**ATTACK DETECTION USING DEEP LEARNING IN VANET**

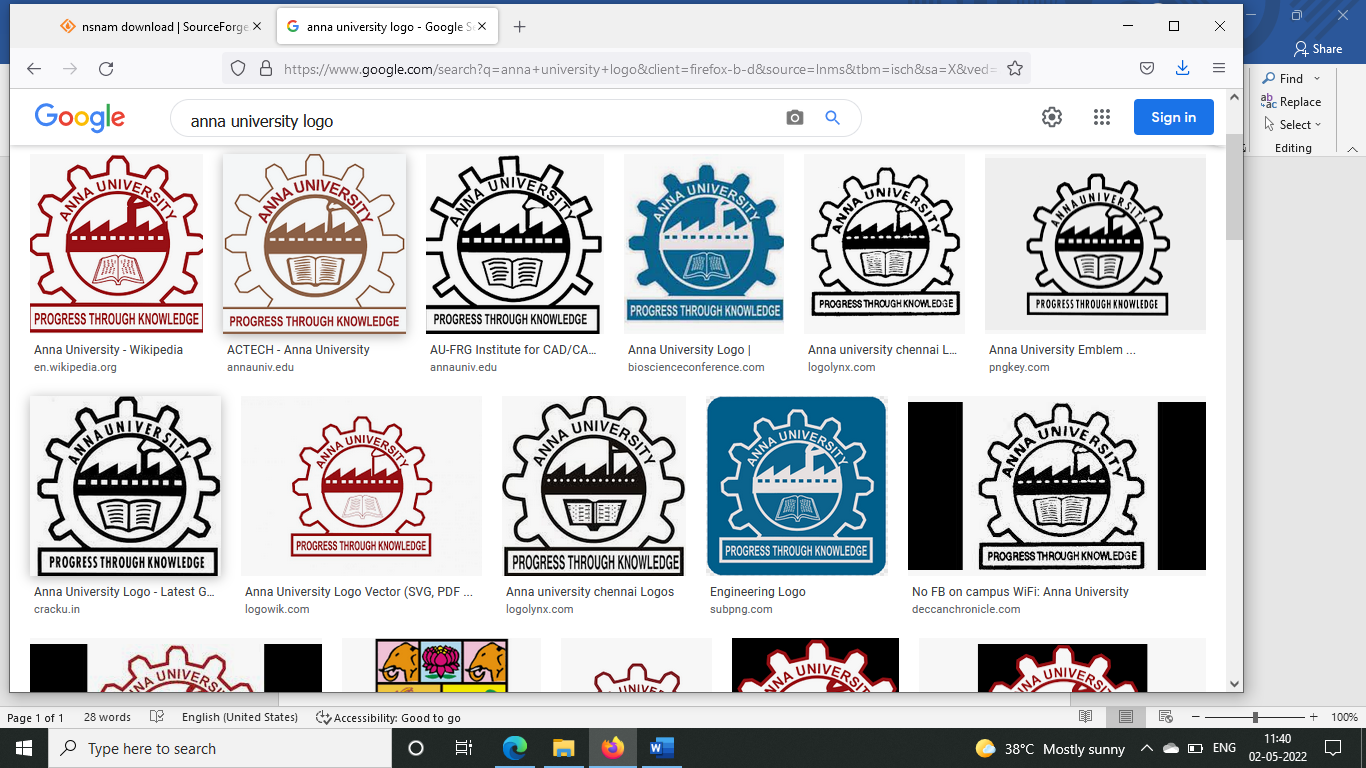
**PHASE I REPORT**

***Submitted by***

**P. SRILAKSHMI**

***In partial fulfilment for the award of the degree of***

**MASTER OF COMPUTER APPLICATION**



**DEPARTMENT OF INFORMATION SCENCE AND TECHNOLOGY**

**ANNA UNIVERSITY, CHENNAI**

**MAY, 2022**

**ANNA UNIVERSITY, CHENNAI**

**BONAFIDE CERTIFICATE**

Certified that this Report titled **ATTACK DETECTION USING DEEP LEARNING IN VANET** is the bonafide work of **P. SRILAKSHMI (2019272037)** who carried out the work under my supervision. Certified further that to the best of my knowledge the work reported herein does not form part of any other thesis or dissertation on the basis of which a degree or award was conferred on an earlier occasion on this or any other candidate.

Dr. S. Sridhar Ms. G. Mahalakshmi

Professor and head Teaching Fellow

Department of information Department of information

Science and technology science and technology

Anna university Anna university

Chennai - 600 025 Chennai – 600 025

**TABLE OF CONTENTS**

**CHAPTER NO. TITLE PAGE NO.**

**ABSTRACT 4**

1. **INTRODUCTION 5**
   1. MOTIVATION
   2. PROPOSED SYSTEM
   3. OBJECTIVE
2. **REVIEW OF LITERATURE 6**
   1. EXISTING / RELATED WORKS
3. **SYSTEM REQUOREMENT**

**SPECIFICATION 9**

3.1 REQUIREMENT ANALSIS

3.2 SYSTEM SPECIFICATION

1. **DESIGN CONCEPTS 10**
   1. DETAILED ARCHITECTURE

DIAGRAM

1. **IMPLEMENTATION 11**
   1. LIST OF MODULES
   2. ALGORITHMS
   3. MODULE BASED OUTPUT
2. **CONCLUSION 19**
3. **REFERENCES 20**

**ABSTRACT:**

Vehicular Ad hoc Networks (VANETs) are the core of Intelligent Transportation Systems (ITS), allowing vehicles to communicate between themselves and with other entities. However, these are very complex networks with volatile architectures, ever-changing members, and multiple types of entities, making them an appealing target for attackers since they can find vulnerabilities and perform attacks with massive impact. The presence of a large number of communicating vehicles greatly increases the number and types of possible anomalies in the network. However, since there can be a multitude of anomalies possible in the network, there is a need for better anomaly detection frameworks that can address this unprecedented scenario. In this project, we propose an anomaly detection framework for VANETs based on deep neural networks (DNNs) using PCA and DNN algorithms. Our DNN model learns the abstract and high-dimensional feature representation of the IDS data by passing them into many hidden layers.

**CHAPTER 1: INTRODUCTION**

* 1. **MOTIVATION**
* Intrusions occurs frequently in the networks. So, in order to identify and detect these intrusions this project is used.
* In this way, we can detect the intrusion early and save our data. The main objective is to identify the attacks and then classify them into different categories.
* It uses DNN to predict an incoming value as attack or not and classify them accordingly.
  1. **PROPOSED SYSTEM**

The project aims to detect and identify the different types of attacks that occur in the VANETs. We use Deep learning-based intrusion detection system. In this project we present an end-to-end DL-Based intrusion detection method for the VANET with only the given datasets. We also evaluate our method on two public datasets, experimental results show the capability of applying this in the VANET and the effectiveness of detecting malware traffic.

This project uses DNN algorithm. They are structured in the form of interconnected nodes with an input layer, an output layer and one or more hidden layers. The model as various layers where input to each node is produced by applying some non-linear function on the data.

* 1. **MOTIVATION**

The aim of our study is to incorporate feature engineering to enhance the performance of Deep Learning techniques for attack classification. Due to the wide variety of attacks, and the unavoidable loopholes in traditional security methods, it is not possible to entirely prevent attacks on VANETs. This is done using the available feature selection and classification algorithm through which we get best results for the dataset. Numerical results will show that we can correctly detect data corresponding to several anomaly types.

**CHAPTER 2: LITERATURE SURVEY**

**2.1 PROPOSED / EXISTING WORKS:**

1. **Deep Learning Approach for Intelligent Intrusion Detection System:**

Authors: R. Vinayakumar, Mamoun Alazab, K. P. Soman, Prabaharan

Poornachandran , Ameer Al-Nemrat , And Sitalakshmi Venkatraman.

Paper published in: IEEE Access (Volume: 7) Digital Object Identifier 10.1109/ACCESS.2019.2895334.

**Concept in the paper**:

In this paper, a hybrid intrusion detection alert system is proposed which has the capability to analyze the network and host-level activities. It uses DNNs for handling and analyzing very large-scale data in real-time. The proposed architecture is able to perform better than previously implemented classical machine learning classifiers in both HIDS and NIDS. The execution time of the proposed system can be enhanced by adding more nodes to the existing cluster. In addition, the proposed system does not give detailed information on the structure and characteristics of the malware.

