Lab Logbook

Link to GitHub Folder:
https://github.com/Romanamarvi/Cyber_Security_AI_Case_Studies.git

SID: 2360926

Week # 1

Introduction to Cyber Security and AI Case Studies

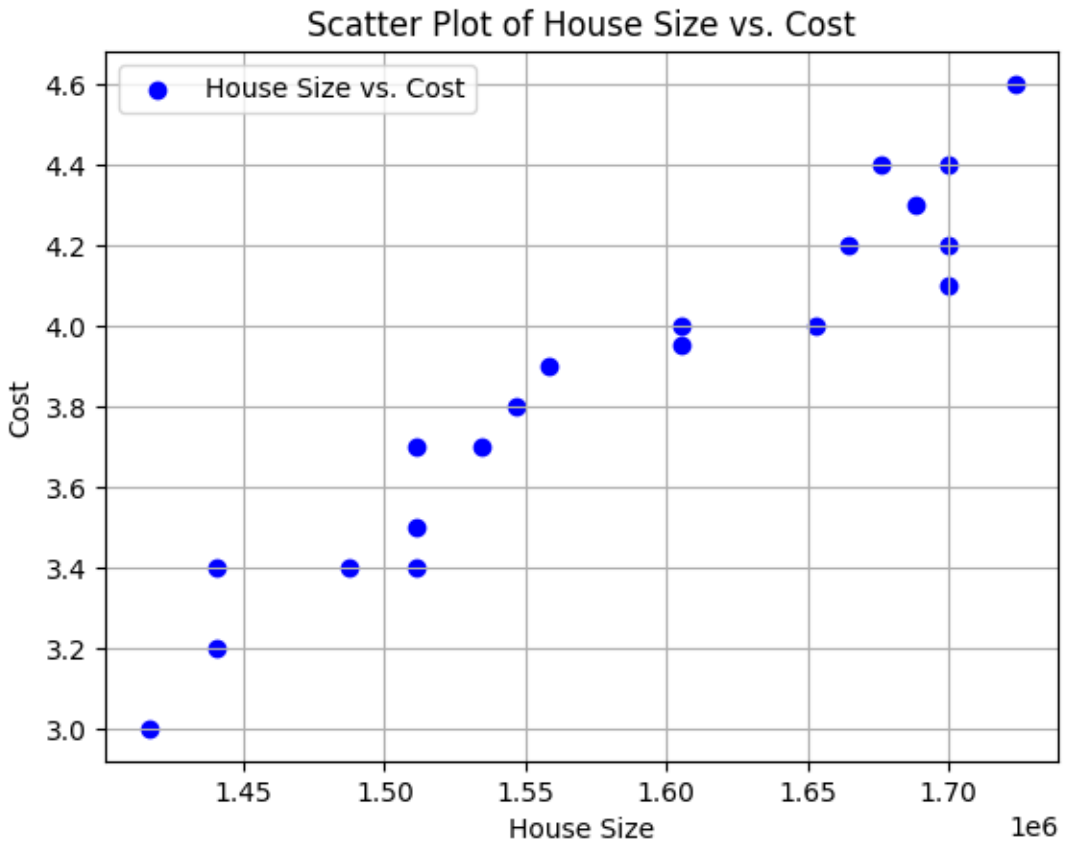
This week, I dove into some core concepts of Pandas and came across a few classes that really stood out to me:

1. **DataFrame** – Think of this as an advanced table that neatly arranges data into rows and columns, making it super handy for analyzing and managing structured data.
2. **Series** – A Series is like a simplified version of a column from a spreadsheet. Each item has a label, which makes it easy to work with single columns of data.
3. **Index** – The Index class is like a built-in organizer that helps label and access specific rows or columns quickly and efficiently.
4. **DatetimeIndex** – When working with dates and times, things can get complicated. This class makes it much easier to manage time-related data smoothly.
5. **Categorical** – Instead of storing the same text over and over, this class groups similar values, which saves memory and speeds up processing.

