# Lab Logbook

**Link to GitHub Folder:** https://github.com/taqisherazi/cybersecurity.git

SID: 2363665

**Week # 1**

## Introduction to Cyber Security and AI Case Studies

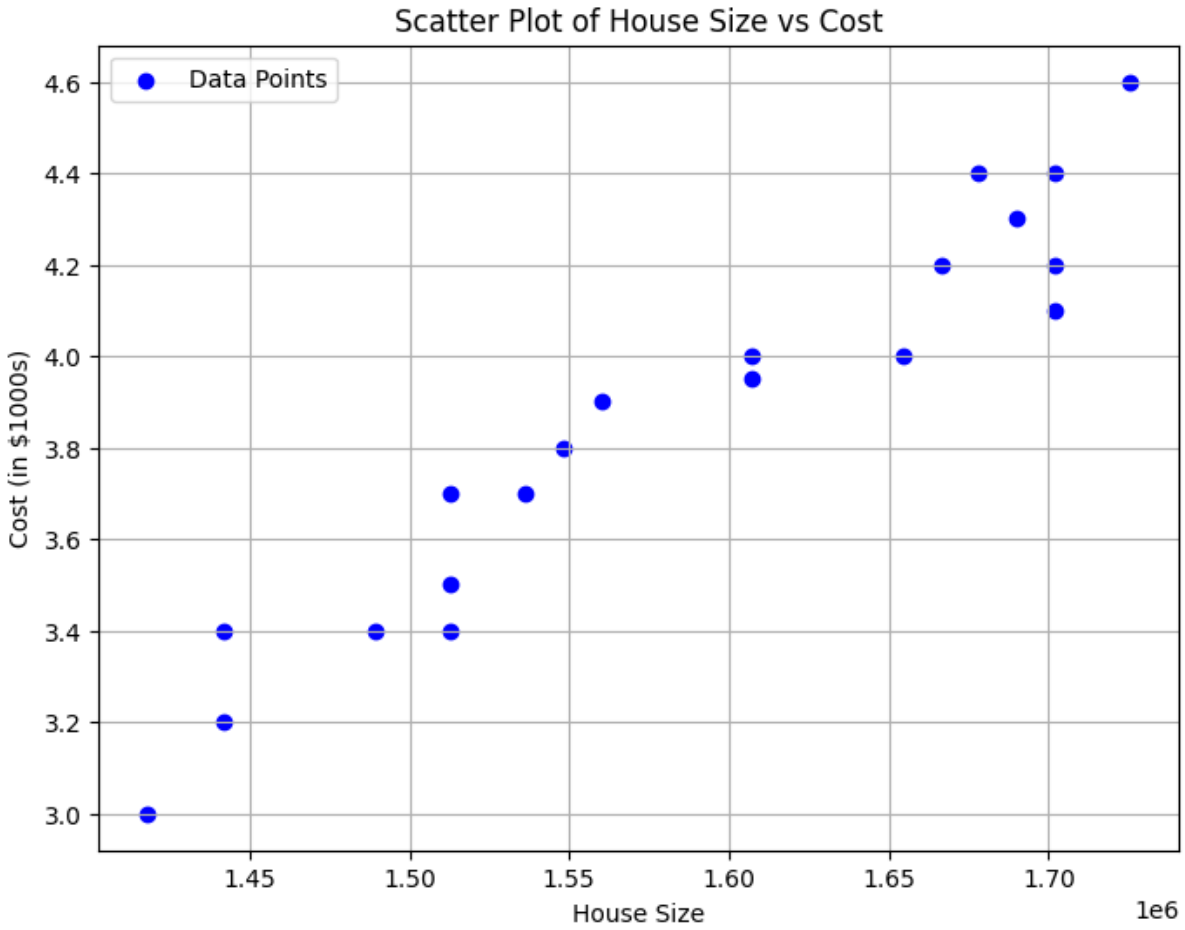
This week, I explored different Pandas classes and found five of them particularly interesting:

1. **DataFrame** – This is like a supercharged table that organizes data in rows and columns. It makes it easy to analyze and manipulate structured data.
2. **Series** – A Series feels like a single-column spreadsheet, where each value has a label, makes it simple to work with individual data columns.
3. **Index** – The Index class acts like a built-in organizer. it helps to label and quickly access data in both rows and columns.
4. **DatetimeIndex** – Working with time-based data can be tricky, but this class makes handling dates and times smooth and efficient.
5. **Categorical** – Instead of storing repetitive text data inefficiently, this class groups similar values together, saves memory and speeds up operations.

**Week # 2**

**Anomaly Detection and Regression**

# Scatter plot between house size and cost

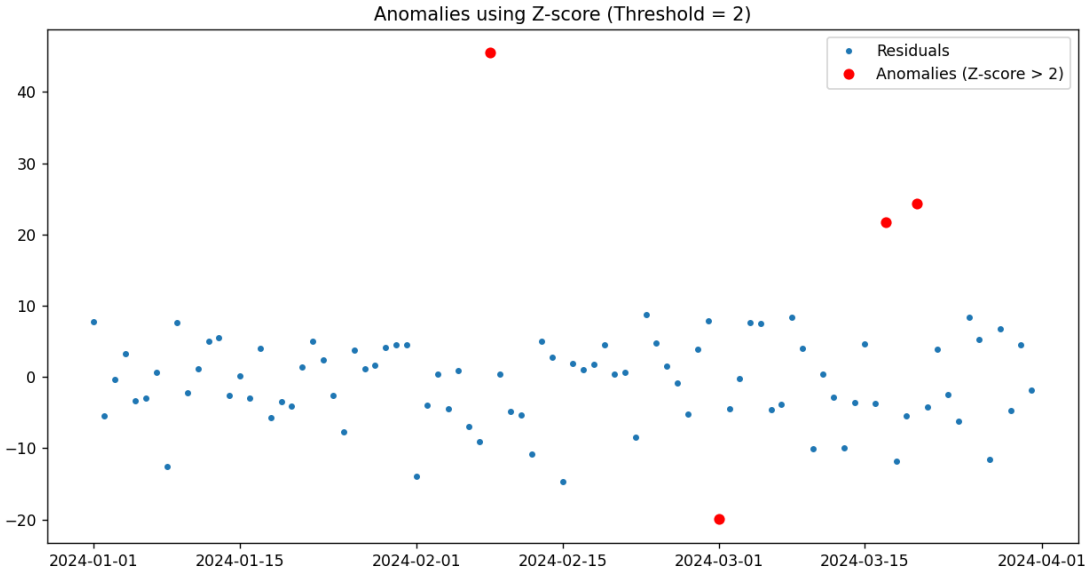


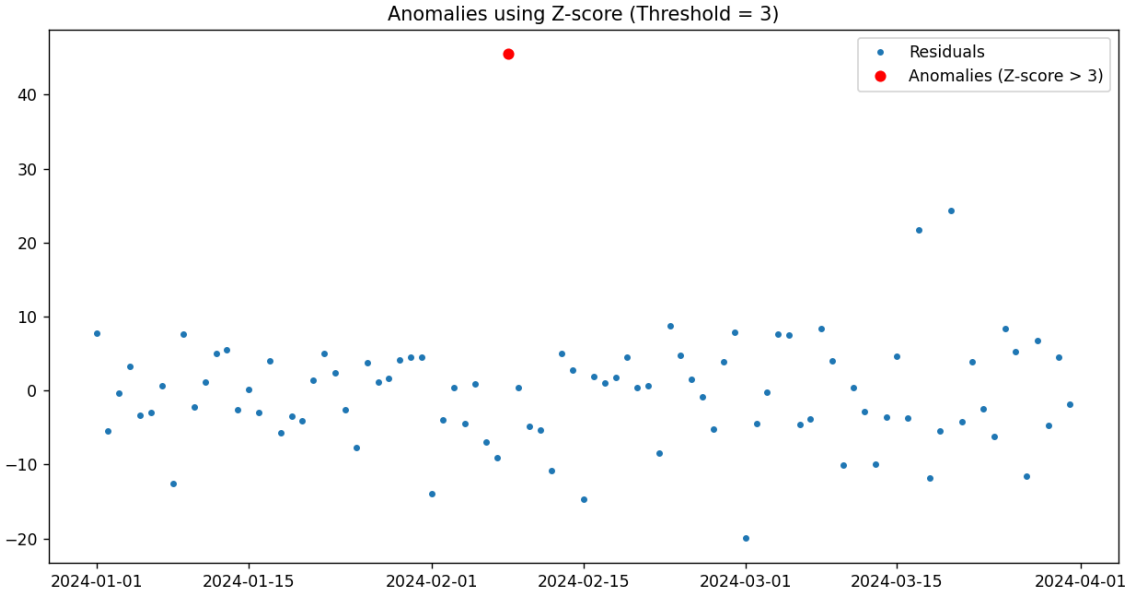

Estimated cost for house size 1772748.75: 4.6

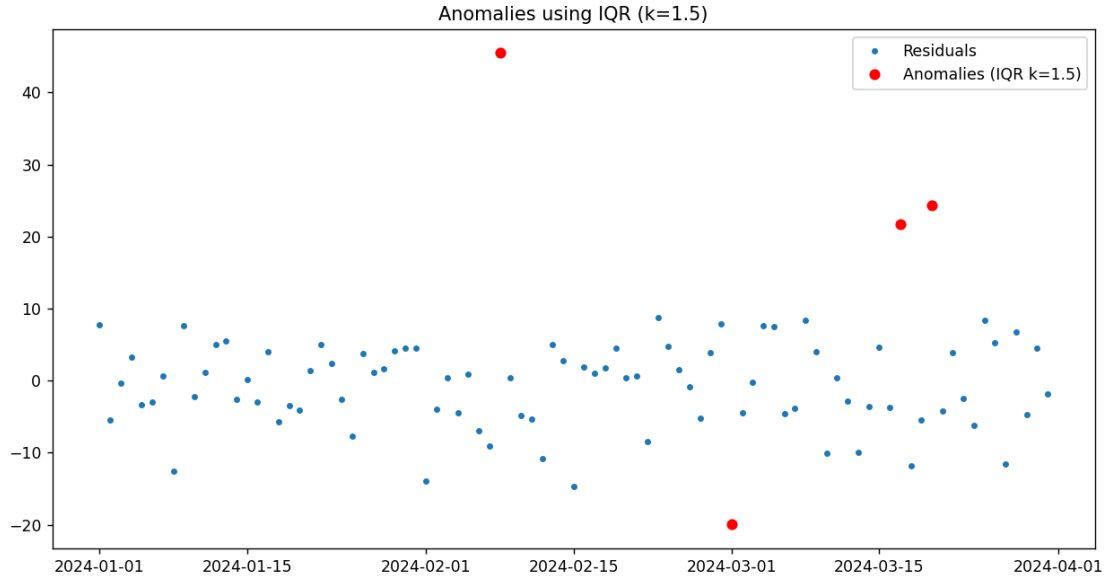
**Week # 3**

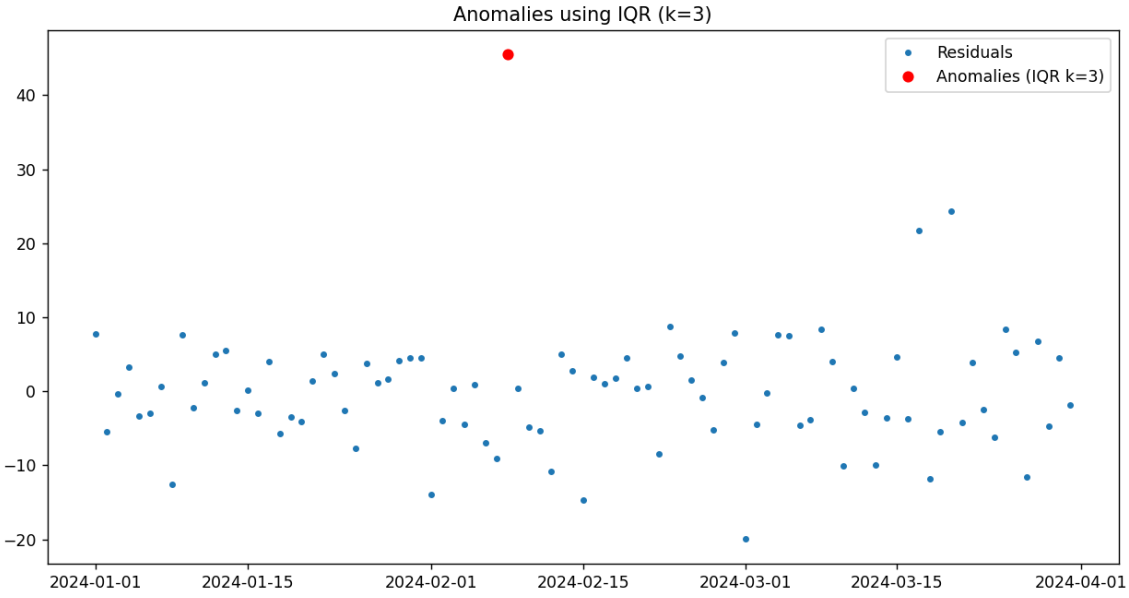
**Neural Networks and AI-Specific attacks**