1. **DeepADV: A Deep Neural Network Framework for Anomaly Detection in VANETs:**

Authors: Tejasvi Alladi,Bhavya Gera, Ayush Agrawal, Vinay Chamola and Fei Richard Yu

Paper published in: IEEE TRANSACTIONS ON VEHICULAR TECHNOLO-GY, VOL. 70, NO. 11, NOVEMBER 2021

**Concept in the paper:**

A DNN-based anomaly detection framework for the identification of anomalous data pertaining to various possible anomalies in VANETs. Anomaly scenarios are considered for analyzing the performance of the proposed framework. Performance analysis of the framework using key evaluation metrics is presented by employing several DNN architectures.

1. **Malicious Node Detection in Vehicular Ad-Hoc Network Using Machine Learning and Deep Learning:**

Authors: Elvin Eziama , Kemal Tepe , Ali Balador , Kenneth Sorle Nwizege and Luz M. S. Jaimes

Paper published in: 2018 IEEE Globecom Workshops (GC Wkshps)

**Concept in the paper**:

The paper proposes the Bayesian Neural Network (BNN) model framework for high performance prediction, classification accuracy and low detection latency, in trust computation in VANET. The idea of BNN framework is needed to overcome the challenges in NN. The future work aims at implementing the proposed framework in Veins simulator and providing simulation experiments.

1. **Deep Neural Networks for Securing IoT Enabled Vehicular Ad-Hoc Networks**

Authors: Tejasvi Alladi, Ayush Agrawal , Bhavya Gera, Vinay Chamola, Biplab Sikdar, Mohsen Guizani

Paper published in: CC 2021 – IEEE International Conference on Communications.

**Concept in the paper**:

In this paper, a deep neural network architecture for securing IoT-enabled VANETs is proposed. Deep learning models were trained on time sequences generated from normal vehicle data in the network. The paper talks about classify sequences into normal data and anomalies and perfectly classify most of the anomalous types. The proposed CNN & LSTM model is shown to give a higher performance compared to a stacked LSTM model.

1. **DeepVCM: a Deep Learning Based Intrusion Detection Method in VANET:**

Authors: Yi Zeng, Meikang Qiu, Dan Zhu, Zhihao Xue, Jian Xiong, and Meiqin Liu

Paper published in: IEEE Intl Conference on Intelligent Data and Security (IDS)

**Concept in the paper**:

The DeepVCM procedure is consist of two common DL models, namely CNN and LSTM. This method does not require the heavy work of selecting features and private featured details. Moreover,it can attain a much more robust and accurate performance on intrusion detection than state-of-art methods with a less storage resource requirement.

**CHAPTRER 3: SYSTEM REQUIREMENT SPECIFICATION**

**3.1 REQUIREMENT ANALYSIS**

Language used:

* Python

Platform used:

* Jupyter notebook

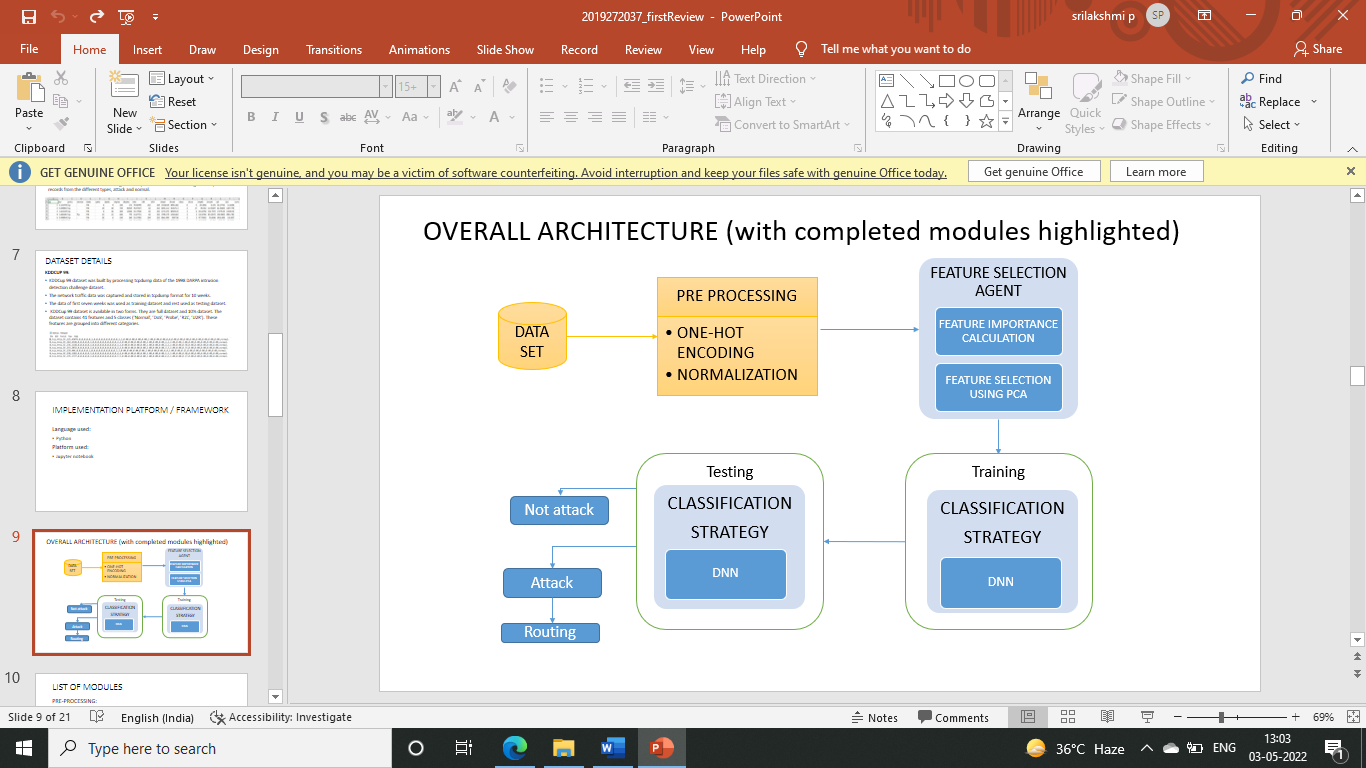
**3.2 SYSTEM SPECIFICATION**

Hardware specification:

* Processor: standard processor with a speed of 1.6 GHz or more
* RAM: 4GB
* Windows 10 operating system (64-bit)

