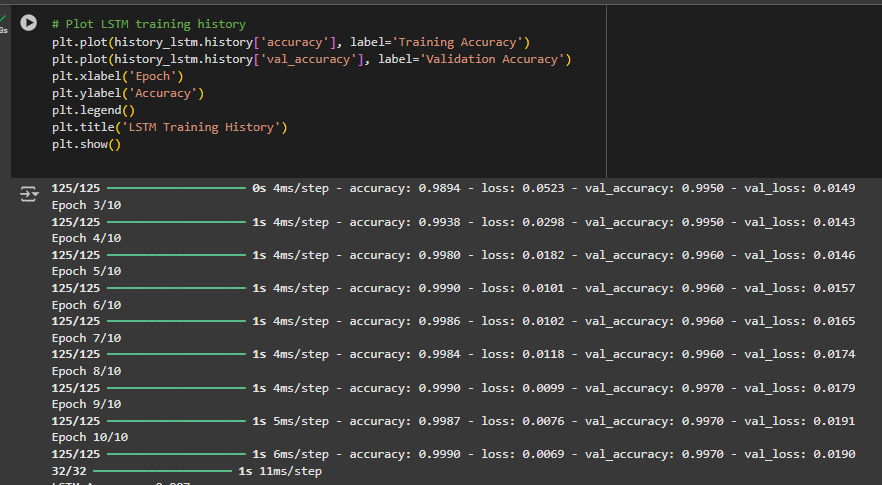
Lab 10

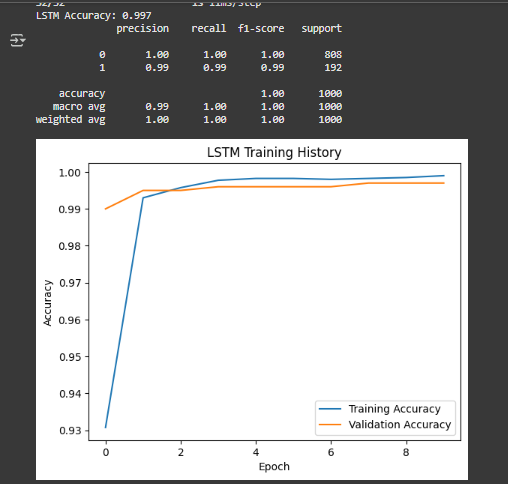
1. Decision Tree Classifier (ML)

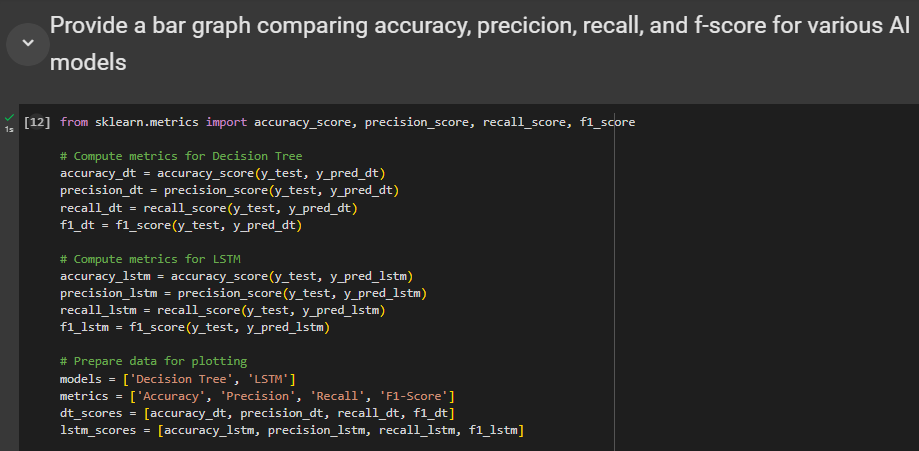


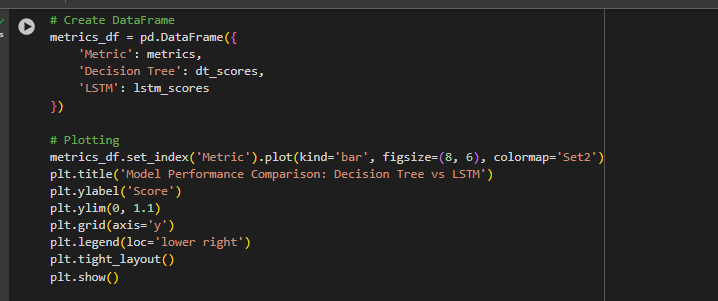
1. Long Short-Term Memory (LSTM) Neural Network (DL)

