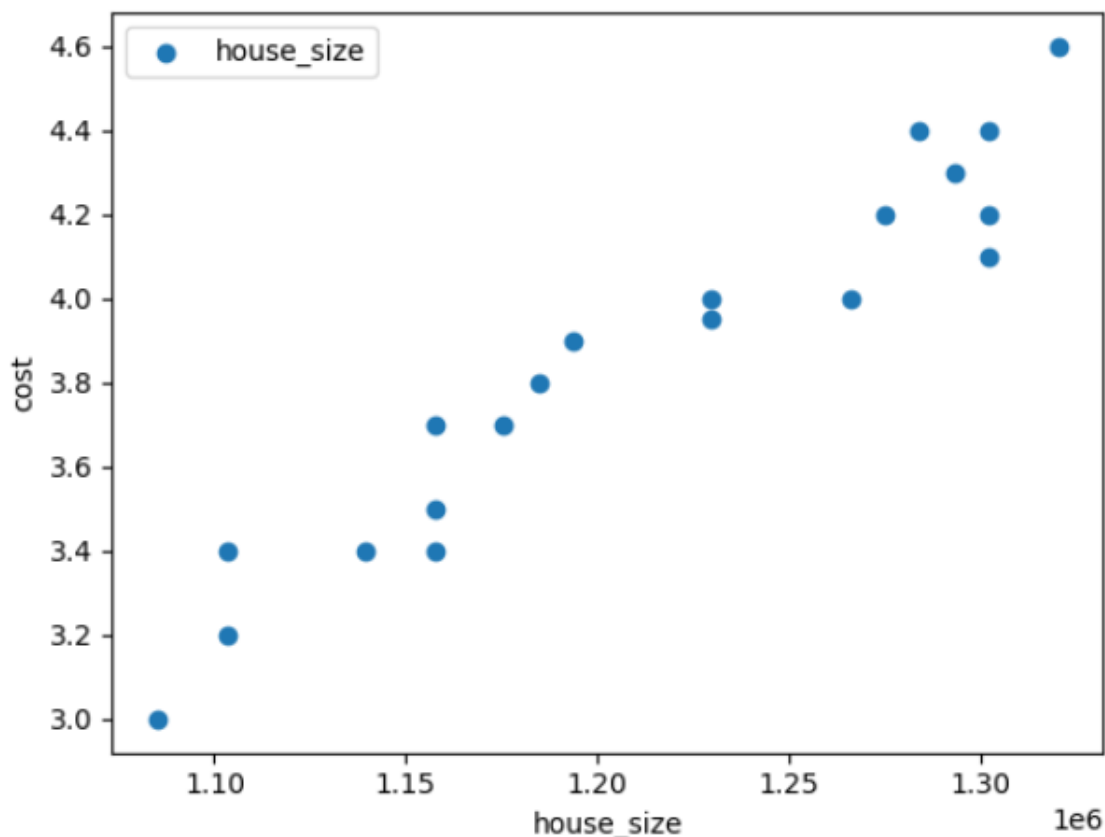


# LAB Logbook

## Lab 1

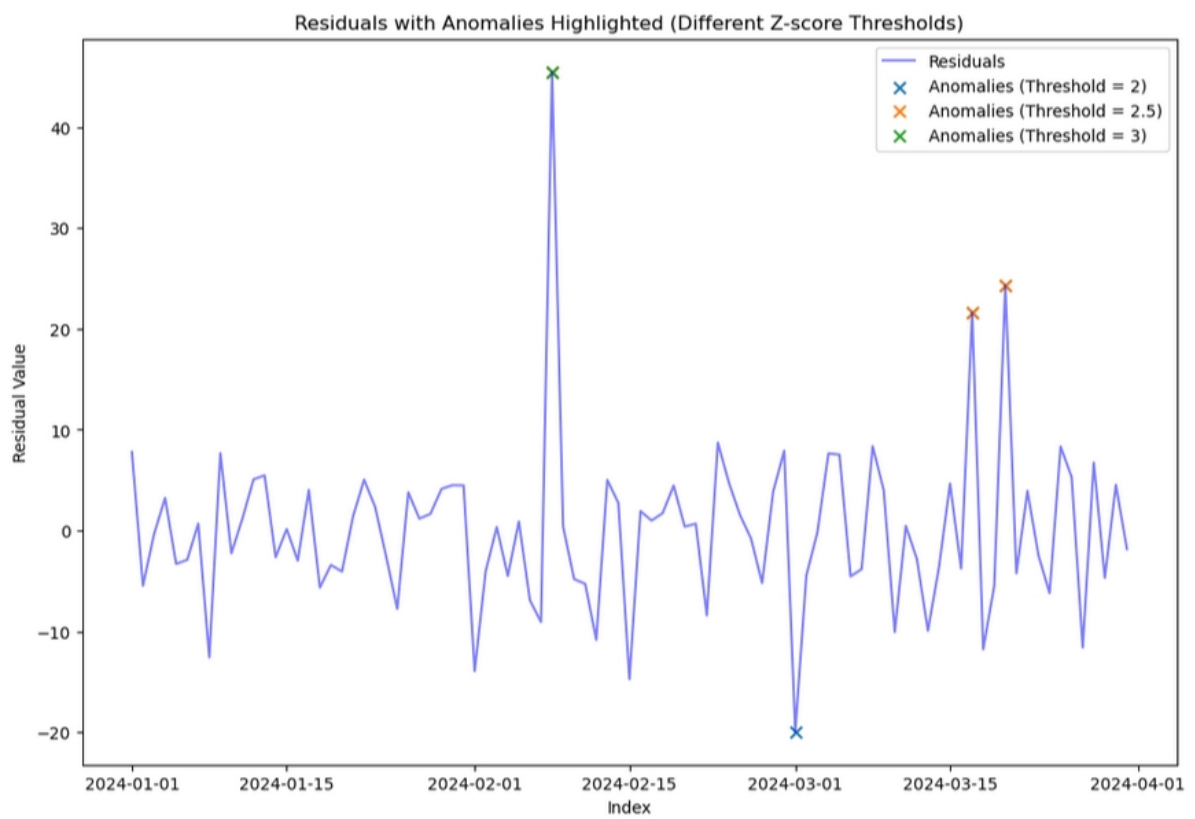
- **Series:** A Pandas Series is a one-dimensional array-like object that can hold any data type and has an associated index for easy labelling and access.
- **DataFrame:** A DataFrame is a two-dimensional, tabular data structure with rows and columns, making it ideal for storing and manipulating datasets.
- **Index:** An Index in Pandas is an immutable array used for labelling and aligning data in Series or DataFrames, enabling efficient data retrieval and manipulation.
- **Categorical:** The Categorical type in Pandas allows for efficient storage and manipulation of data with a fixed number of possible values, making it ideal for handling categorical data.
- **DatetimeIndex:** A DatetimeIndex is a specialised index in Pandas for handling time series data, allowing for fast date-based indexing and resampling operations.