**CHAPTER 4: DESIGN CONCEPTS**

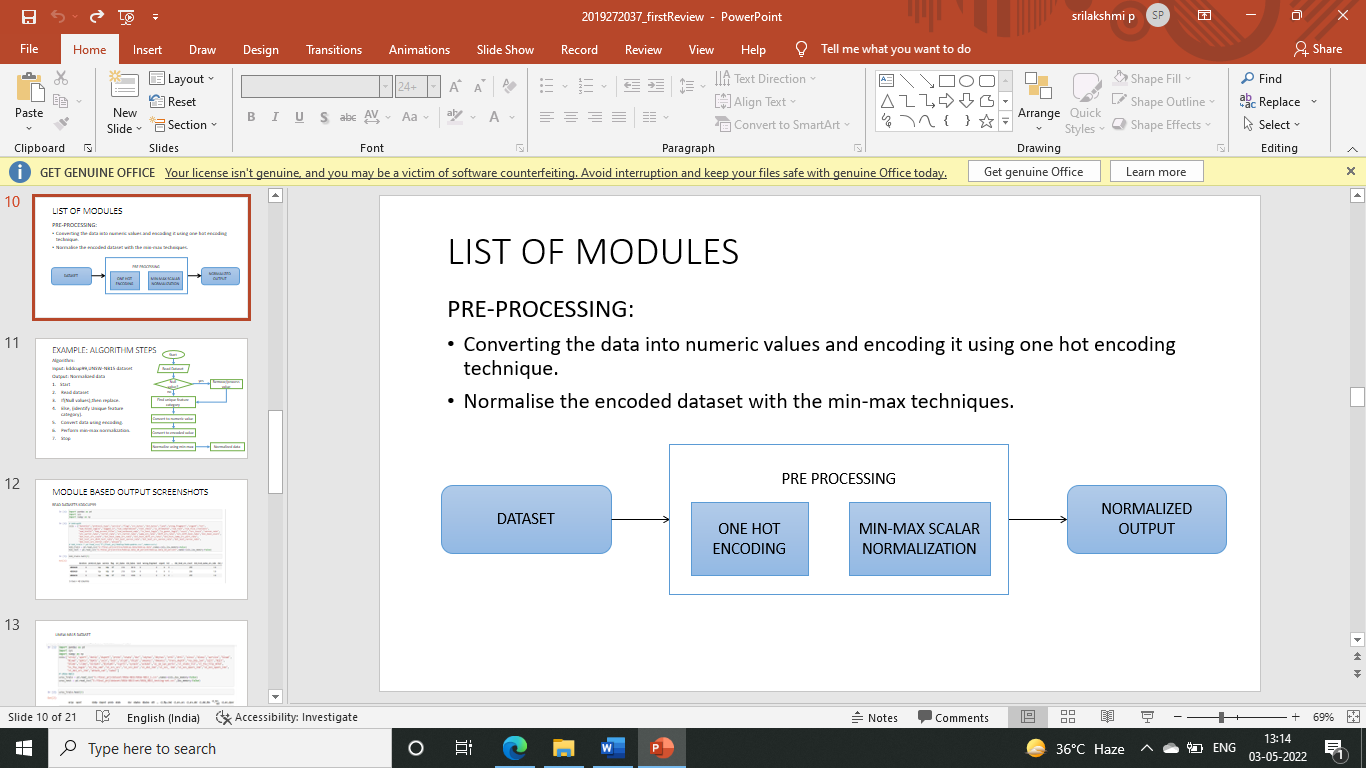
**4.1 DETAILED ARCHITECTURE DIAGRAM:**



**CHAPTER 5: IMPLEMENTATION**

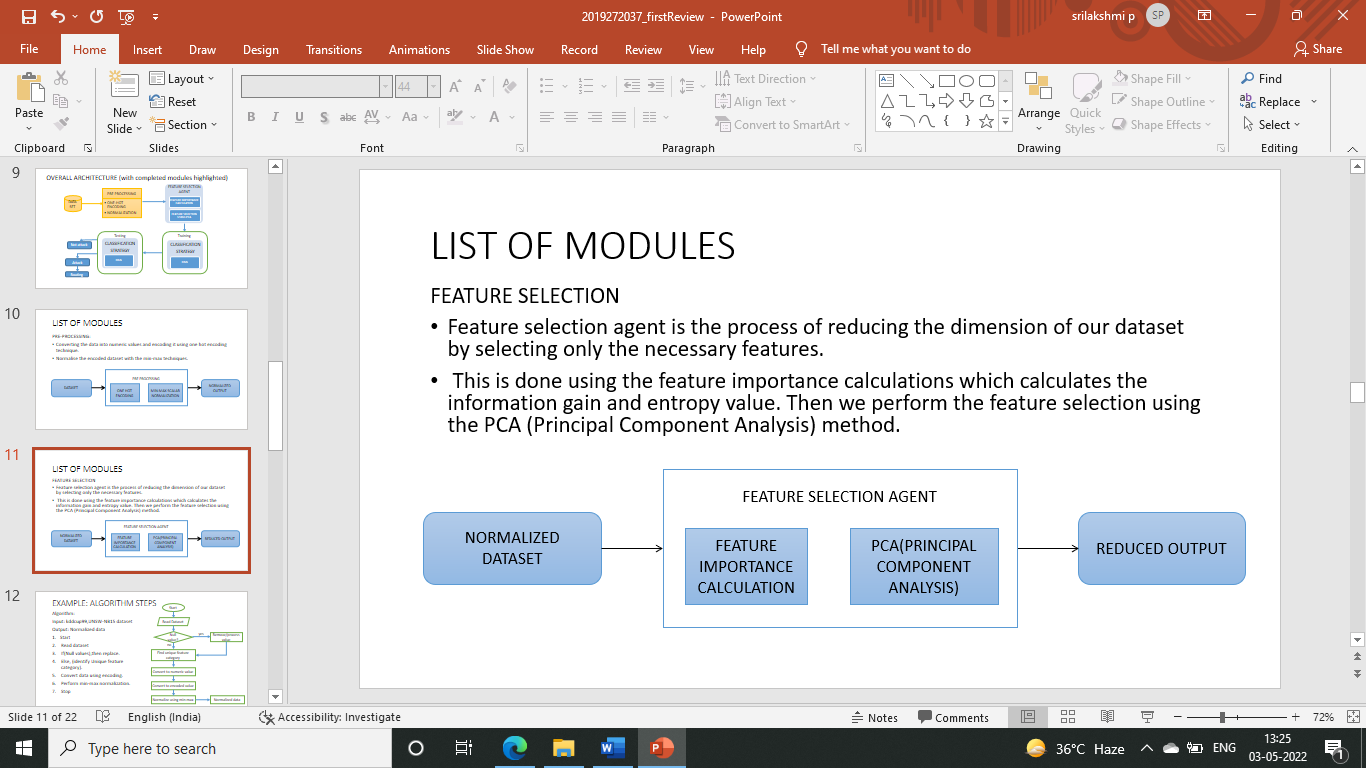
* 1. **LIST OF MODULES**
     1. **Pre-processing**:

Converting the data into numeric values and encoding it using one hot encoding technique. Normalise the encoded dataset with the min-max techniques.



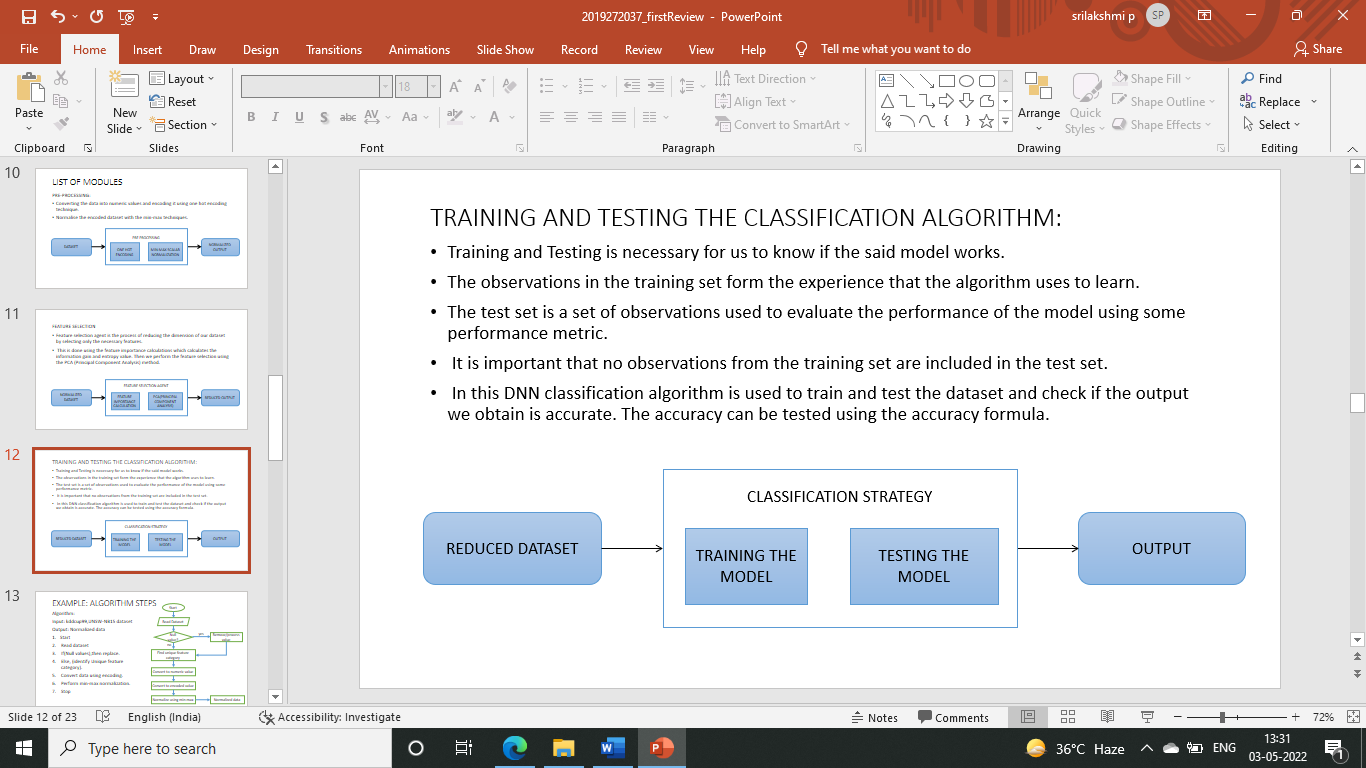
* + 1. **Feature selection:**

Feature selection agent is the process of reducing the dimension of our dataset by selecting only the necessary features. This is done using the feature importance calculations which calculates the information gain and entropy value. The we perform the feature selection using the PCA (Principal Component Analysis) method.



* + 1. **Training and testing the classification Algorithm:**

Training and Testing is necessary for us to know if the said model works. The observations in the training set form the experience that the algorithm uses to learn. The test set is a set of observations used to evaluate the performance of the model using some performance metric. It is important that no observations from the training set are included in the test set. In this DNN classification algorithm is used to train and test the dataset and check if the output we obtain is accurate. The accuracy can be tested using the accuracy formula.