Week2

Anomaly Detection and Regression

Scatter plot between house size and cost

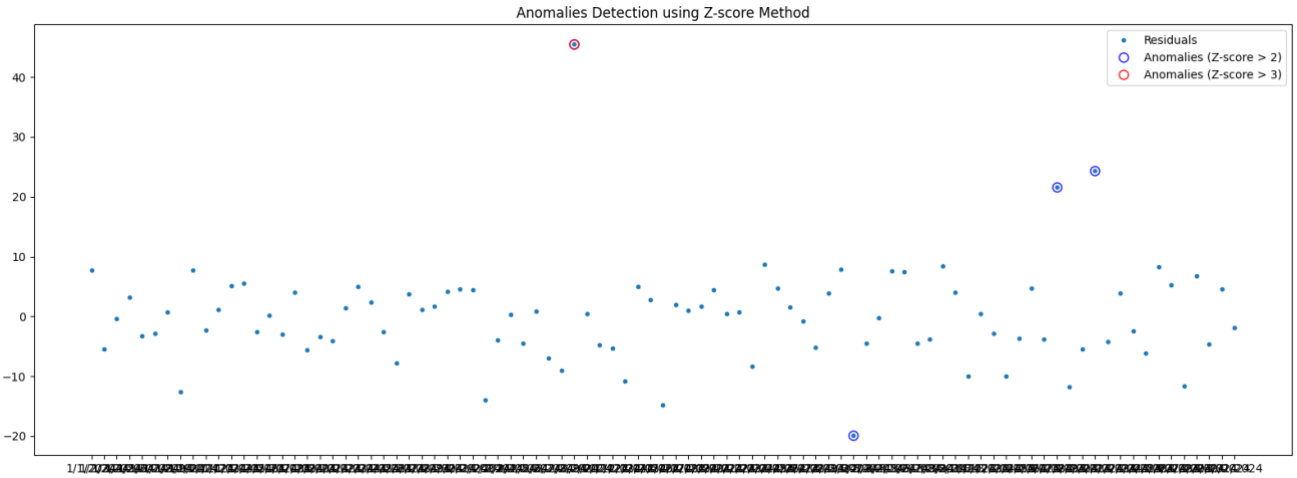


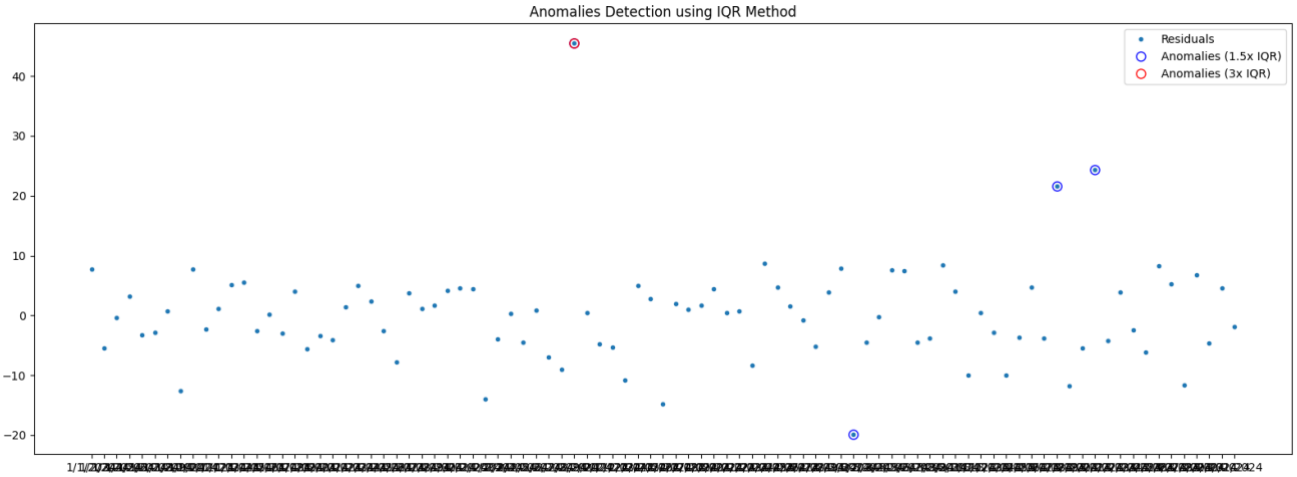
Predicted size for a larger house: 1292606.9849999999

