VISVESVARAYA TECHNOLOGICAL UNIVERSITY

"Jnana Sangama", Belagavi-590018

A

Project Work Phase - II Report

On

"DEEP LEARNING FRAMEWORK TO DETECT CYBER ATTACKS IN IoT NETWORK"

SUBMITTED IN PARTIAL FULFILLMENT FOR THE AWARD OF DEGREE OF

BACHELOR OF ENGINEERING

IN

COMPUTER SCIENCE AND ENGINEERING

SUBMITTED BY

NISCHITHA B	(1JB20CS073)
PALLAVI R	(1JB20CS076)
PREETHI V	(1JB20CS084)
RAKSHITH N MAGI	(1JB20CS092)

Under the Guidance of

Mrs. MANJULA H S

Assistant professor

Dept. of CSE, SJBIT

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

SJB INSTITUTE OF TECHNOLOGY

No.67, BGS Health & Education City, Dr.Vishnuvardhan Rd, Kengeri, Bengaluru, Karnataka 560060

2023 – 2024

|| Jai Sri Gurudev ||
Sri Adichunchanagiri Shikshana Trust ®

SJB INSTITUTE OF TECHNOLOGY

No.67, BGS Health & Education City, Dr.Vishnuvardhan Rd, Kengeri, Bengaluru, Karnataka 560060

Department of Computer Science and Engineering

CERTIFICATE

Certified that the Project Work Phase - II entitled "**DEEP LEARNING FRAMEWORK TO DETECT CYBER ATTACKS IN IoT NETWORK**" carried out by Ms. **Nischitha B** ,Ms. **Pallavi R** ,Ms. **Preethi V** ,Mr. **Rakshith N Magi** bearing USN [1JB20CS073], [1JB20CS076], [1JB20CS084], [1JB20CS092] are bonafide students of **SJB Institute of Technology** in partial fulfilment for 8th semester of **BACHELOR OF ENGINEERING** in **COMPUTER SCIENCE AND ENGINEERING** of the **Visvesvaraya Technological University**, **Belagavi** during the academic year **2023-24.** It is certified that all corrections/suggestions indicated for Internal Assessment have been incorporated in the Report deposited in the Departmental library. The project report has been approved as it satisfies the academic requirements in respect of Project work phase-II prescribed for the said Degree.

28/5/24		25/5/
Signature of Guide	**Signature of HOD**	**Signature of Principal**
Mrs. Manjula H S	**Dr. Krishna A N**	**Dr. K. V. Mahendra Prashanth**
Assistant Professor	**Professor & Head**	**Principal, SJBIT**
Dept. of CSE, SJBIT	**Dept. of CSE, SJBIT**	

Principal
SJB Institute of Technology
67, BGS Health & Education City,
Dr. Vishnuvardhan Road,
Kengeri, Bengaluru - 560 060.

EXTERNAL VIVA

Name Of The Examiners	**Signature with date**
1. Dr. Pavithra G S	28/5/24
2. Dr. Bindiya M K	28/5/24

ACKNOWLEDGEMENT

We would like to express our profound grateful to His Divine Soul **Jagadguru Padmabhushan Sri Sri Sri Dr. Balagangadharanatha Mahaswamiji** and His Holiness **Jagadguru Sri Sri Sri Dr. Nirmalanandanatha Mahaswamiji** for providing us an opportunity to complete our academics in this esteemed institution.

We would also like to express our profound thanks to **Revered Sri Sri Dr. Prakashnath Swamiji**, Managing Director, SJB Institute of Technology, for his continuous support in providing amenities to carry out this Project Phase - II in this admired institution.

We express our gratitude to **Dr. K.V. Mahendra Prashanth,** Principal, SJB Institute of Technology, for providing us an excellent facilities and academic ambience; which have helped us in satisfactory completion of Project Phase - II work.

We extend our sincere thanks to **Dr. Krishna A N,** Head of the Dept, CSE for providing us an invaluable support throughout the period of our Project Phase – II work.

We wish to express our heartfelt gratitude to our guide **Mrs. Manjula H S,** Assistant Professor, Dept. of CSE for her valuable guidance, suggestions and cheerful encouragement during the entire period of our Project Phase - II work.

We express our truthful thanks to **Dr. Roopa M J**, Associate Professor, Project Coordinator, Department of CSE, for her valuable support.

Finally, we take this opportunity to extend our earnest gratitude and respect to our parents, Teaching & Non teaching staffs of the department, the library staff and all our friends, who have directly or indirectly supported us during the period of our Project Phase - II work.

