Lab Logbook

## Link to GitHub Folder: https://github.com/Romanamarvi/Cyber\_Security\_AI\_Case\_Studies.git

**Week # 1**

**Introduction to Cyber Security and AI Case Studies**

SID: 2360926

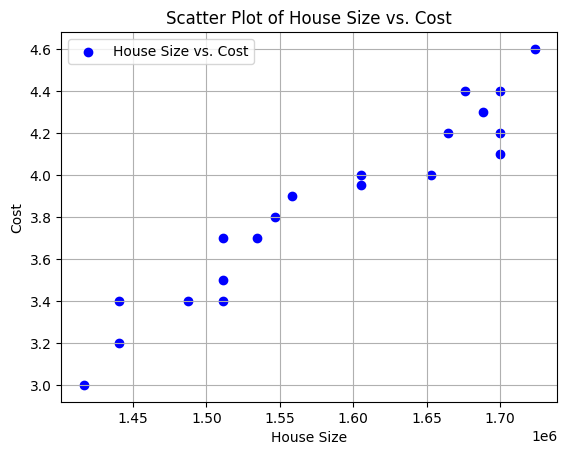
This week, I dove into some core concepts of Pandas and came across a few classes that really stood out to me:

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

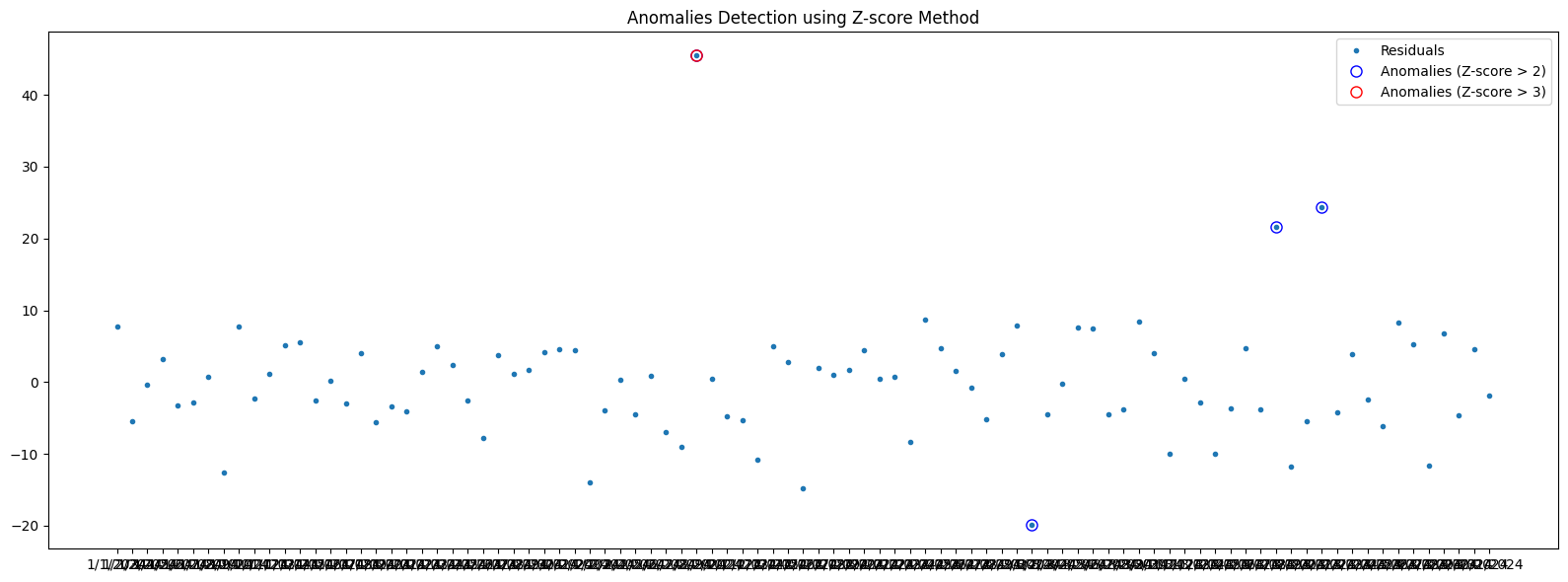


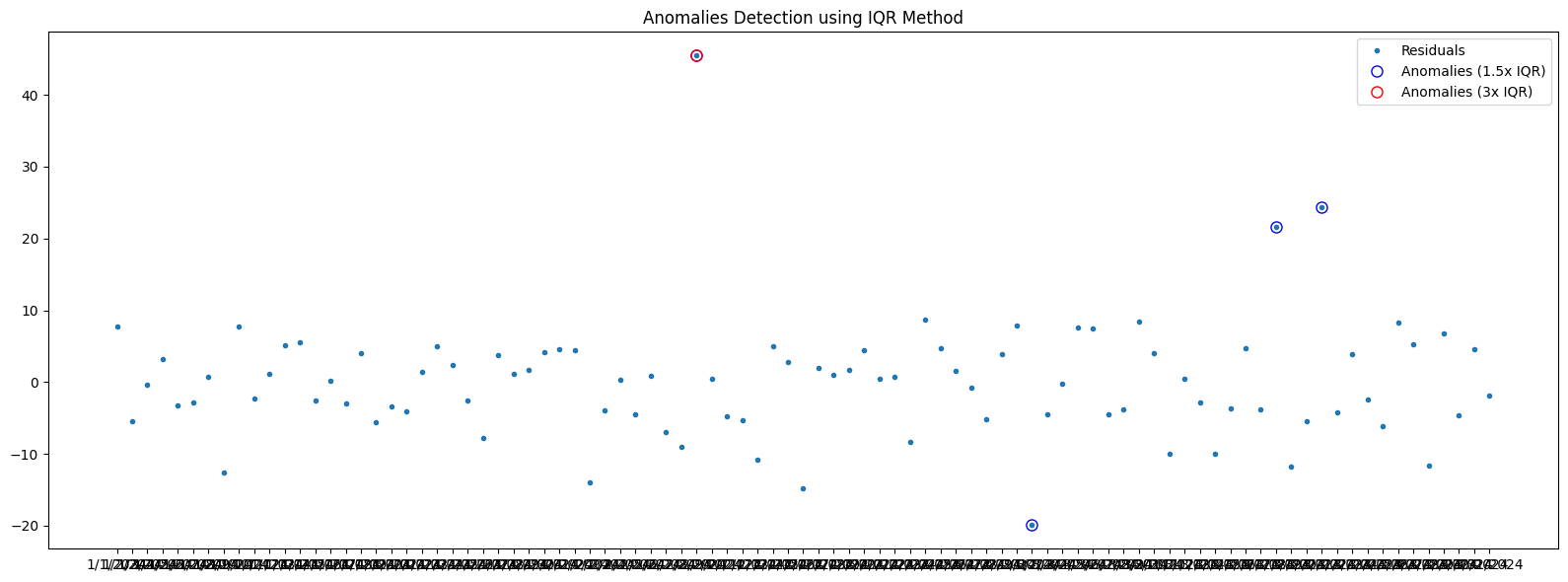
Predicted size for a larger house: 1292606.9849999999