Week3

Neural Networks and AI-Specific attacks

Plot of anomalies using Z-score and IQR methods

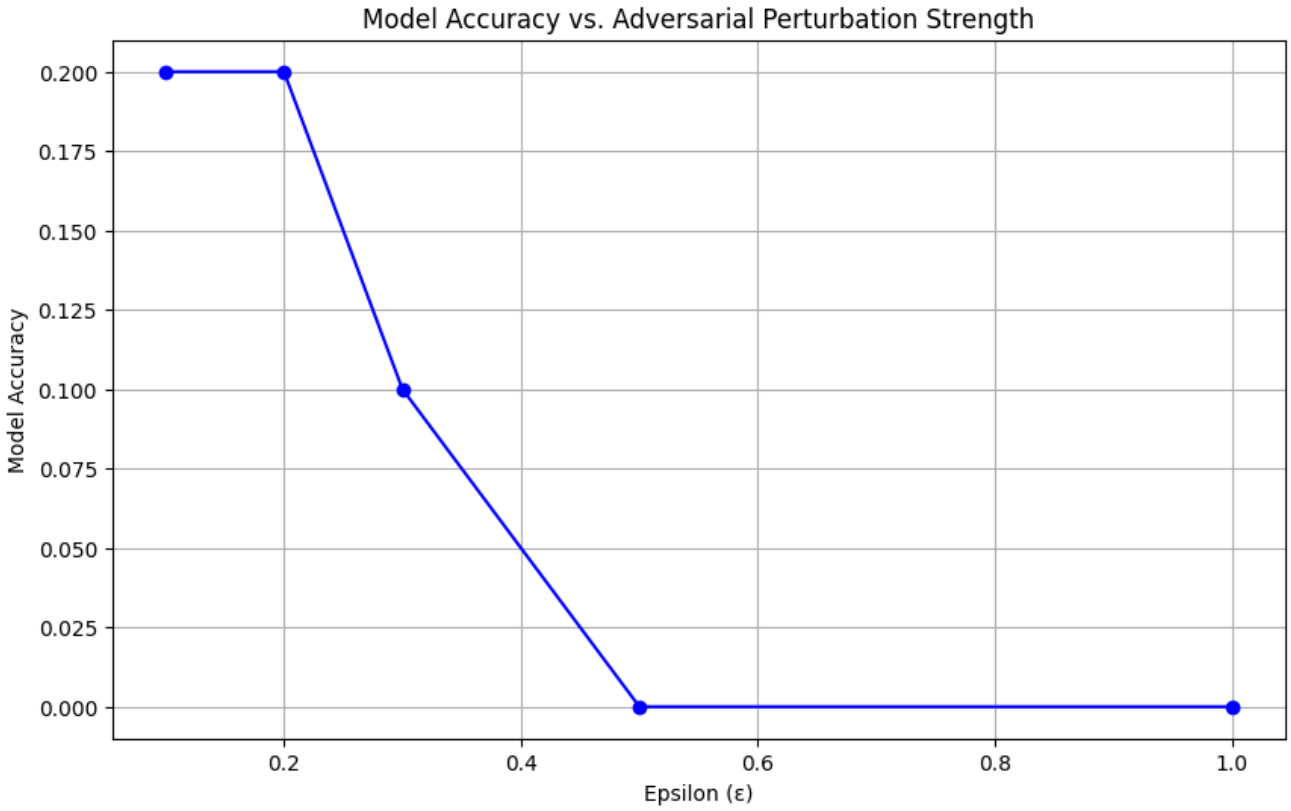




Week4

Deep Fake Images

Plot a graph showing the model's accuracy for each epsilon value.



The model accuracy before and after data poisoning.