Regards,

Nischitha B	(1JB20CS073)
Pallavi R	(1JB20CS076)
Preethi V	(1JB20CS084)
Rakshith N Magi	(1JB20CS092)

ABSTRACT

The internet of things, or IoT,is a network of interrelated devices that connect and exchange data with other IoT devices and the cloud.These devices represent a vast attack surface for cyberattacks. For example, these IoT devices can be infected with botnets to enable Distributed Denial of Service (DDoS) attacks. Signature-based intrusion detection systems are traditional countermeasures for such attacks and these are very time consuming and may not exhaust all the attacks.

The problems with traditional methods for detecting computer network attacks, like viruses and malicious activities are discussed. These methods often make mistakes, miss threats, and struggle to adapt to new types of attacks. To solve these issues, the paper suggests a new approach using deep learning, a type of advanced technology that can learn and understand patterns. This new method focuses on telling if something is a threat or not, rather than trying to categorize it in a specific way.

The paper describes using a special type of deep learning called a "generative adversarial network" to find and stop cyber threats in networks connected to the Internet of Things (IoT). The results showed a significant improvement in accuracy, reliability, and efficiency, reaching higher accuracy in detecting various types of attacks. This research could help make computer networks safer from cyber threats. There are many problems to solve, and adapting deep learning methods for effective attack detection is quite tricky. The deep learning approaches help simplify things by reducing the complexity of patterns and features, which makes it easier to detect cyber threats. The study uses deep learning techniques for identifying and discriminating against cyber-attack malware.

With the increase in the Iot devices being connected to the internet the chances of the cyberattacks have increased .Hence the KDD network dataset was used to train the models to detect and classify the attacks with high accuracy.

TABLE OF CONTENTS

LIST OF FIGURES

Chapter 1

INTRODUCTION

1.1 Overview

The Internet of Things (IoT) refers to a network of devices being connected through internet and the effective communication between the devices can be shown and analyzed. They form several networks that exchanged information between the various devices. This includes devices such as actuators, sensors. The IoT applications have found its use in the domains such as health care, education, home automation, smart phone application, etc. [1] IoT applications have 3 layers , namely perception layer, network layer and application layer. In the perception layer it uses sensors to detect the nearby applications or devices and collects large amounts of data. In the network layer , the data collected from the perception layer is to be analyzed and stored accordingly, this is done in this layer. And the last layer is the application layer, in this layer the user is allowed to communicate with the IoT devices. For example, they can interact with the device in case of any emergency in the health care systems where the sirens starts to ring upon any emergency.[2] In the IoT layers ,each of the layers are exposed to severe risks. In home applications several attacks such as DDoS attack, sensor attack and Router attacks are detected.[3] With the connection of IoT devices to the internet it has lead to the exposure of data to the attackers providing an attack surface, this leads to loss of data and threat to the data. The increase in the use of IoT devices the protection of the information is a must and most essential feature to be taken care off. The use of IoT device has shown a progress towards the increase in the IoT manufacturing industries.[4] Attacks such as Denial of Service attacks are detected on most of the IoT devices. Signature based Intrusion Detection Systems are mostly exposed to such attacks and there must be some way to detect such attacks. [5] IoT systems have been benefitting people in several ways; however ,it also poses several weakness. Security is the challenging aspect of the IoT networks. And they cannot be prevented from threats. Different communication protocols can introduce additional complexity when implementing an IoT framework. The Man-In -the middle attacks are all threats applied to the every scenario of cyber attacks.[6] The rise in the malicious threats requires efficient security and protection. The Intrusion detection systems were hence used and have gained reactive network security. These IDS aim to evaluate the different network data to ensure its security is maintained. Several security approaches are taken up to protect the devices and data from the intruders. Anomaly detection systems methods were used and the types of attacks are identified. [7] A large number of critical vulnerabilities on IoT networks are also a threat. Common cyber-attacks involve DDoS (Distributed Denial of Service), ransomware, and botnet attacks, which seek to exploit IoT networks and destroy their computational capabilities. The volume of data produced by these devices increases exponentially and can contain confidential information. [8]

Attacks such as DDoS and other hacking techniques are commonly used .The attackers intend to target the IoT networks with malicious behaviour. The protection of systems are more better than the past. The CNNs were used for anomaly detection and the multiclass classifiers were categorized into 15 types of attacks, and significant contributions are made; A strategy for creating a new dataset from the existing one.

The most common attacks identified are polymorphic attacks which is said to maintain a low false positive rate. Attacks in smart health systems are found that it has the following attacks Denial of Service Attack (DoS), Fingerprint and Timing based Snooping (FATS), Router Attack, Select Forwarding (SF) Attack, Sensor Attack and Replay Attack. In general, the perception layer can suffer from attacks such as malicious code injection, eavesdropping and interference. This can be overcome by using some Machine learning techniques.