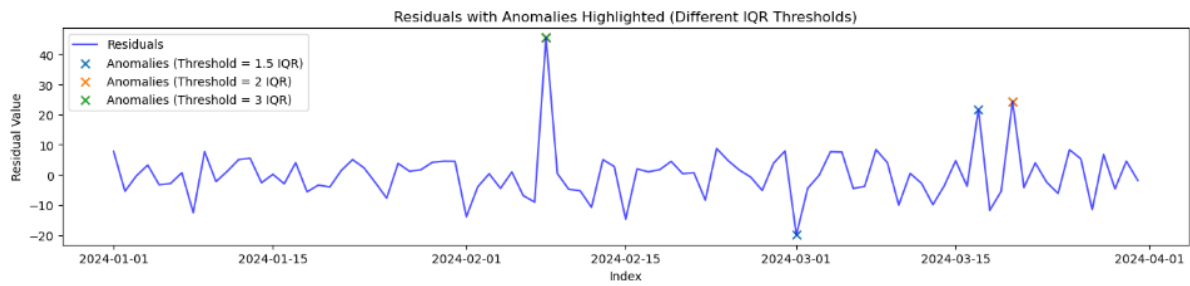
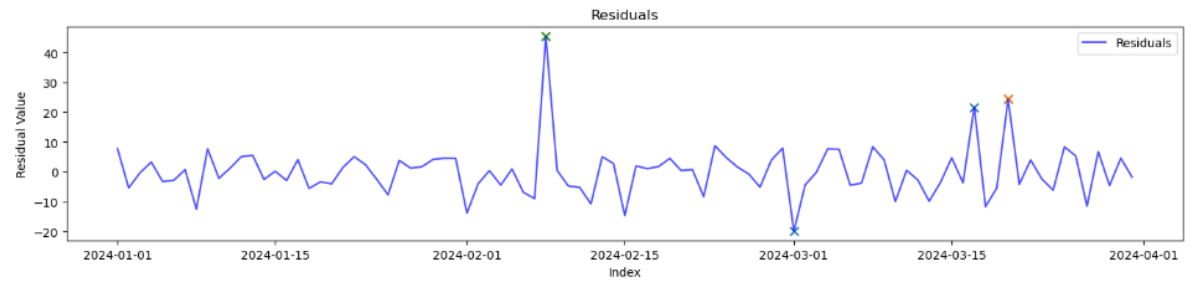
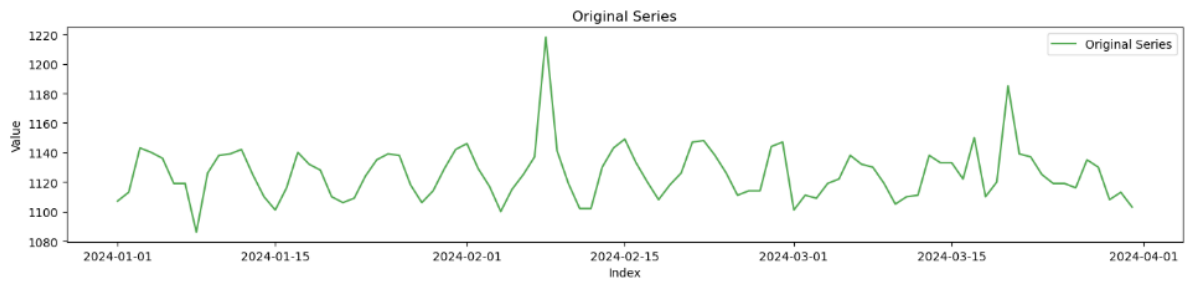
## Lab 2



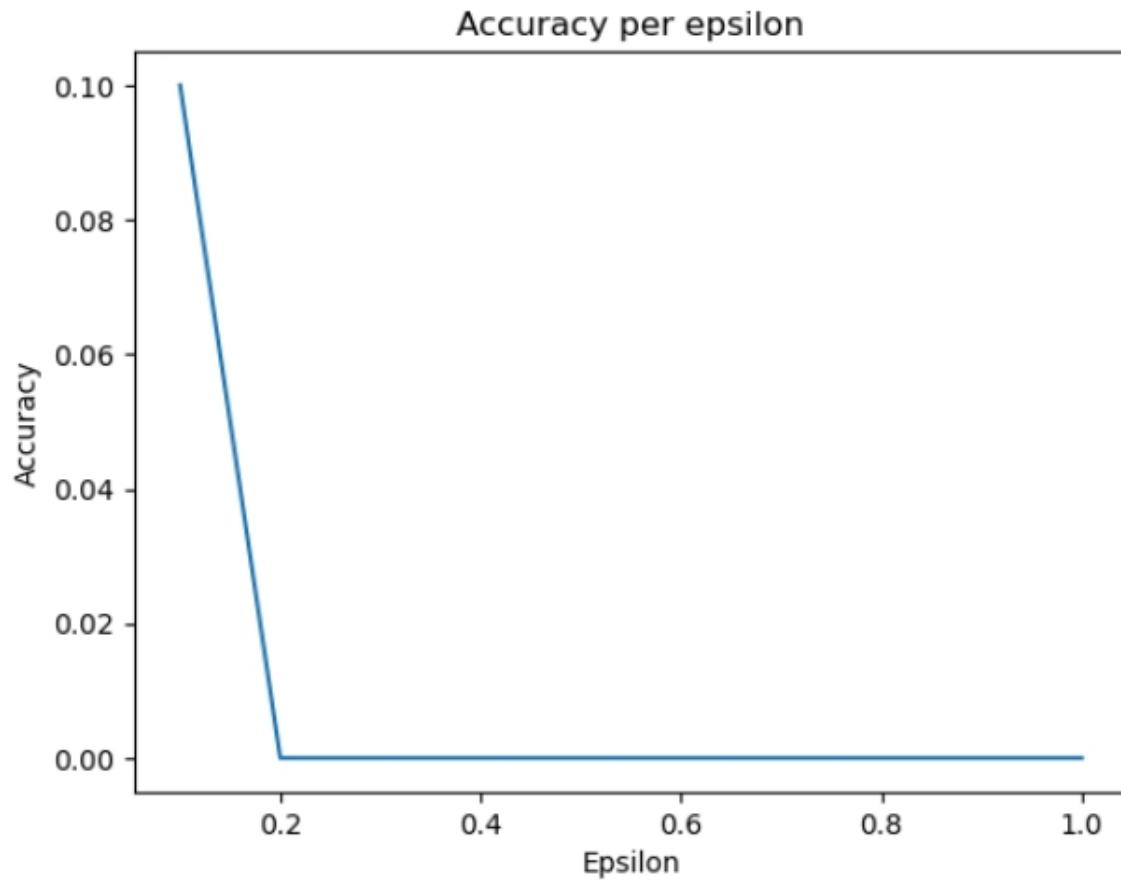
Price guess for size of  $SID \cdot 0.75 = 4.9$