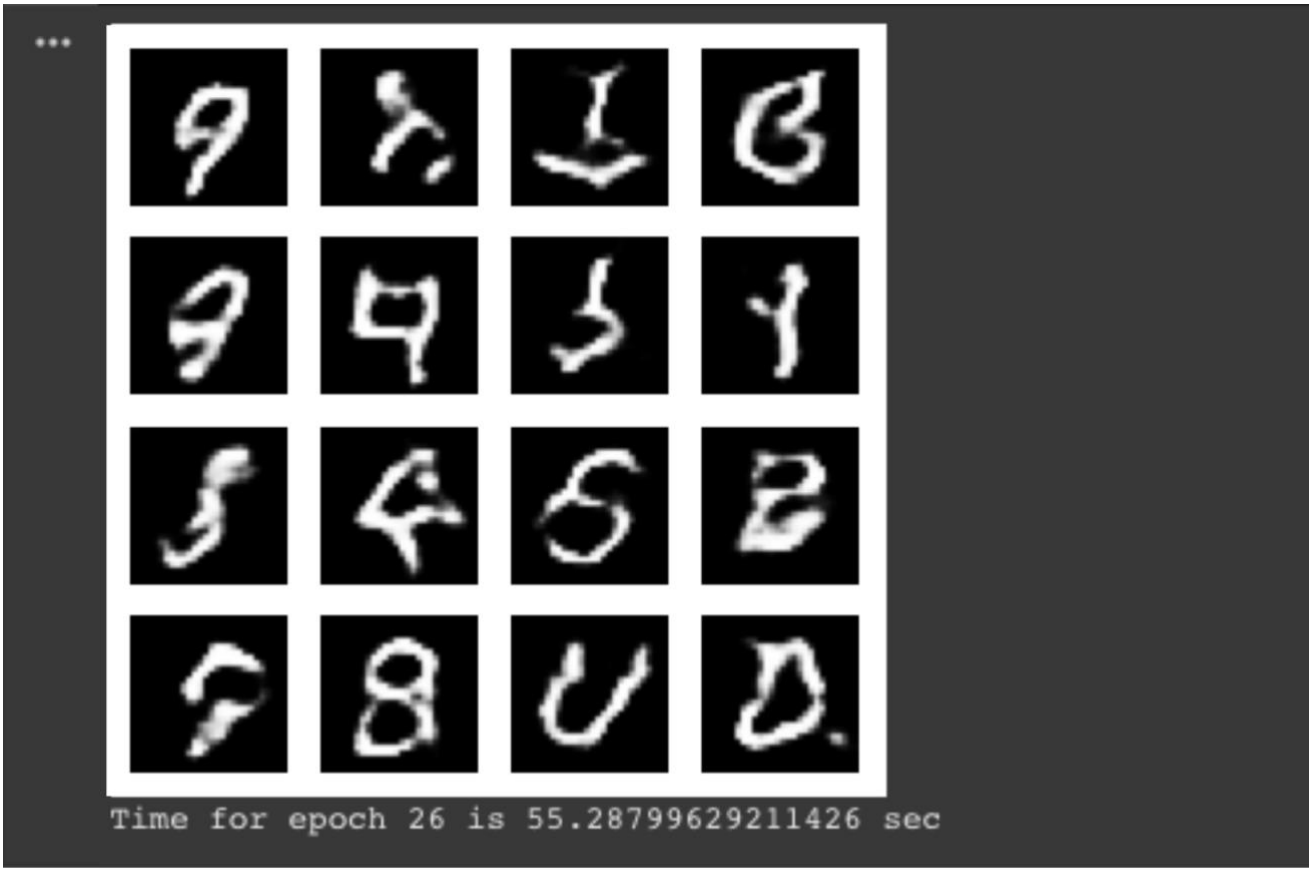
```
Training original model...
313/313 ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 1s 2ms/step - accuracy: 0.9797 - loss: 0.0980
Original model accuracy: 0.9821

Training poisoned model...
313/313 ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 1s 2ms/step - accuracy: 0.0022 - loss: 23.6577
Poisoned model accuracy: 0.0018
```