# Plot of anomalies using Z-score and IQR methods



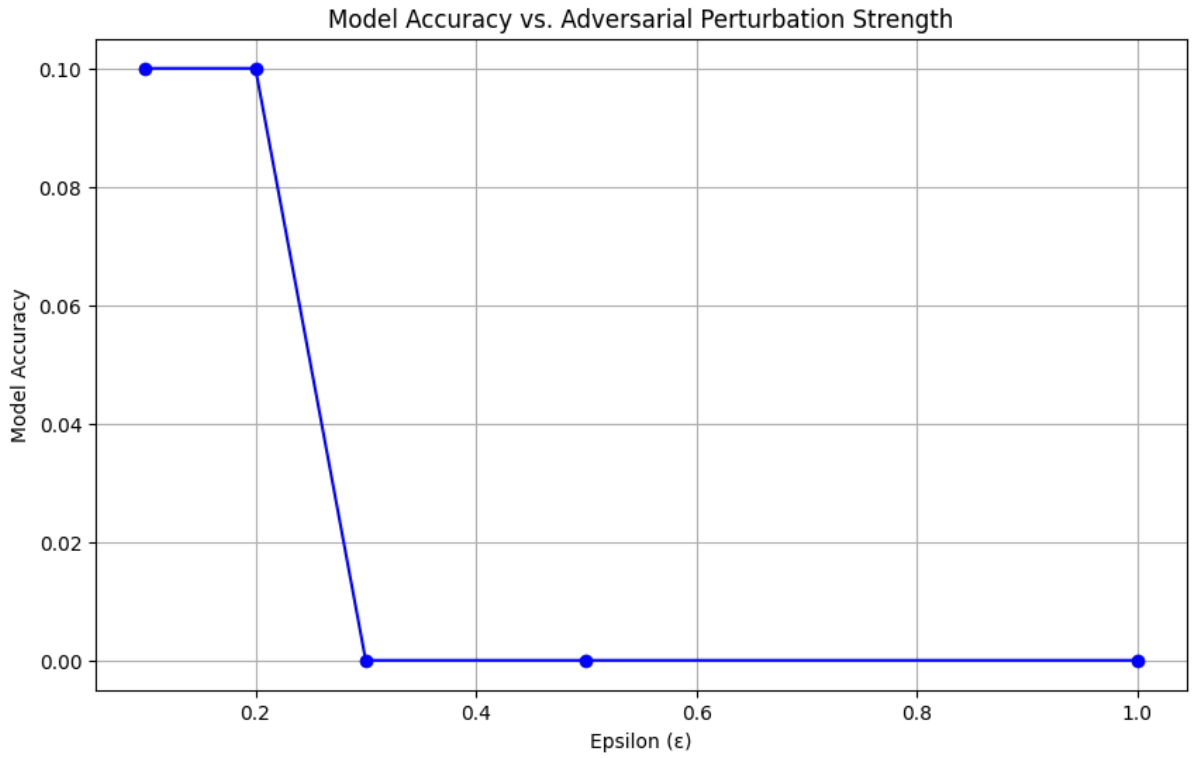

Anomalies using IQR (k=1.5)
Residuals
Anomalies (IQR k=1.5)
40
30
20
10
0
−10
−20
2024-01-01
2024-01-15
2024-02-01
2024-02-15
2024-03-01
2024-03-15
2024-04-01


Anomalies using IQR (k=3)
Residuals
Anomalies (IQR k=3)
40
30
20
10
0
−10
−20
2024-01-01
2024-01-15
2024-02-01
2024-02-15
2024-03-01
2024-03-15
2024-04-01