## Lab 3





## Lab 4



The higher the epsilon value, the less accuracy there is. The model is very weak against adversarial attacks.

**313/313** ————— **1s** 4ms/step - accuracy: 0.9769 - loss: 0.1016  
Test Accuracy Original: 0.9798

---

**313/313** ————— **1s** 4ms/step - accuracy: 0.1027 - loss: 123255.7109  
Test Accuracy poisoned: 0.1028

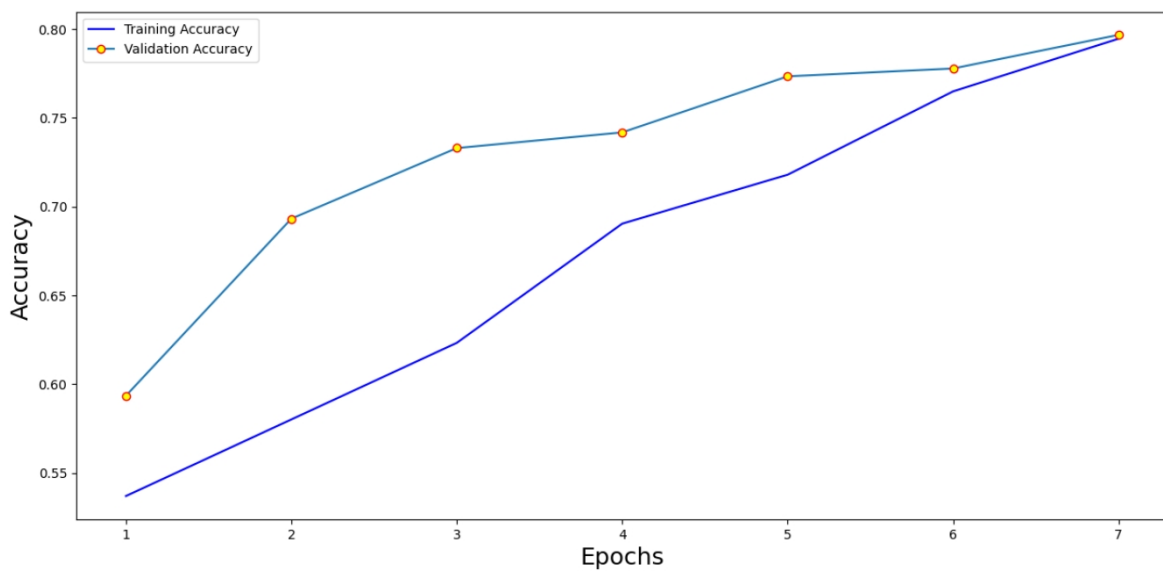
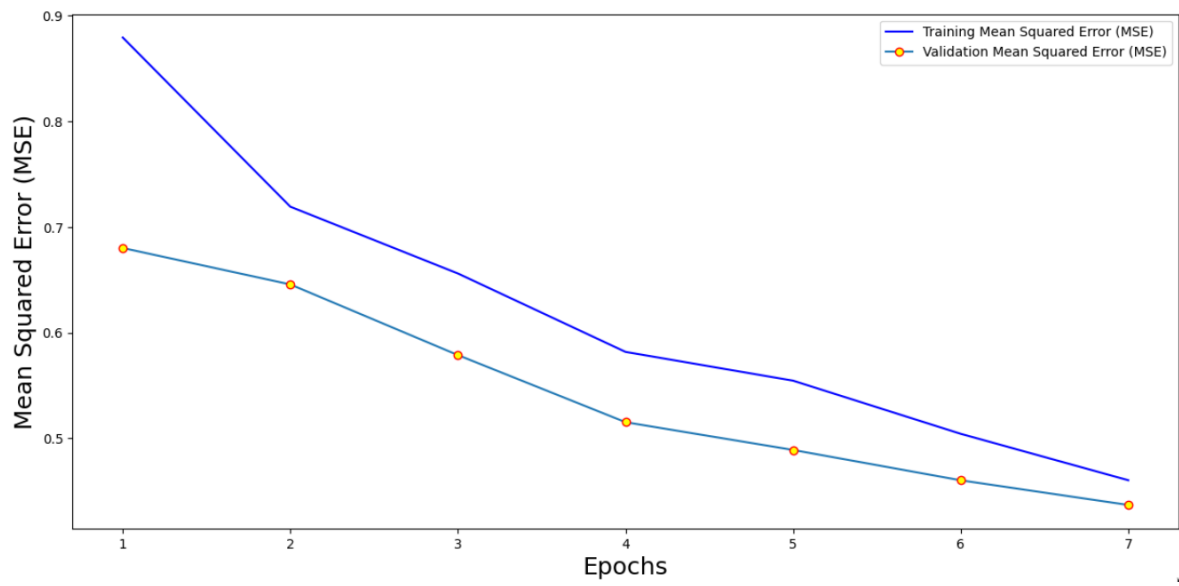
## Lab 5