Week5

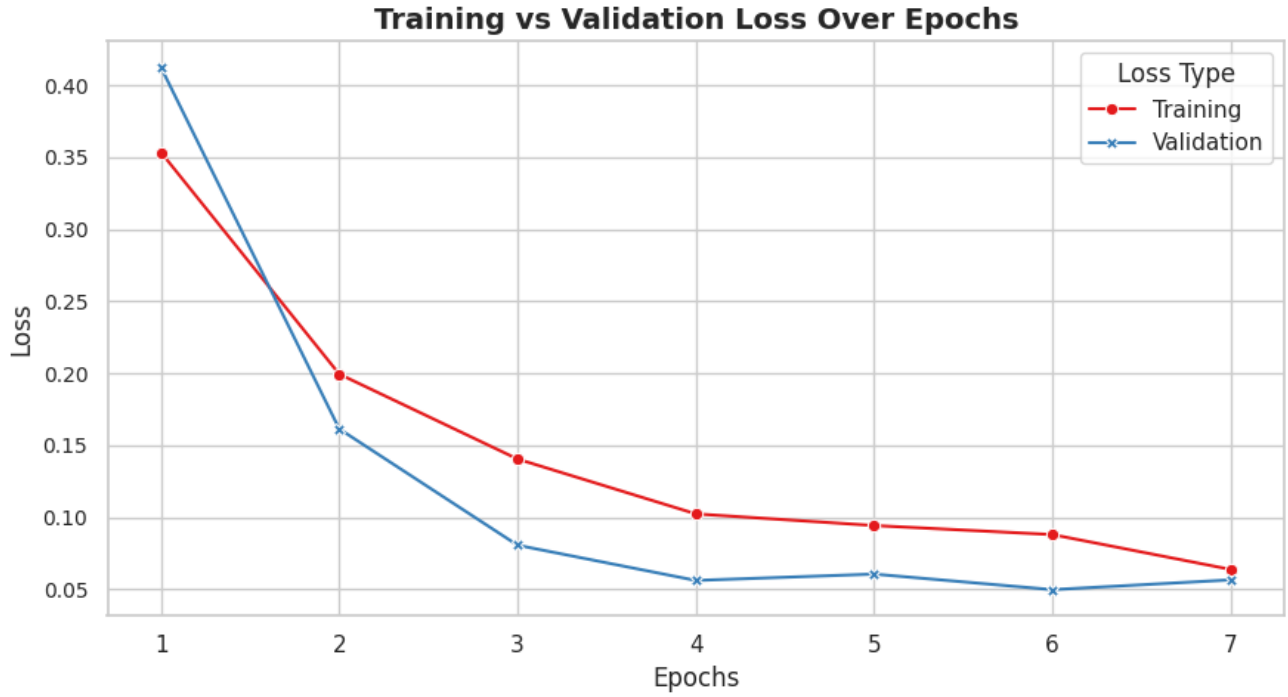
Text-based Cyber attacks

My SID **2360926**. So, 26 is used as epoch.



Week6

Cryptography



Week#7

Cryptography II

1. **A. Sample of plain and cypher text for DES**

```
print("\n--- DES Encryption ---")
des_key = b'SecretKe'  # 8 bytes
des_plain = input("Enter plaintext for DES: ")
des_cipher = des_encrypt(des_plain, des_key)
print("Encrypted (DES):", des_cipher)
print("Decrypted (DES):", des_decrypt(des_cipher, des_key))
```

```
--- DES Encryption ---
Enter plaintext for DES: Romana Marvi Rashid
Encrypted (DES): b'%=\xb1S\xa8\xc0F\xf6\xd43\xfa\x93\xe9\n\x01\xc3\x11\x84j#\x91\x88\x8d}'
Decrypted (DES): Romana Marvi Rashid
```