**Week # 4**

**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 3ms/step - accuracy: 0.9746 - loss: 0.1186
Original model accuracy: 0.9788

Training poisoned model...
313/313 ━━━━━━━━━━━━━━━━━━━━ 1s 3ms/step - accuracy: 0.0024 - loss: 24.6678
Poisoned model accuracy: 0.0018
```

**Week # 5**

## Text-based Cyber attacks

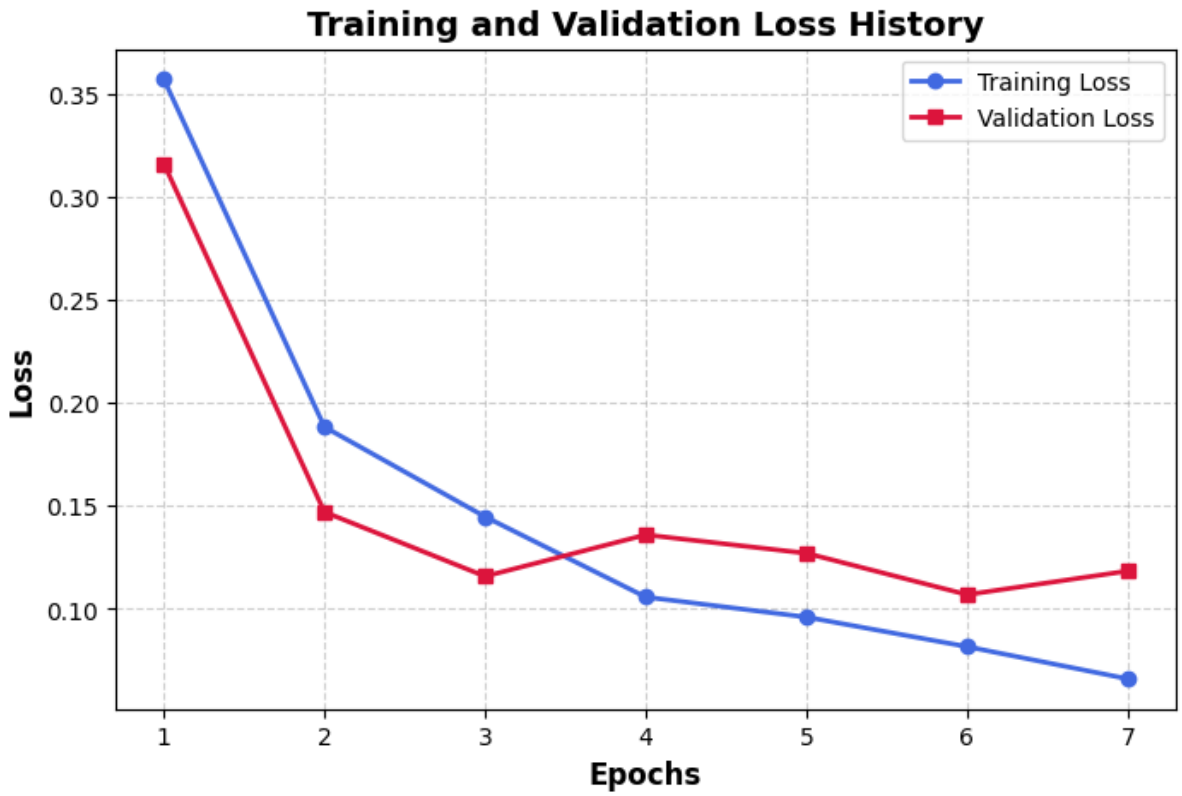
My SID is 2363665. So, 65/2 is 32.5, used epoch 33(ceil it).

...