**Week3**

**Neural Networks and AI-Specific attacks**

# Plot of anomalies using Z-score and IQR methods

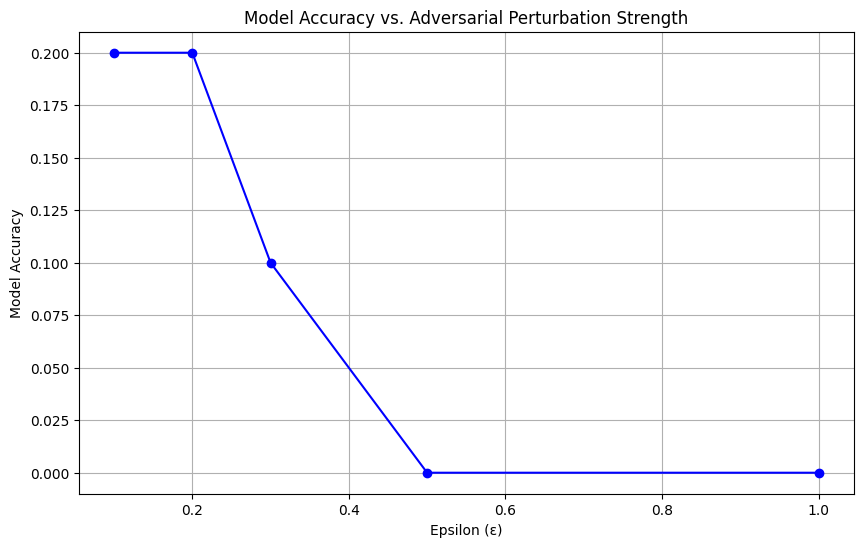




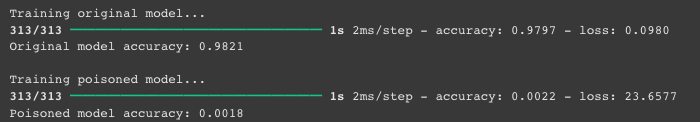
**Week4**

**Deep Fake Images**

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



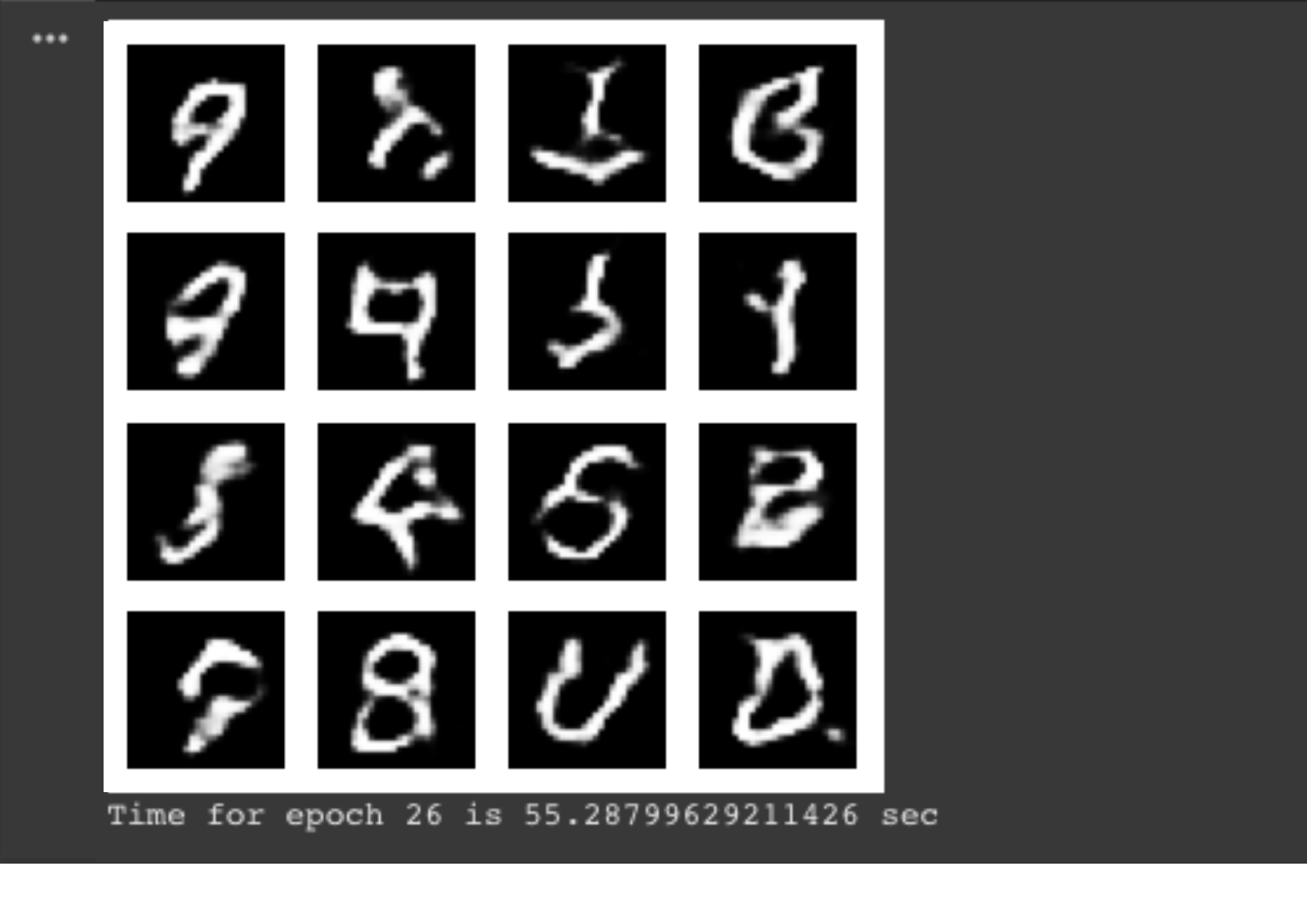
The model accuracy before and after data poisoning.