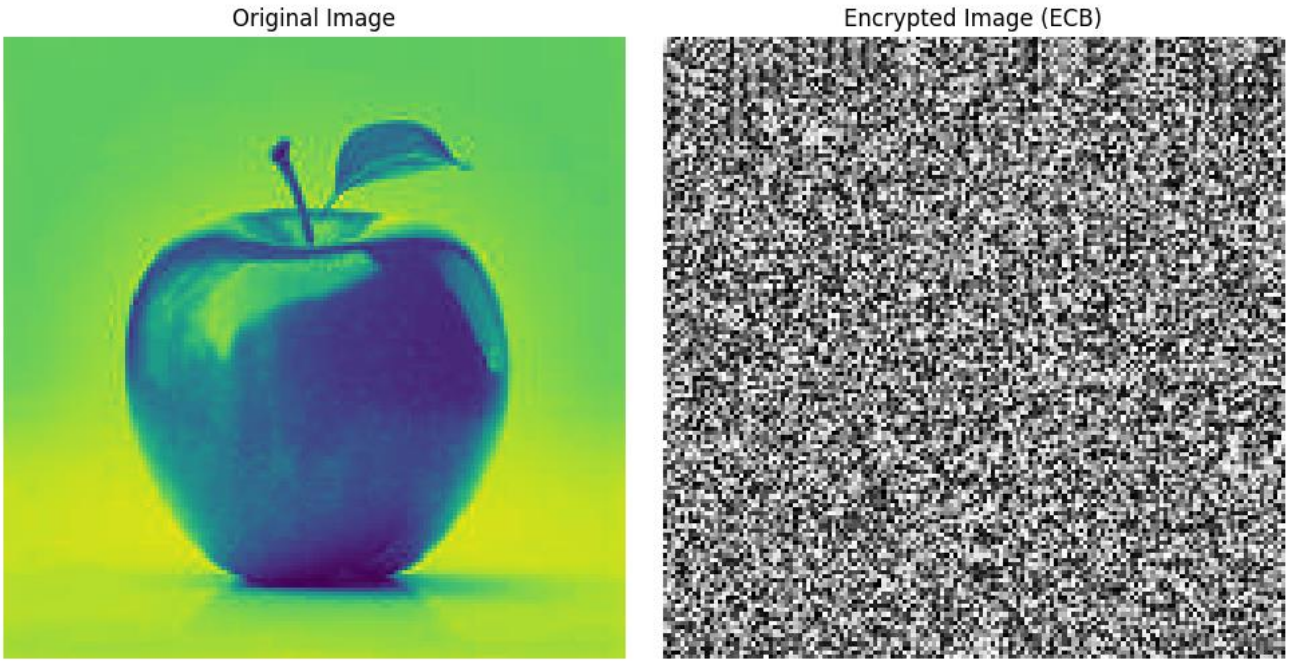
1. **B. Sample of plain and cypher text for AES**

```
# AES
print("\n--- AES Encryption ---")
aes_key = b'123456789012345678901234'  # 24 bytes for Task 4
aes_plain = input("Enter plaintext for AES: ")
aes_cipher = aes_encrypt(aes_plain, aes_key)
print("Encrypted (AES):", aes_cipher)
print("Decrypted (AES):", aes_decrypt(aes_cipher, aes_key))
```

```
--- AES Encryption ---
Enter plaintext for AES: Romana Marvi Rashid
Encrypted (AES): b"1\x11\xc3V\xac\x87\xd6\xb7\xc2\x98\xaa\xad'\xcc?\xaf(\x14K\x92k%R\xdf\x8a\x0b\xc7D\xbd\xcf\xfa\xde"
Decrypted (AES): Romana Marvi Rashid

--- AES Timing ---
AES Encryption Time: 0.0003 sec
```

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



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

Answer: No
Explanation: AES in ECB (Electronic Codebook) mode is not recommended for encrypting images because it doesn't hide patterns well. Identical parts of the image result in identical encrypted blocks, which can still reveal the original structure of the image.