```
Time for epoch 33 is 51.22585964202881 sec
```

**Week # 6**

## Cryptography



**Week # 7**

# Cryptography II

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

```
# Testing DES
# Example usage:
key = b'SecretKe'  # DES key must be exactly 8 bytes long
plain_text = "Taqi Sherazi"
encrypted = des_encrypt(plain_text, key)
print("Encrypted text:", encrypted)
decrypted = des_decrypt(encrypted, key)
print("Decrypted text:", decrypted)
```

✓ 0.0s

```
Encrypted text: 3Q1BcH3aRLp8n7rn05LA7Q==
Decrypted text: Taqi Sherazi
```

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

```
# Testing AES
key = b'16bytekeylengthp'  # AES requires 16-byte, 24-byte, or 32-byte key
plain_text = "The ARU"  # The text to encrypt
encrypted_text = aes_encrypt(plain_text, key)  # Encrypt the text
decrypted_text = aes_decrypt(encrypted_text, key)  # Decrypt the text

# Print the results
print(f"AES Encrypted: {encrypted_text}")  # Output the encrypted text
print(f"AES Decrypted: {decrypted_text}")  # Output the decrypted text
```

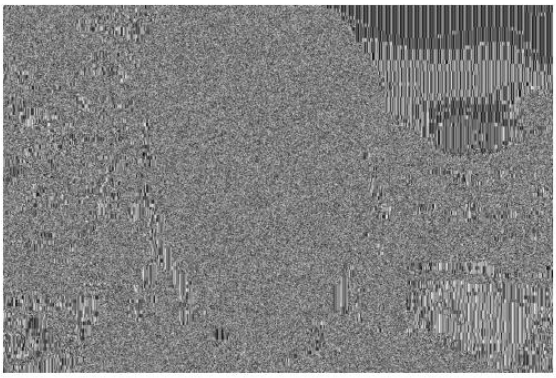
[11] ✓ 0.0s