**Week5**

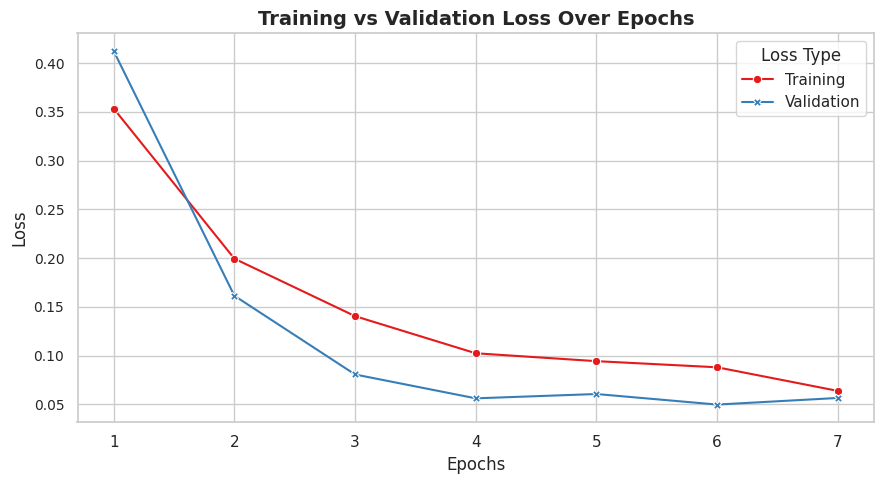
**Text-based Cyber attacks**

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



**Week6**

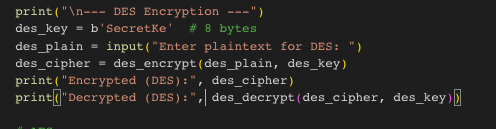
**Cryptography**

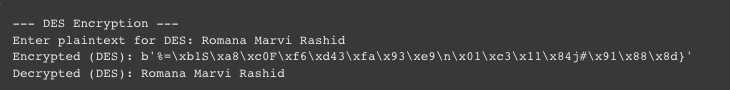
****

**Week#7**

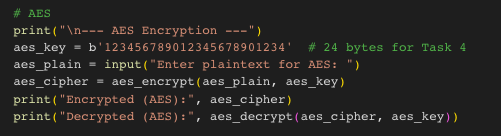
**Cryptography II**

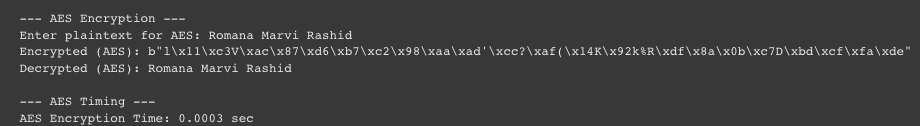
1. **A. Sample of plain and cypher text for DES**