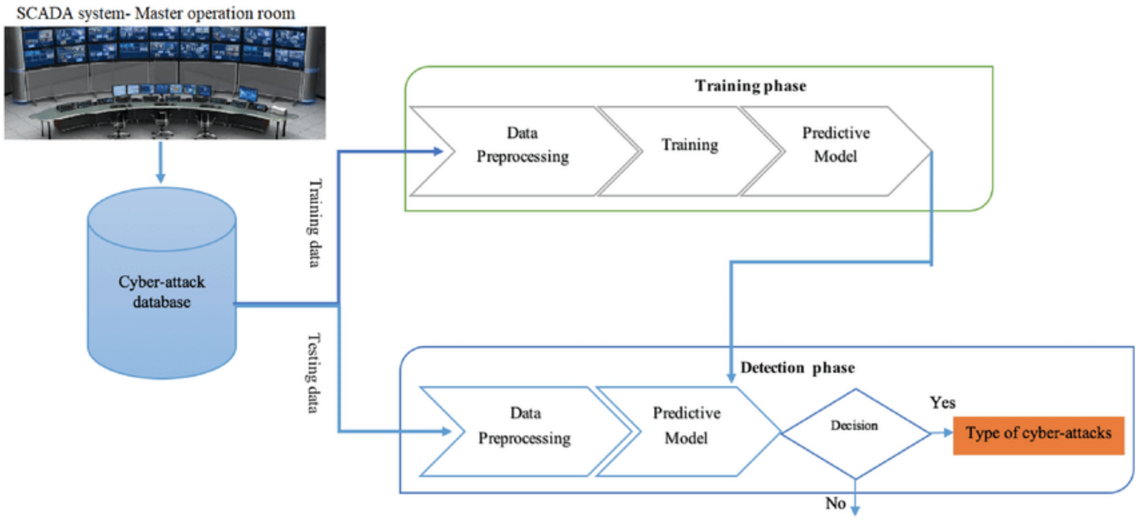


Fig 1.1 CAD Architecture

In this project a novel approach to resolve the problems of existing network intrusion detection and defense technologies. It is based on deep learning techniques, but it can be differentiated from other deep learning-based approaches in the following aspects.

This project used the KDD network intrusion data set to explore the use of generative deep learning techniques that can automatically detect and classify IoT cyber attacks. The primary contribution of this paper is that it used the complete KDD network intrusion dataset for building an IDS and achieved state-of-the-art result in anomaly detection.

Use of advanced artificial intelligence algorithms such as CNN, LSTM, and a hybrid CNN-LSTM to develop a system to detect intrusions into the IoT environment. The proposed system was developed using IoT network data that are not commonly used; this dataset was generated in 2020 and was the biggest challenge for developing a robust framework. The proposed system was compared with a research article that developed these data. It was noted that the results of our system were outperformed.

1.2 Challenges

- IoT is vulnerable to security risks at every architectural layer and has faced security challenges since its emergence.
- Many IoT devices have constrained resources(CPU,memory,power),making it difficult to implement sophisticated security measures.
- The large number of interconnected devices in IoT increases the attack surface.Detecting anamolies or malicious activities across complex networks requires advanced methods to identify potential threats.
- Many IoT devices are deployed in physically accessible locations,making them susceptible to physical tampering.Attackers with physical access can compromise the devices directly.

1.3 Motivation

In June 2021,a hacker by the name of “God User” stole information on 700 million LinkedIn users.Although no financial or private messaging data was hacked,user’s email addresses,names,phone numbers and other information was hacked.Even though identity theft has been cracked down in recent years,it is still affecting lots of citizens.To avoid the security breaches we have motivated to choose this topic.

1.4 Objectives

- To implement an efficient network intrusion detection system.
- To implement a multi–class classification to identify different types of attacks.
- To design an intelligent intrusion detection and prevention system.

- To compare various ML algorithms to detect intrusion detection system.

1.5 Benefits

By implementing this project we can get following benefits.

- Automatic detection of anomaly in IOT networks .
- Comparing to current technology this project saves time of anomaly detection system.
- Comparing to current mechanism this project gives high accuracy in anomaly detection.