```
<class 'str'>
AES Encrypted: XsLEmrhOHvvmg9Bg3n8Pug==
AES Decrypted: The ARU
```

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

Real Image

Cipher Image



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

**No.** AES in ECB (Electronic Codebook) mode is not secure for encrypting images because identical plaintext blocks produce identical ciphertext blocks.

**Week # 8**

## Hash Functions, Digital Signature, and Blockchain

**Partner's Name:** Zanib Shafqat

Values:

p (Prime Number): 23

g (Generator): 5

My Private Key (a): 6

Computed Public Key (A):

A = g^a mod p = 5^6 mod 23 = 8

p: 23

g: 5

s (Shared Secret): 2

My Private Key: 6

**Week # 9**

## Network-based attacks

**Attack Type Chosen:**

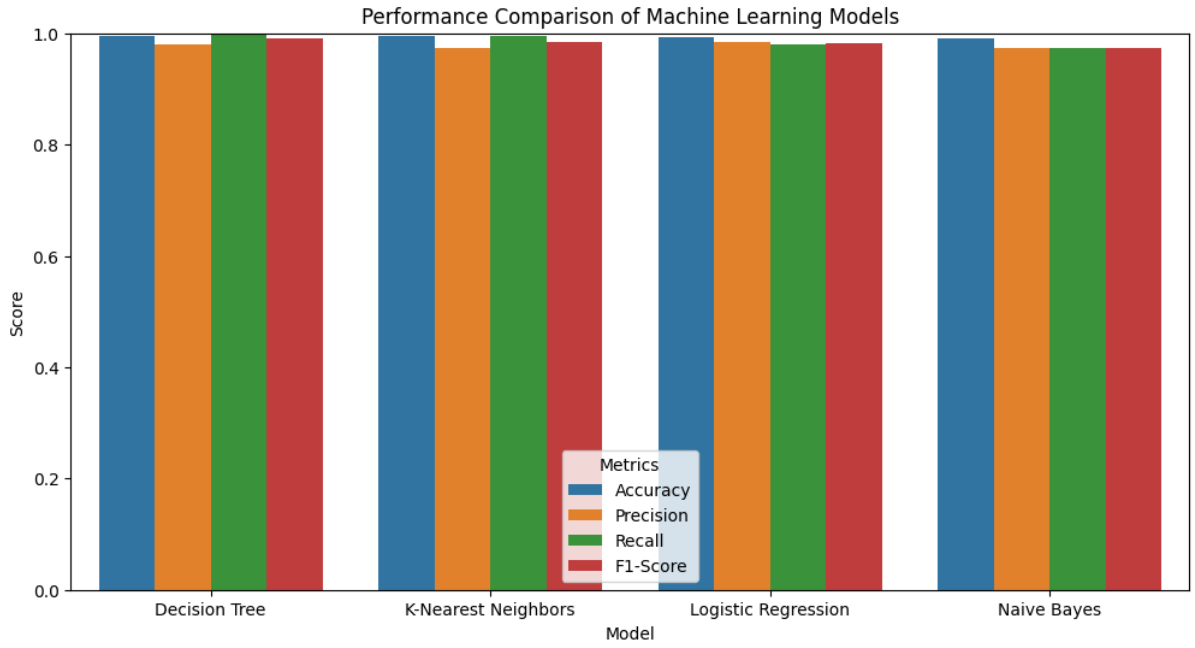
SolarWinds Supply Chain Attack (2020)

**Key Research Source:**

CISA Advisory AA20-352A: "Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations" https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-352a

## Week # 10

# Network Intrusion Detection and Malwares



## Week # 11

# Honeypots, DMZ, CTI sharing and Cyber security framework

```
Detailed Model Performance:

Random Forest:
  Accuracy: 0.9999
  Precision: 0.9999
  Recall: 0.9999
  F1 Score: 0.9999
  Cross-validation Accuracy: 0.9988

Logistic Regression:
  Accuracy: 0.9990
  Precision: 0.9990
  Recall: 0.9990
  F1 Score: 0.9990
  Cross-validation Accuracy: 0.9983

SVM:
  Accuracy: 0.9994
  Precision: 0.9994
  Recall: 0.9994
  F1 Score: 0.9994
  Cross-validation Accuracy: 0.9985

KNN:
  Accuracy: 0.9997
  Precision: 0.9997
  Recall: 0.9997
  F1 Score: 0.9997
  Cross-validation Accuracy: 0.9988

Best performing model: Random Forest
```