Time for epoch 31 is 11.749621391296387 sec

---

## Lab 6



## Lab 7

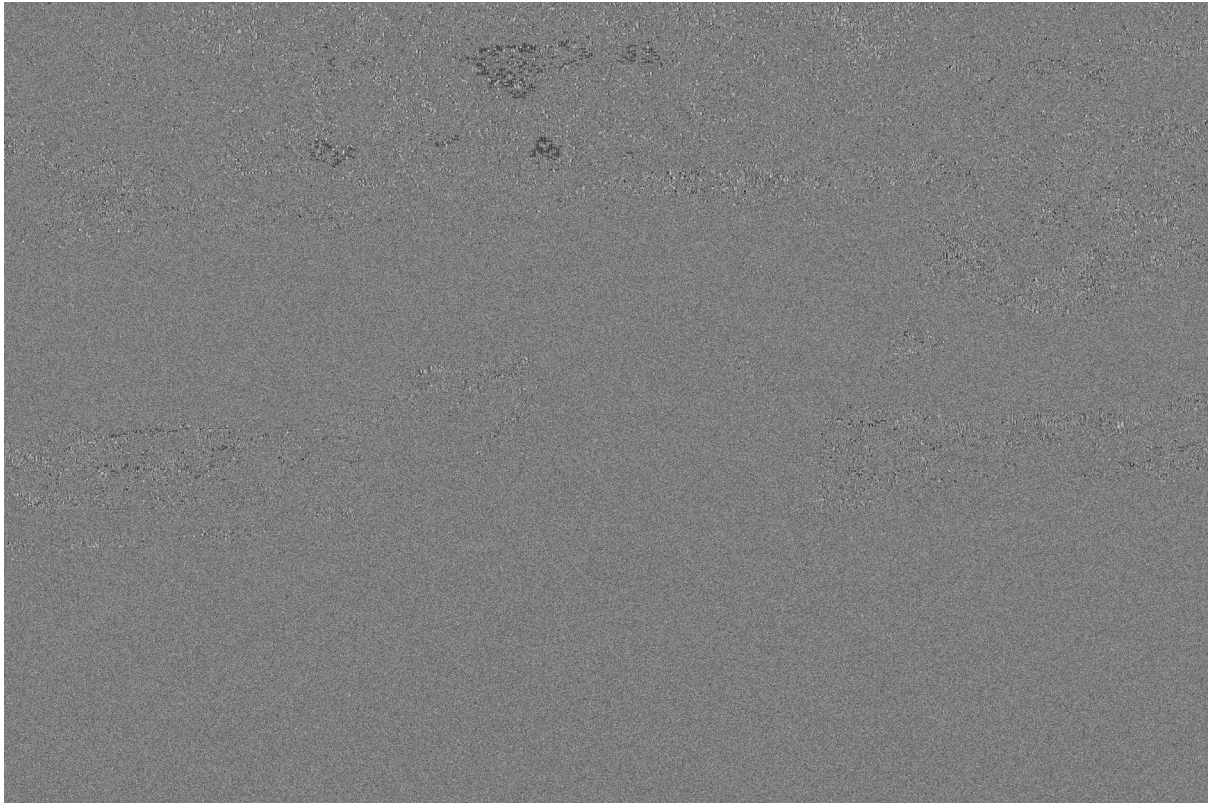
## DES

```
Enter the key (8 bytes): SecretKe  
<class 'bytes'>  
Enter the text to encrypt: HelloCrypto  
Encrypted text: HQqgsqSEljgBPH7L4con0w==  
Decrypted text: HelloCrypto
```