****

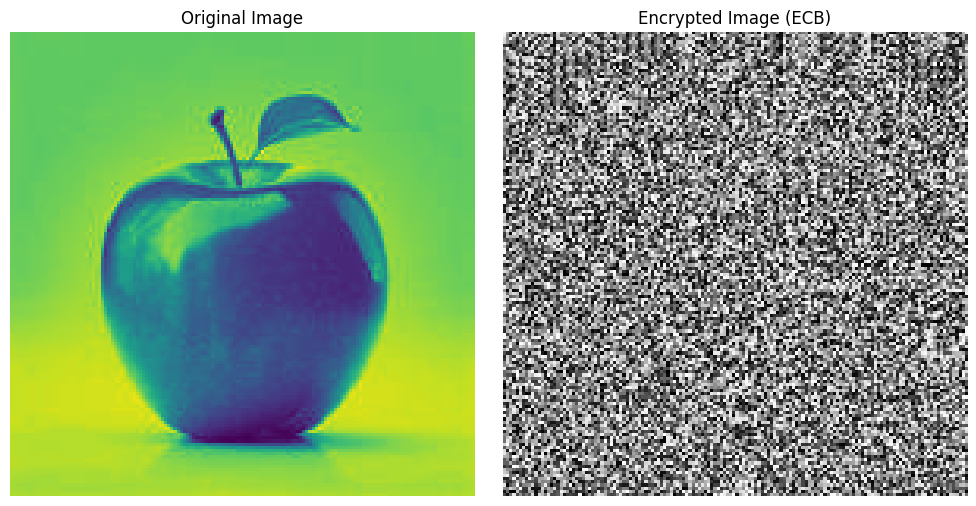
****

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

****

****

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



## 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:** Zanib Shafqat **Partner's Name:** Zanib Shafqat

#### **Values Used:**

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

#### **Computed Public Key (A):**

A = g^a mod p = 3^7 mod 31 = 4

#### **Shared Secret (s):**

* **s = 9**

**Week#9**

**Network-based attacks**

**Attack Type Chosen:**

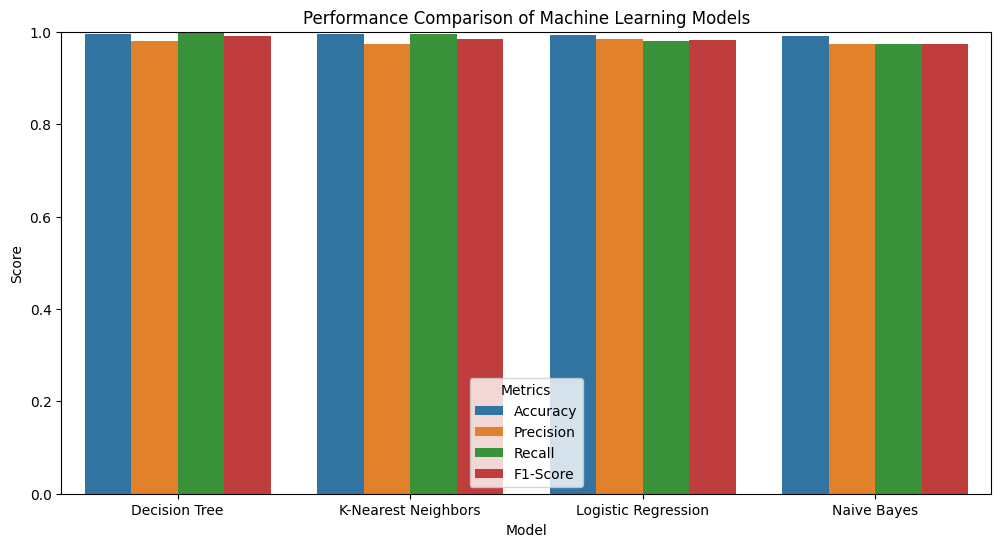
**Colonial Pipeline Ransomware Attack (2021)**  
This attack involved a ransomware incident that disrupted the fuel supply chain on the East Coast of the United States, causing widespread fuel shortages and significant financial losses.

**Key Research Source:**

**CISA Advisory on Colonial Pipeline Ransomware Attack (2021)**  
(Link: https://www.cisa.gov/news-events/cybersecurity-advisories)