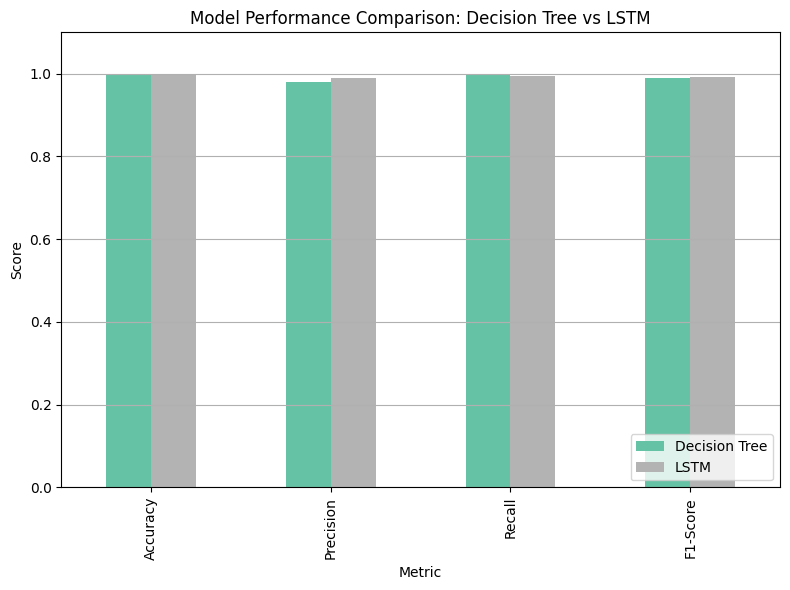




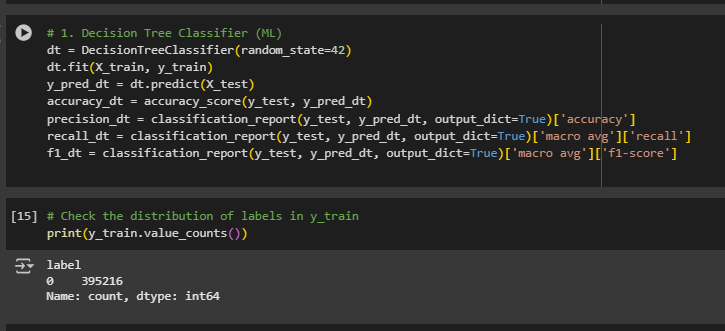
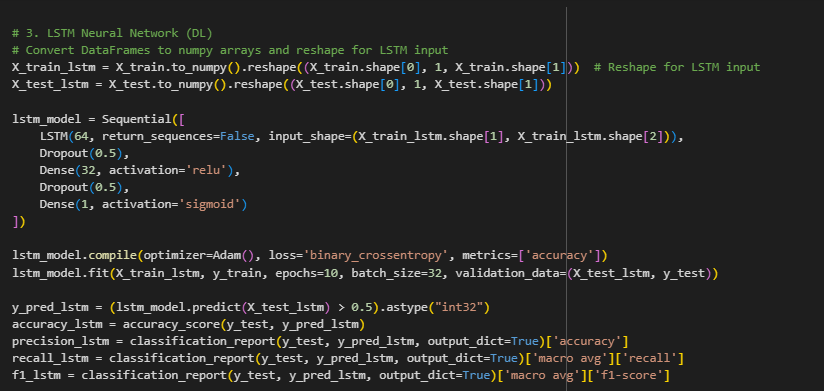


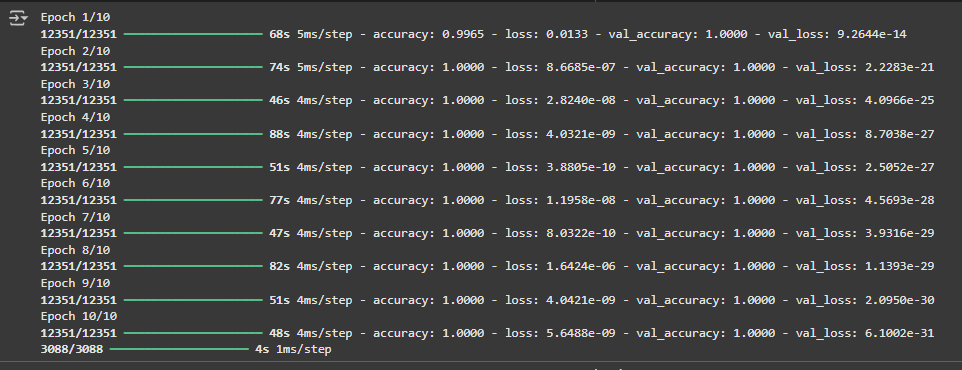
1. Provide a bar graph comparing accuracy, precision, recall, and f-score for various AI models

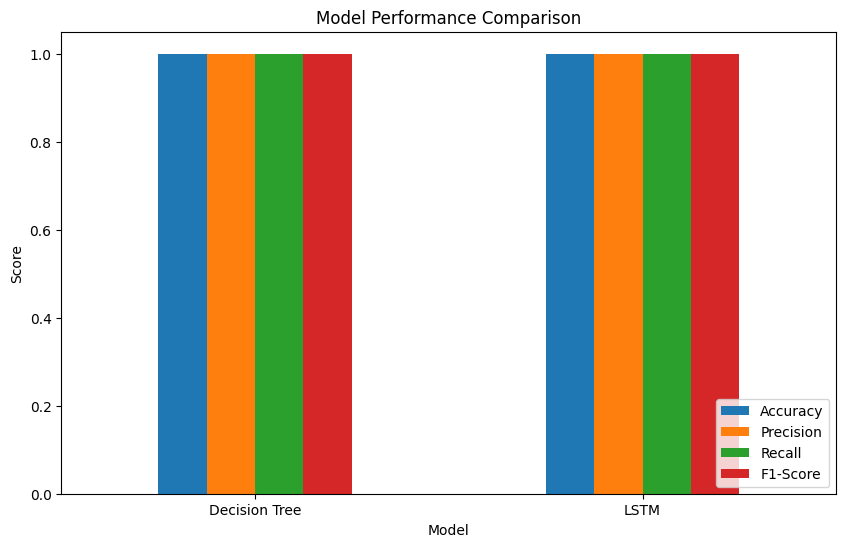




Lab 11

ML and LSTM:



Provide a graph comparing the performance of the AI model that you have developed.

Lab 12