## AES

```
Enter the key (24 bytes): ffffffffffhhhhhhhhhhjjjj  
Enter the text to encrypt: adsfadfs  
<class 'str'>  
AES Encrypted: JIBUfy1kUpQWa4Tdavd70w==  
AES Decrypted: adsfadfs
```





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

YES

## Lab 8

Maher Salimboev

$p = 23$

$g = 5$

$s = 2$

privatekey = 15



## Lab 9

1. The attack type you have chosen

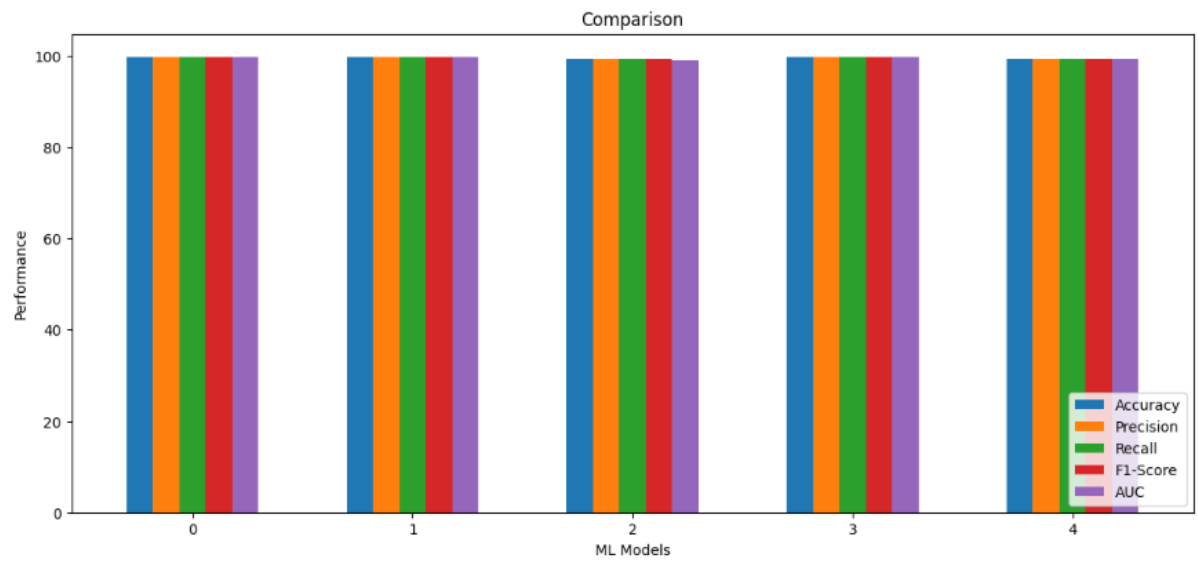
**Log4j Vulnerability Exploit (2021)** – A critical flaw in Log4j allowed remote code execution across various systems.

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

<https://builtin.com/articles/log4j-vulnerability-explained>

## Lab 10

	AI Models	Accuracy	Precision	Recall	F1-Score	AUC
0	rf	99.7	99.7	99.7	99.7	99.81
1	gb	99.7	99.7	99.7	99.7	99.81
2	svm	99.4	99.4	99.4	99.4	99.03
3	nn	99.8	99.8	99.8	99.8	99.68
4	lstm	99.4	99.4	99.4	99.4	99.23



Lab 11

Lab 12