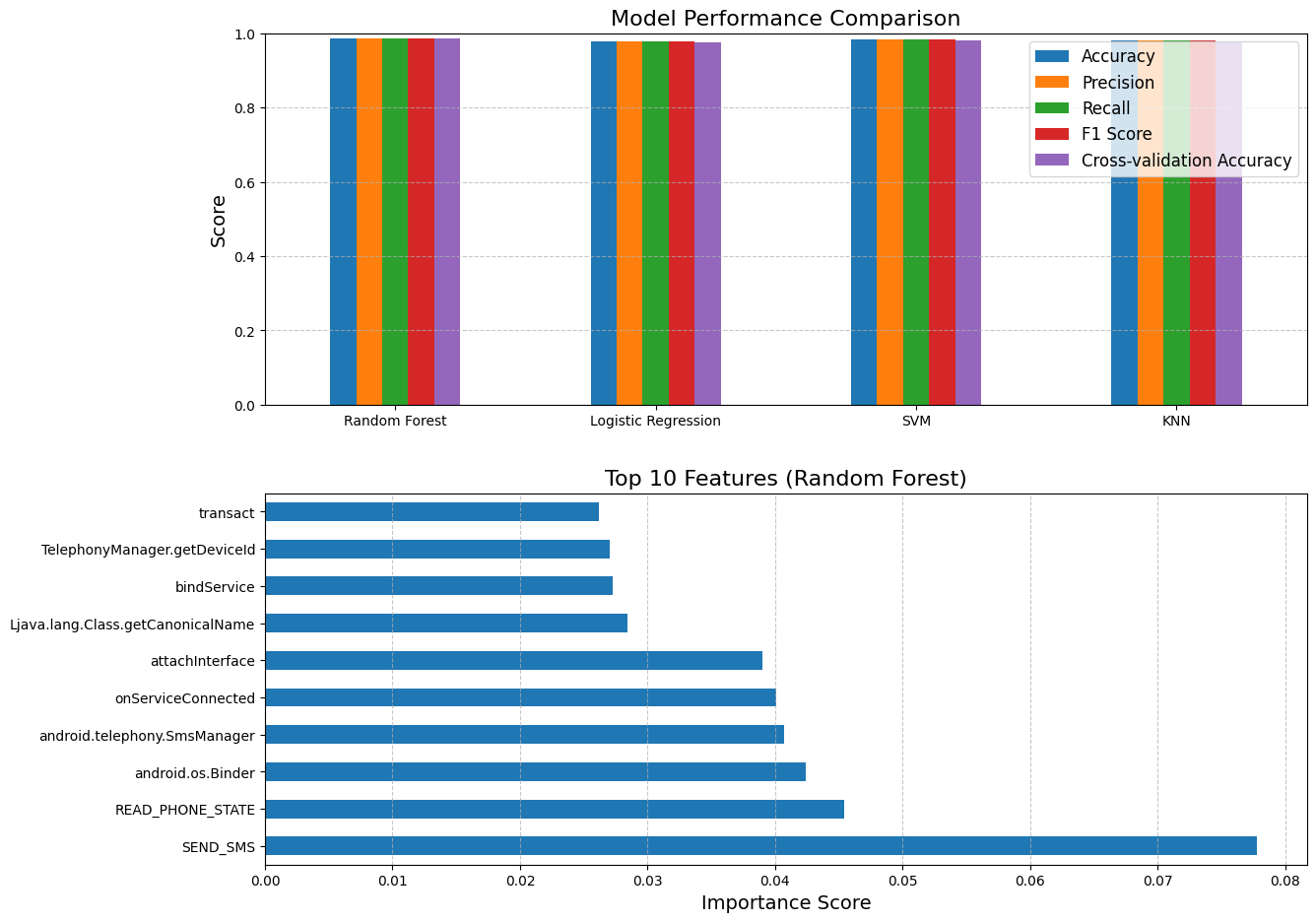
**Week#10**

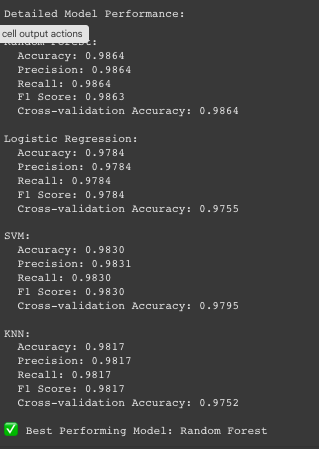
**Network Intrusion Detection and Malwares**

****

**Week#11**

**Honeypots, DMZ, CTI sharing and Cyber security framework**

****

****