**5.2 ALGORITHM AND FLOW DIAGRAM:**

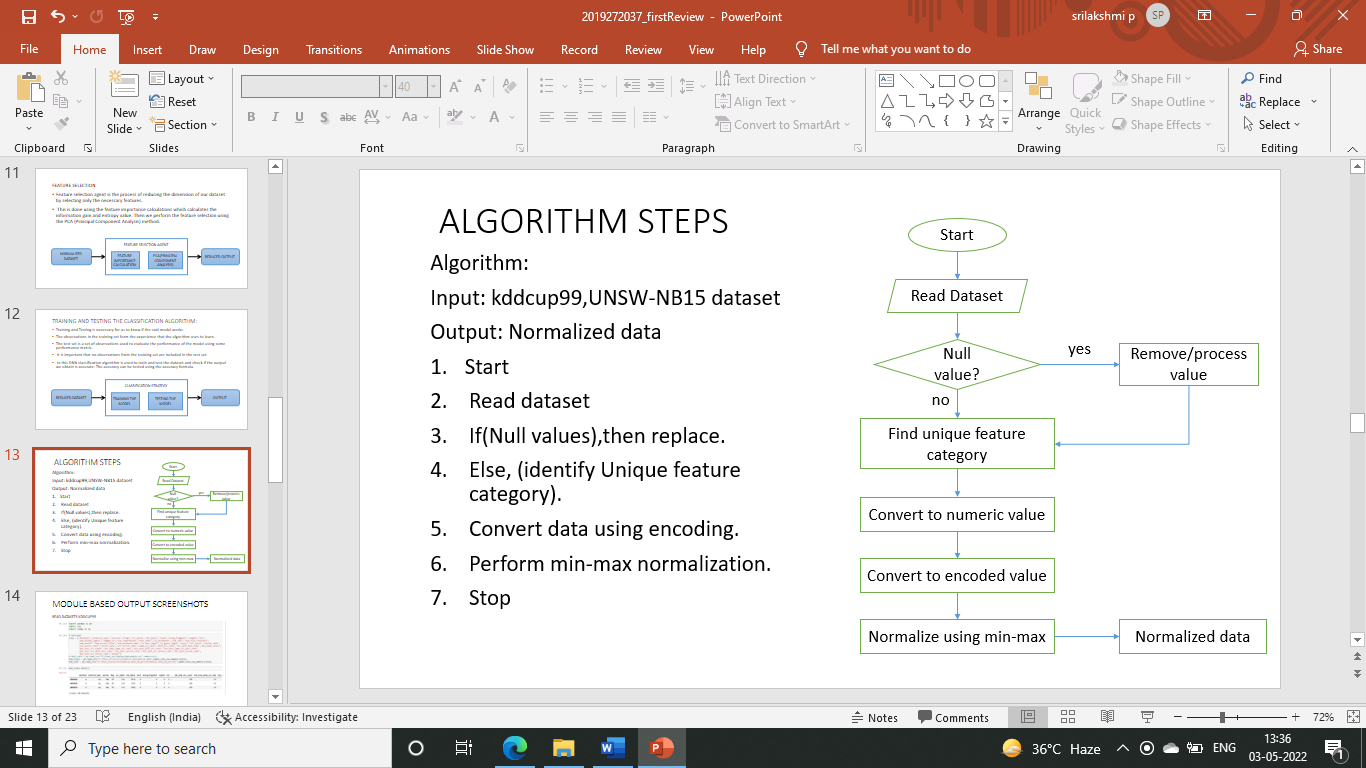
Algorithm:

Input: kddcup99,UNSW-NB15 dataset

Output: Normalized data

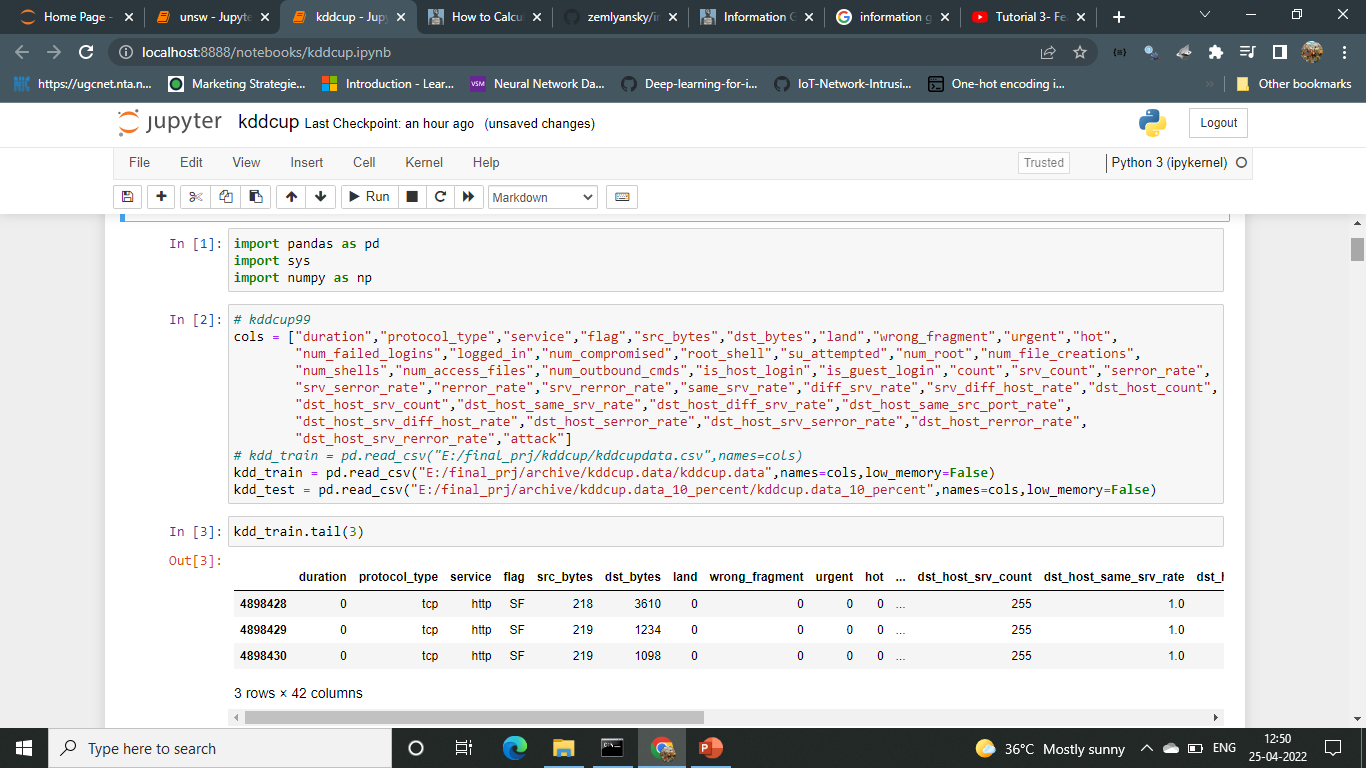
1. Start
2. Read dataset
3. If (Null values),then replace.
4. Else, (identify Unique feature category).
5. Convert data using encoding.
6. Perform min-max normalization.
7. Stop

Flow diagram:

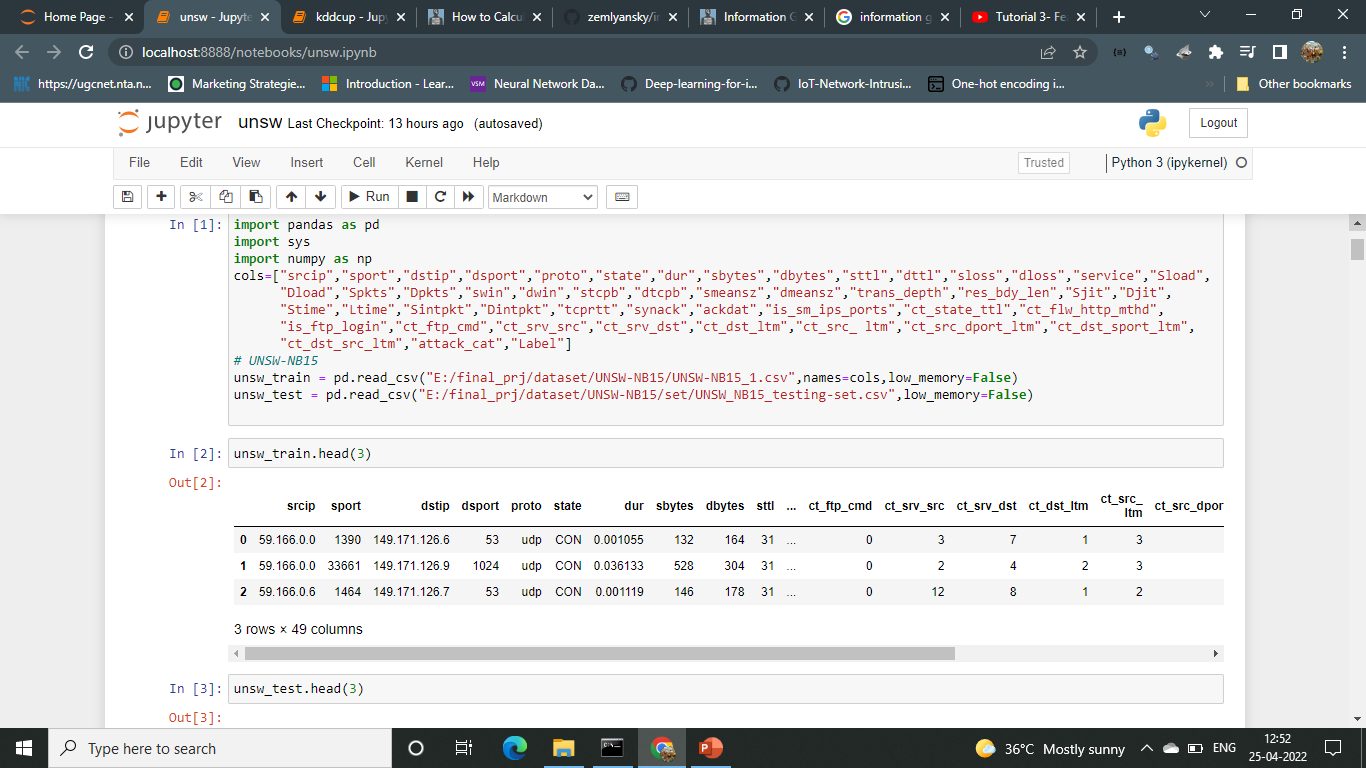


**5.3** **MODULE BASED OUTPUT:**

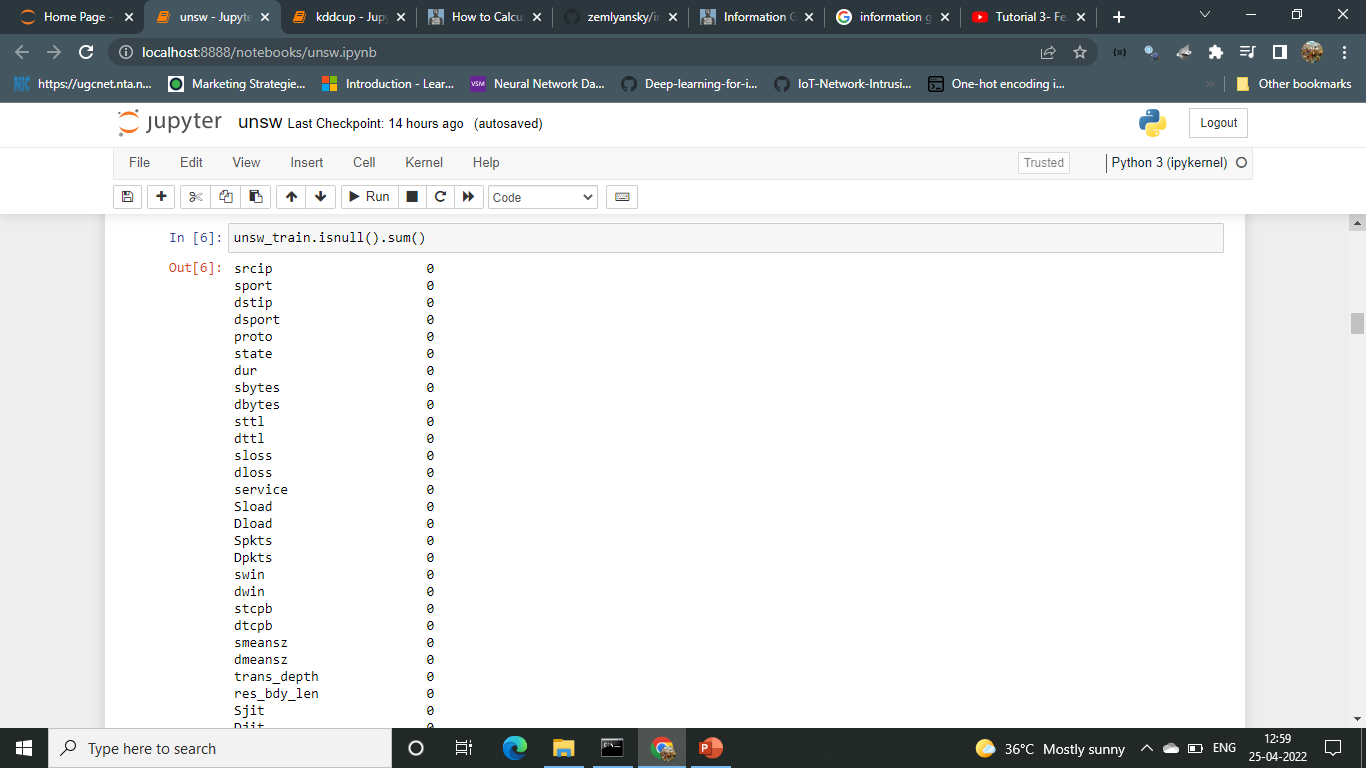
READ DATASETS KDDCUP99

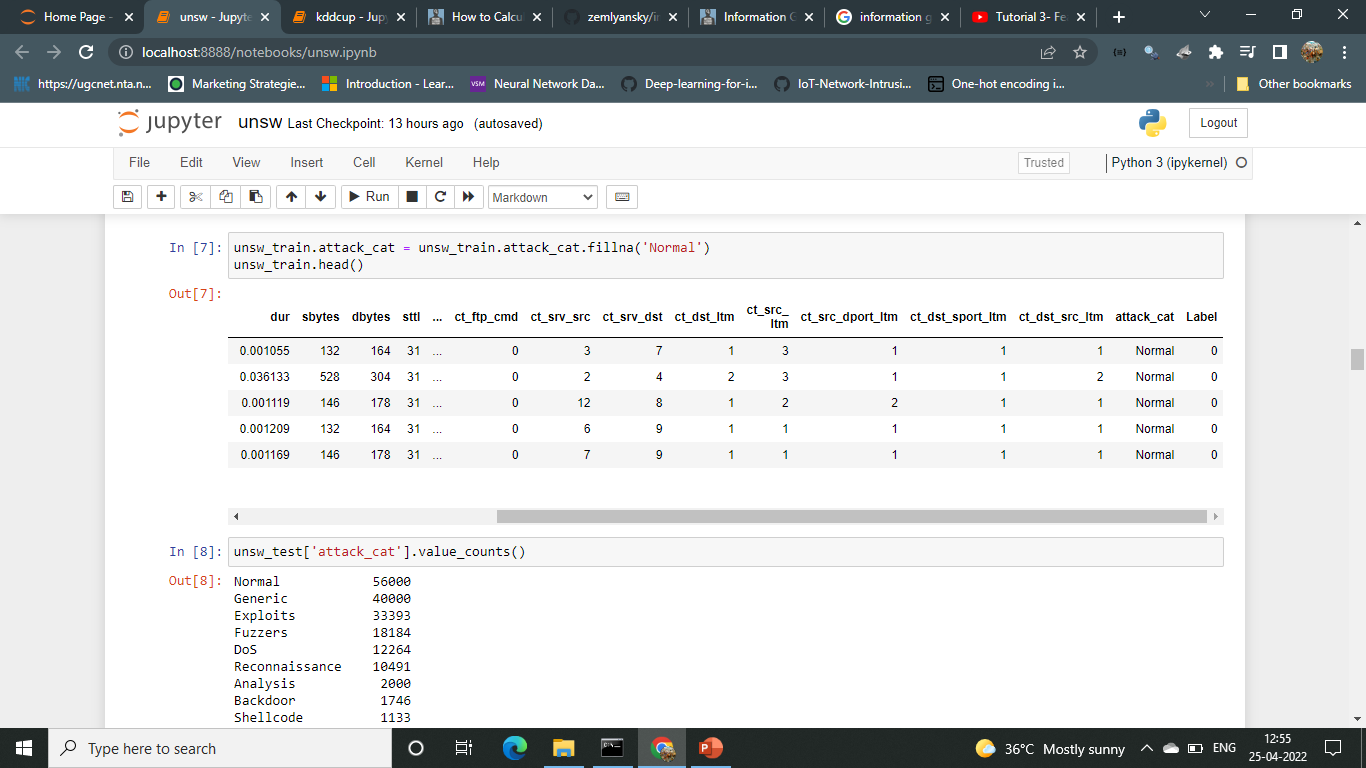
****

UNSW-NB15 DATASET