Week#8

Hash Functions, Digital Signature, and Blockchain

Partner's Name: Umair

Values Used:

- p (Prime Number): 31
- g (Generator): 3
- My Private Key (a): 7

Computed Public Key (A):

$$A = g^a \bmod p = 3^7 \bmod 31 = 4$$

Shared Secret (s):

- s = 9

Week#9

Network-based attacks

Attack Type Chosen:

Colonial Pipeline Ransomware Attack (2021)

This attack involved a ransomware incident that disrupted the fuel supply chain on the East Coast of the United States, causing widespread fuel shortages and significant financial losses.

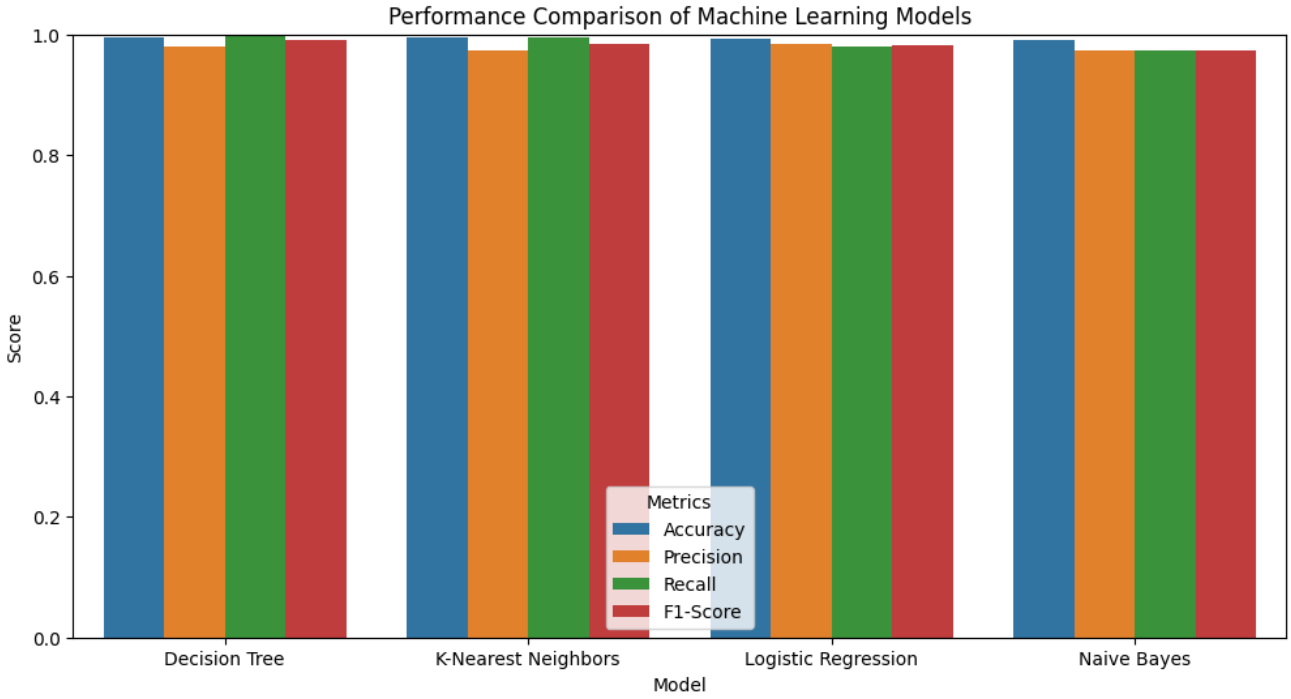
Key Research Source:

CISA Advisory on Colonial Pipeline Ransomware Attack (2021)

(Link: https://www.cisa.gov/news-events/cybersecurity-advisories)