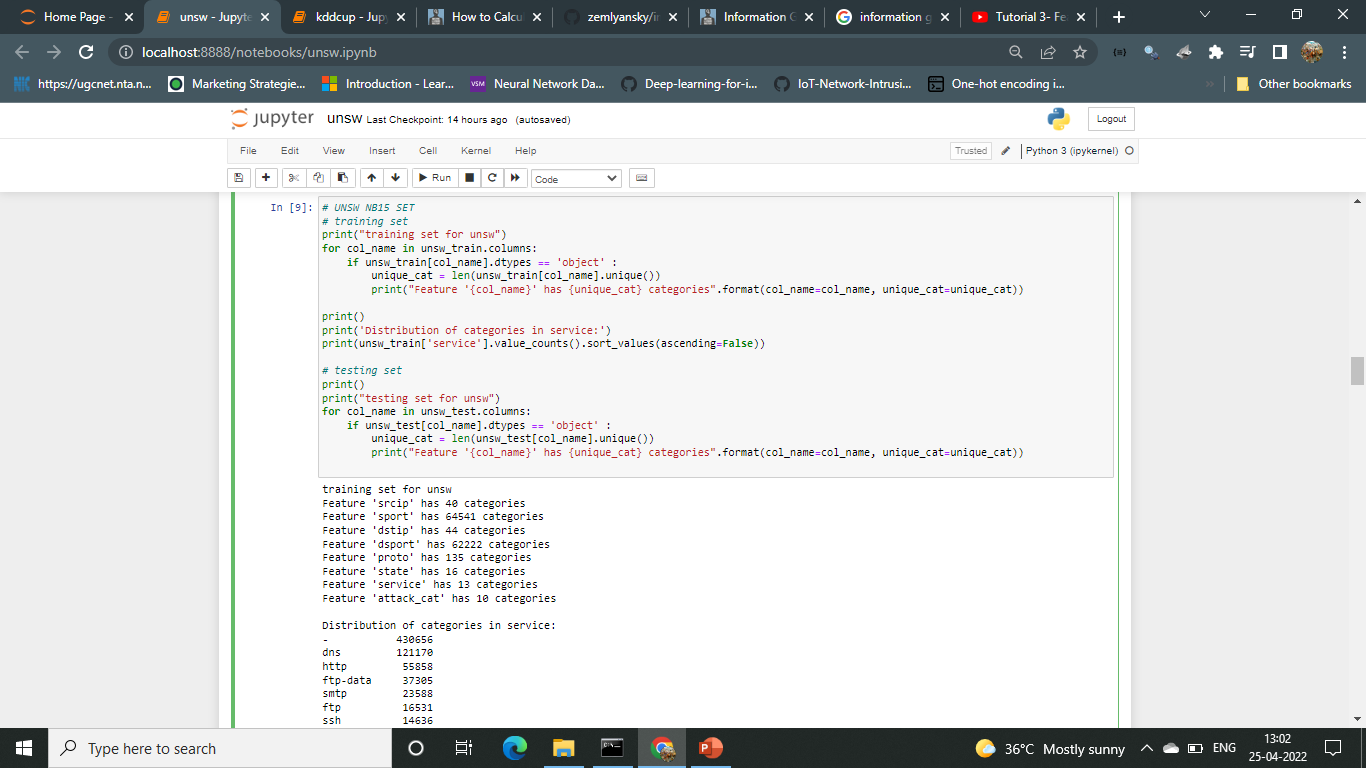
****

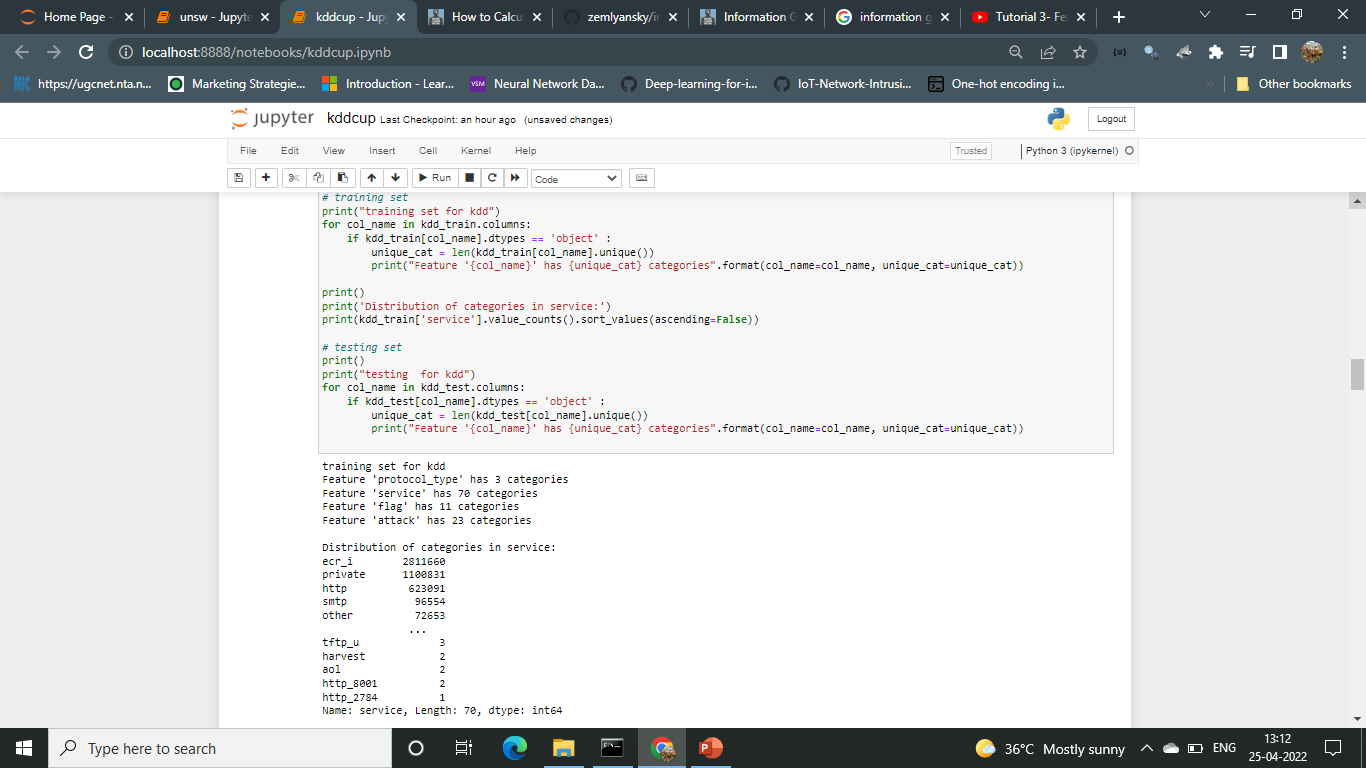
Checking for null values and replacing:





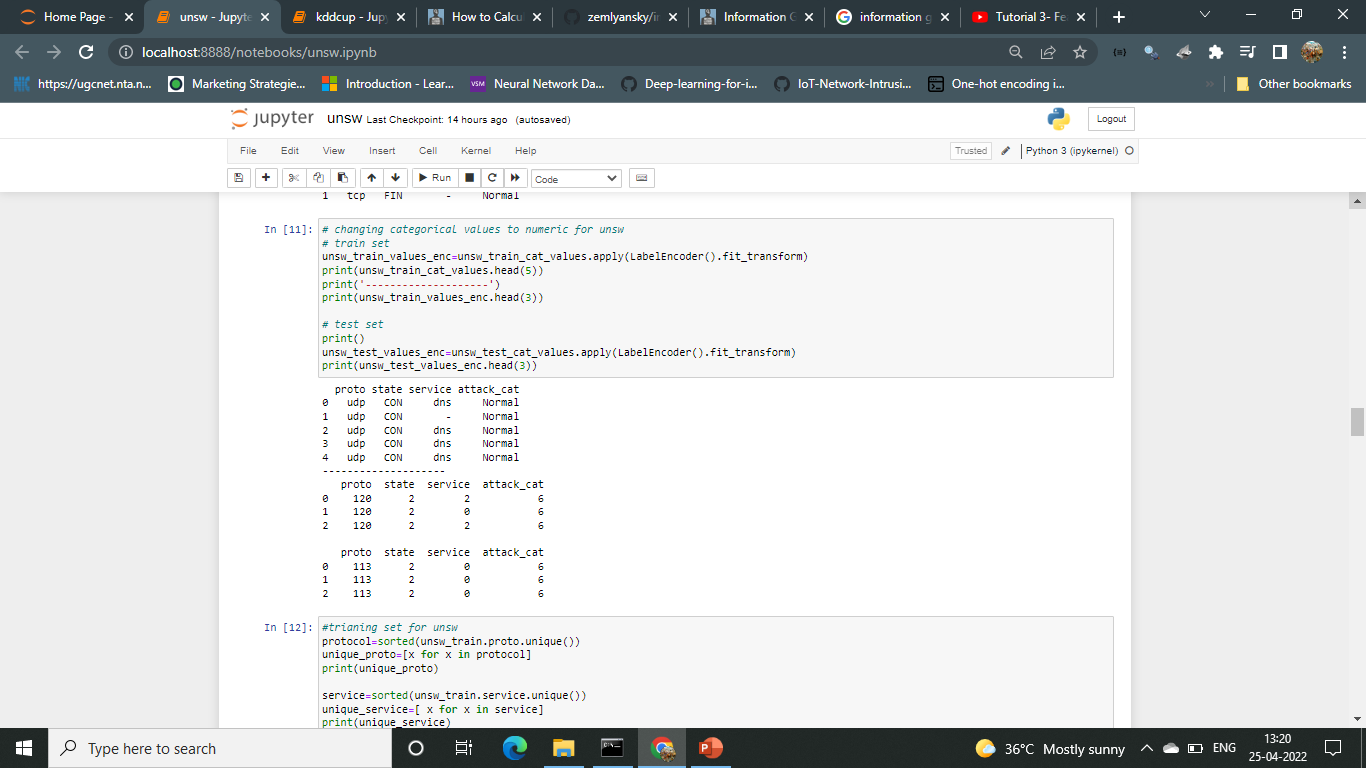
Identify Unique feature category for UNSW AND KDDCUP 99:



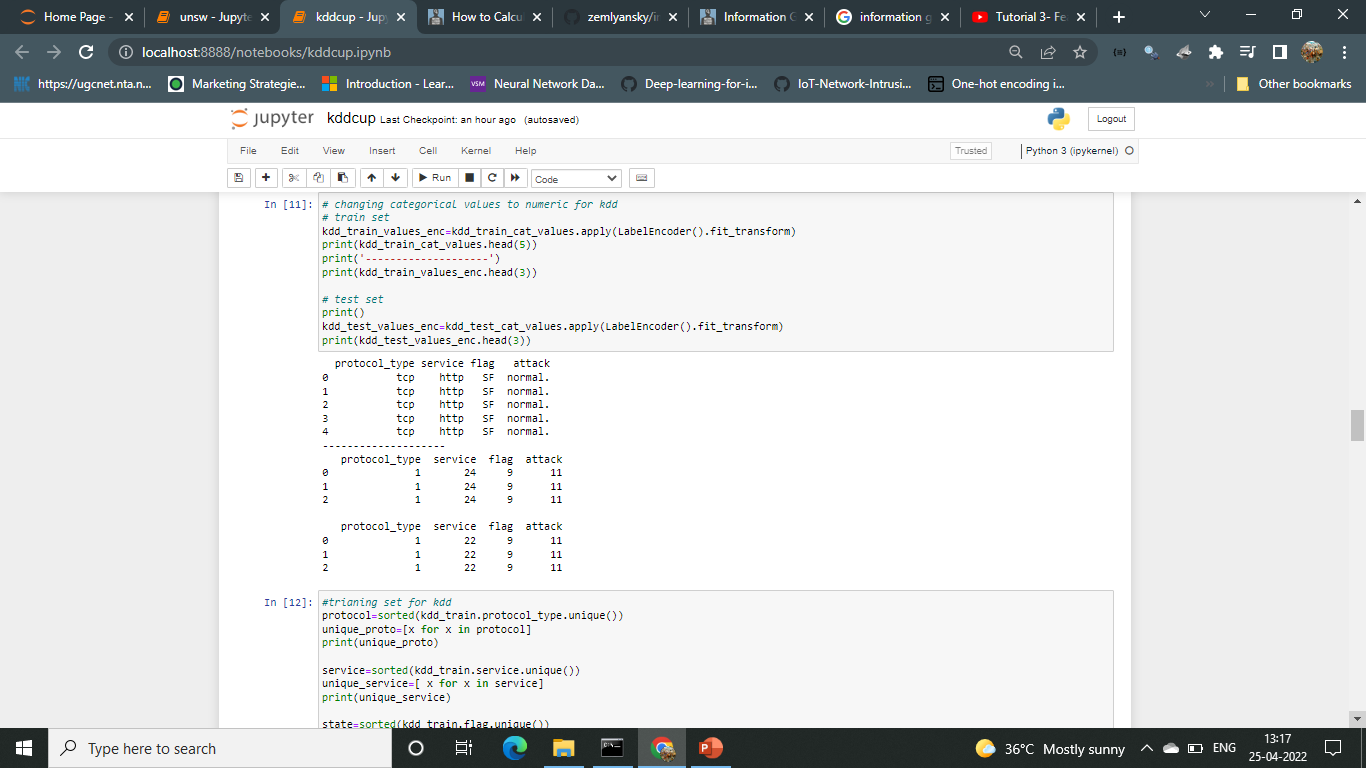
****

Convert to numeric values:

UNSW-NB15:

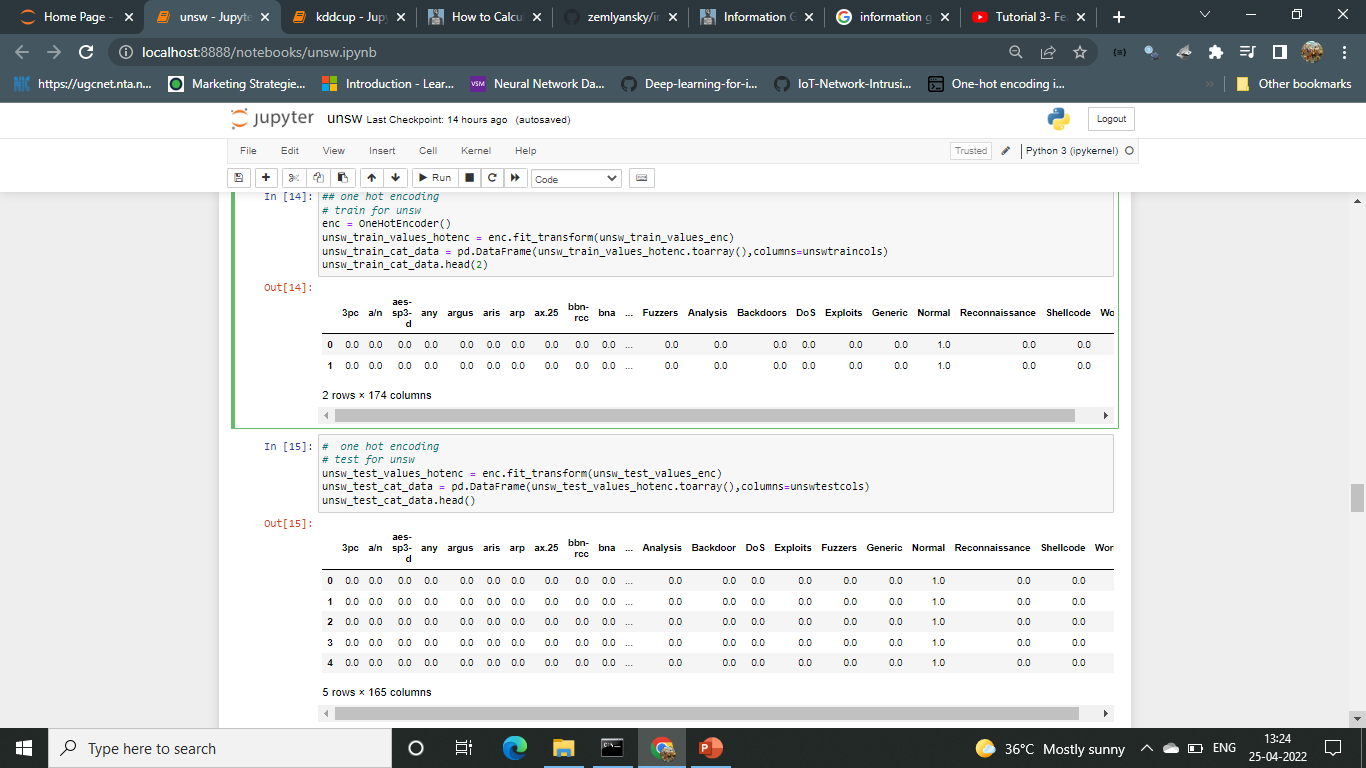


KDDCUP 99:

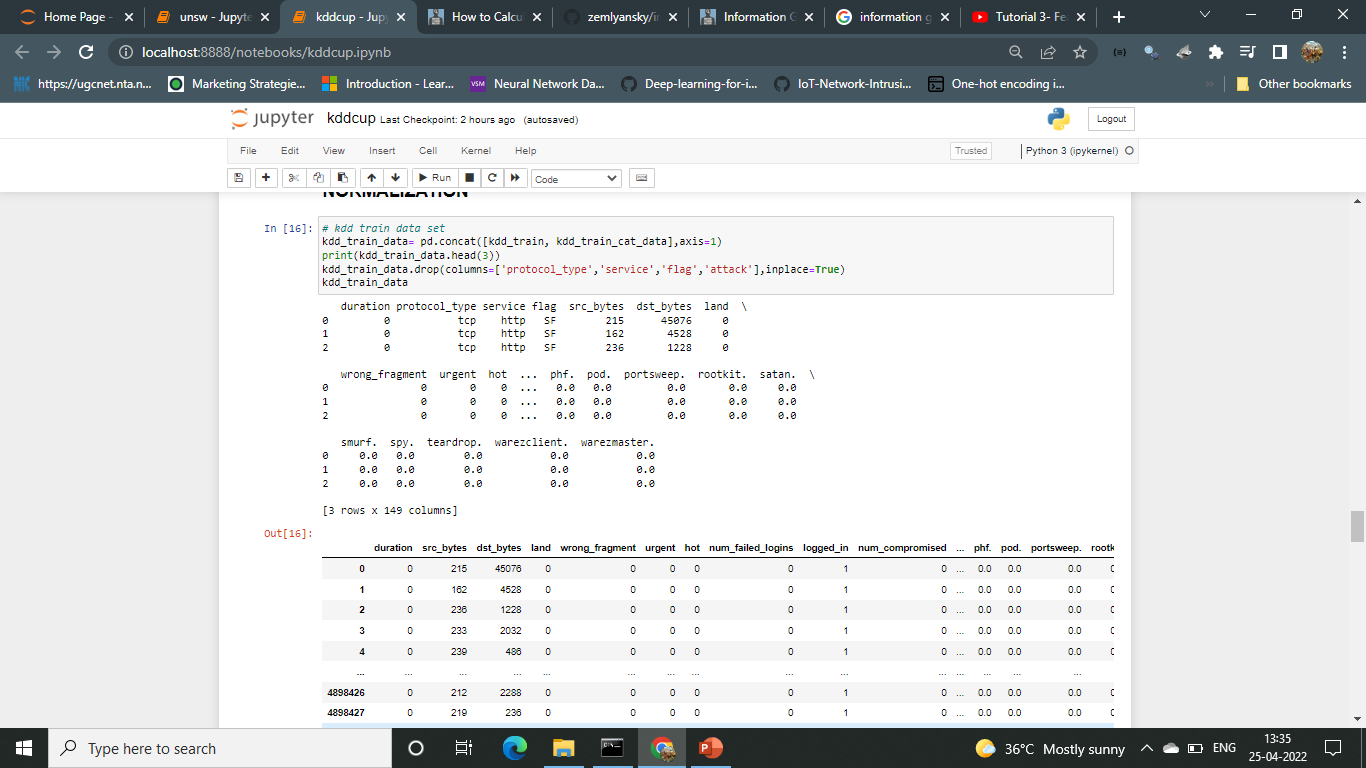
****

**ONE HOT ENCODING:**

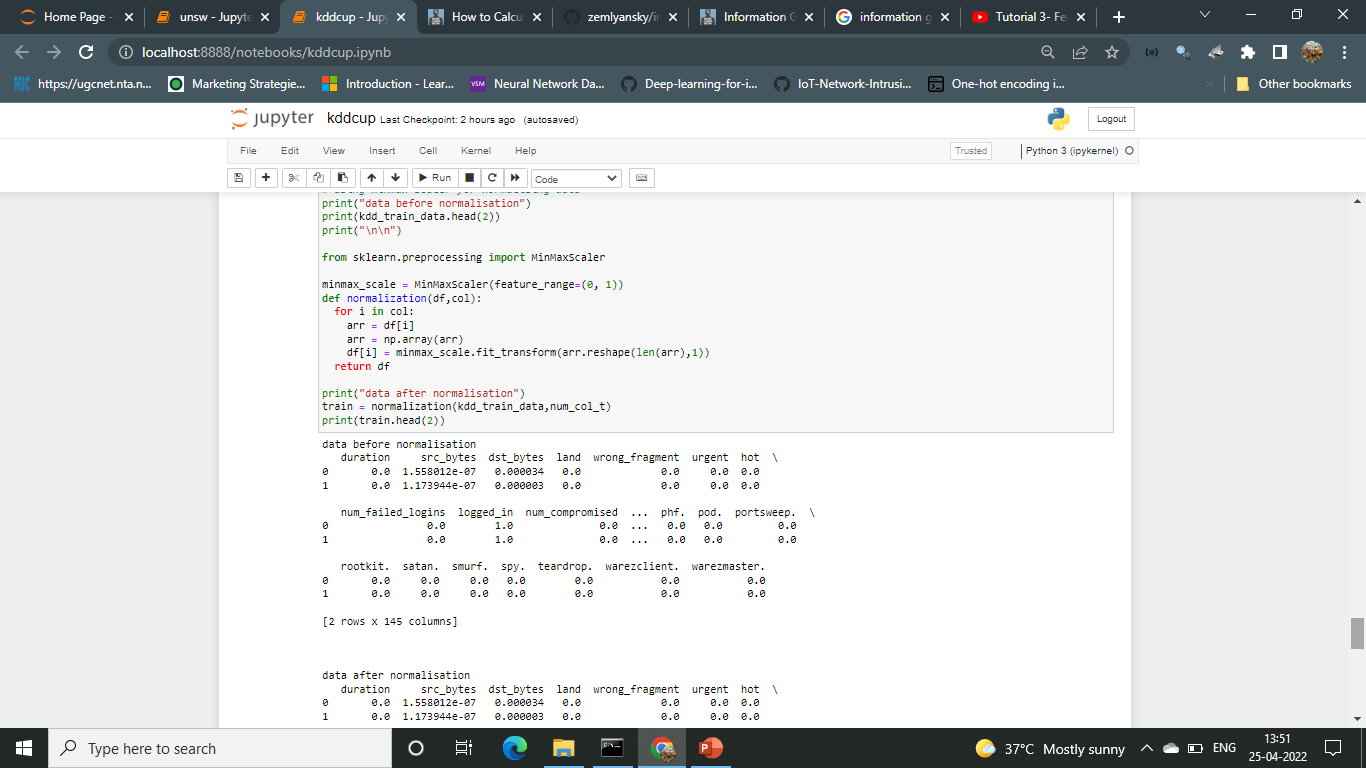
UNSW-NB15

****

KDDCUP 99:



**NORMALIZATION:**



**CHAPTER 6: CONCLUSION**

In this project, I have pre-processed the data set using min-max techniques and one-hot encoding. The next phase will of the project will include information gain and feature selection using PCA (Principal Component Analysis) and training and testing the classification algorithm and finding the category of attack.

**CHAPTER 7: REFERENCE**

1. DeepADV: A Deep Neural Network Framework for Anomaly Detection in VANETs, Tejasvi Alladi,Bhavya Gera, Ayush Agrawal, Vinay Chamola and Fei Richard Yu , IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 70, NO. 11, NOVEMBER 2021
2. DeepVCM: a Deep Learning Based Intrusion Detection Method in VANET, Yi Zeng, Meikang Qiu, Dan Zhu, Zhihao Xue, Jian Xiong, and Meiqin Liu, IEEE Intl Conference on Intelligent Data and Security (IDS).
3. Deep Learning Approach for Intelligent Intrusion Detection System, R. Vinayakumar, Mamoun Alazab, K. P. Soman , Prabaharan Poornachandran , Ameer Al-nemrat , And Sitalakshmi Venkatraman, IEEE Access ( Volume: 7)
4. Deep Neural Networks for Securing IoT Enabled Vehicular Ad-Hoc Networks, Tejasvi Alladi, Ayush Agrawal , Bhavya Gera, Vinay Chamola, Biplab Sikdar, Mohsen Guizani, CC 2021 - IEEE International Conference on Communications.
5. https://www.educative.io/edpresso/one-hot-encoding-in-python
6. https://machinelearningmastery.com/start-here/
7. https://github.com/alik604/cyber-security/blob/master/Intrusion-Detection/UNSW\_NB15.ipynb
8. https://www.youtube.com/watch?v=Fw5iiyIHzew
9. https://github.com/Ahamasaleh/Deep-learning-for-intrusion-detection-using-RecurrentneuralnetworkRNN/blob/main/KDDTest%2BBinary\_Classification.ipynb
10. https://github.com/abhinav-bhardwaj/IoT-Network-Intrusion-Detection-System-UNSW-NB15/blob/master/UNSW\_Project.ipynb