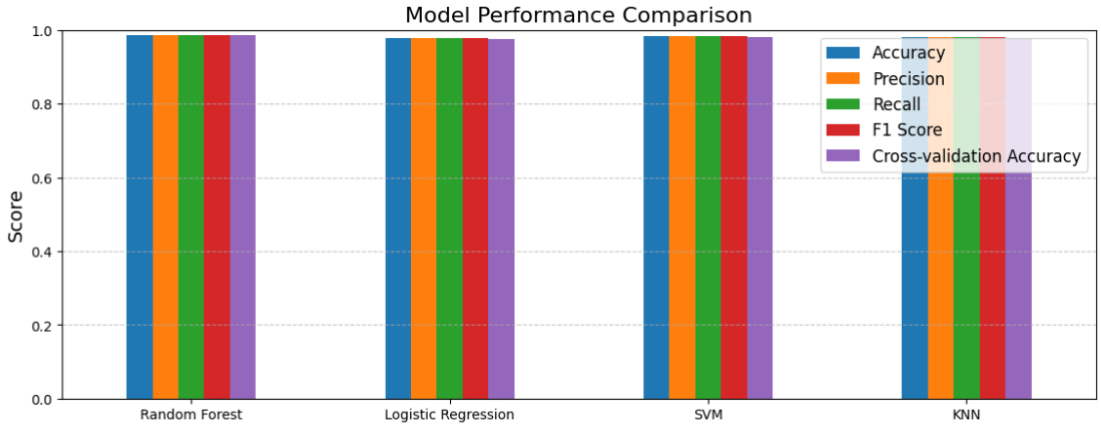
Week#10

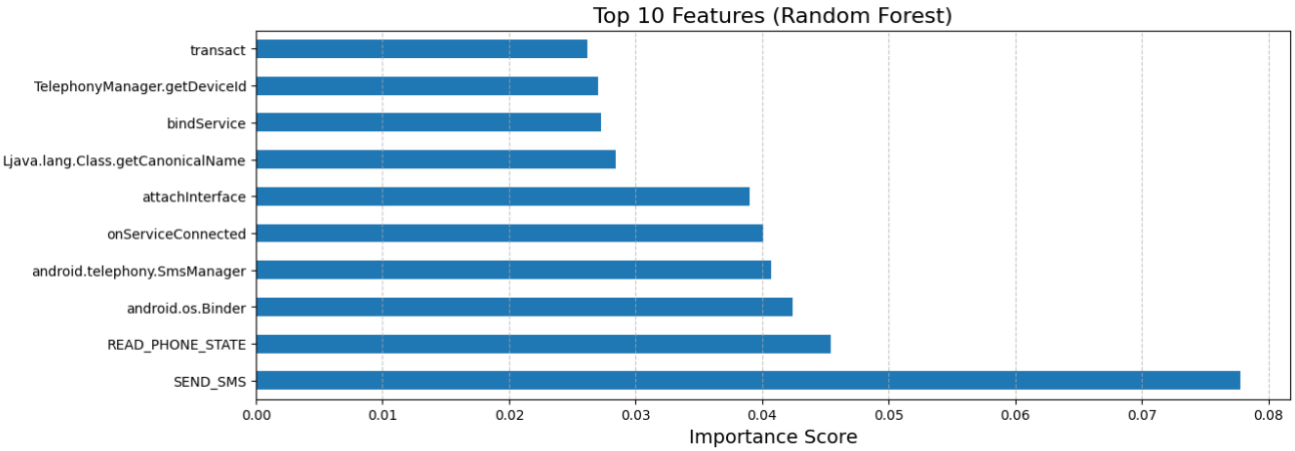
Network Intrusion Detection and Malwares



Week#11

Honeypots, DMZ, CTI sharing and Cyber security framework





```
Detailed Model Performance:
```

cell output actions

```
Random Forest:
  Accuracy: 0.9864
  Precision: 0.9864
  Recall: 0.9864
  F1 Score: 0.9863
  Cross-validation Accuracy: 0.9864

Logistic Regression:
  Accuracy: 0.9784
  Precision: 0.9784
  Recall: 0.9784
  F1 Score: 0.9784
  Cross-validation Accuracy: 0.9755

SVM:
  Accuracy: 0.9830
  Precision: 0.9831
  Recall: 0.9830
  F1 Score: 0.9830
  Cross-validation Accuracy: 0.9795

KNN:
  Accuracy: 0.9817
  Precision: 0.9817
  Recall: 0.9817
  F1 Score: 0.9817
  Cross-validation Accuracy: 0.9752

✅ Best Performing Model: Random Forest
```