1.6 Applications

- Society
- Education
- Network Security

Chapter 2

LITERATURE SURVEY

Shire *et.al.*, in [38] utilised a convolutional neural network(CNN) to detect Man in the middle attack in Simoes dataset and provided an IoT environments a malware Intrusion Detection System.A socket python library was adopted to capture overall network traffic and then this stored network traffic is converted into an image using Binvis tool [39]. At last malware is identified by inserting an image into CNN. Basically, this CNN is constructed using Tensorflow and MobileNet module. The anomaly-based IDS suffer from a high number of False Positives.

Seo *et.al.*, in [41] identified a method called DL-based detection method to detect Ping Distributed DoS (DDoS) attacks in Modbus/TCP network flows dataset. This method steals energy by recognising FDI attacks against SCADA systems. This proposed method is composed of State vector estimation (SVE),Deep-Learning based identification(DLBI).IEEE 118-bus power test system and an IEEE 300-bus system was used to demonstrate the resiliency of the proposed method. The detection results are compared with outcomes of these ML solutions to validate the efficiency of the proposed method.

Saharkhizan *et.al.*, in [42], provided several mechanisms for intrusion detection for Modbus IoT environments. This mechanism aggregates multiple Long-Short-Term-Memory (LSTM) networks, which is a type of recurrent Neural Networks (RNNs).Further Simoes [43] is a dataset that has four categories of cyberattacks namely (a) Man In The Middle (MITM) attacks, (b) Ping Distributed DoS (DDoS) attacks, (c) TCP SYN DoS attacks and (d) Modbus query flood attacks. Decision tree is used to compare output of LSTM networks to classify network flows into above mentioned categories of attacks.This mechanism is said to achieve 99% accuracy based on the evaluation results.

Industrial Control systems (ICSs) focus on safety, where each system is safeguarded and if anything goes wrong, then the system stops. These systems are placed in an isolated environment. There are two types of Intrusion Detection Systems called Signature-based and Learning-based techniques.Signature-based systems are used to detect known attacks and are inefficient in detecting unknown or new attacks [19]. On the other hand learning-based systems are used to identify unexpected intrusions. To develop IDS, a Nonsymmetric Deep Autoencoder (NDAE) was applied by authors in another study [33].In reference [38] data was collected from a Secure Water Treatment (SWaT) testbed and anamolies were detected through the application of unsupervised machine learning algorithms like DNN and SVM.DNN results in less false positives than SVM, while SVM detects more anamolies than DNN.

Sohal *et.al*., [6] identified routers, switches and hubs as different network devices of Fog computing. In order to identify edge devices in Fog environment, Virtual Honeypot Devices together with Markov models were presented by authors. In order to identify attacks at the right time, four ML classifiers were employed that can automatically detect attacks. Pacheco and Hariri in [11] presented an approach to develop a threat modeling methodology to recognize vulnerabilities in each of the four layers in IoT device architecture: devices, network, services and applications, and present counter measures to mitigate each of the vulnerabilities.

Kaur *et.al*., [8] analysed models via CICIDS2017 and CICIDS2018 datasets which provides multiclass attack classification and uses a CNN model to identify and describe several attacks, but the rate of detection of attacks was not satisfactory. Ferrag *et.al*., [9] used 35 well-known datasets to compare seven deep learning models and classify them into seven separate categories. They conducted binary and multiclass classification and checked their strategies on BoT-IoT and CICIDS2018 datasets. The authors investigated several attack methods to evaluate the effectiveness across different deep learning models. These models were evaluated using their false alarm rates, accuracy, and detection rates.

A recently published research [16] has 34 datasets and 15 features for each of Intrusion Detection datasets. There are three types of datasets namely packet-level data, network packet data and accessible datasets. The features are divided into five categories: (1) well-known data, (2) assessment, (3) recording environment, (4) recording volume, (5) recording type.

Goodfellow *et.al*., in 2014 [26] invented GAN which is one of the most powerful tool in deep learning. Some authors used GAN to detect attacks while some used to make system robust. Chhetri *et.al*., [28] analysed the relation between cyber and physical domains in a CPS to observe security issues by proposing a conditional GAN based model. Huang *et.al*., proposed IDS GAN, which leverages a generator to transform original malicious traffic into adversarial malicious traffic examples [33].

Usama *et.al*., [9] proposed a model to attack the Intrusion Detection System using Adversarial attacks generated by GAN. Their unique model is how they defend the Adversarial Attack through IDS. However, the shortcoming of this model is that the IDS can defend against only the adversarial attacks for which it has been trained. The GAN model was applied to evade Malware Detection in

Kawai *et.al.*, [10]. Their model first creates an API list from multiple cleanware and one malware. By doing this, the proposed GAN model tries to evade malware detection by adding cleanware's feature quantities to the malware. Among the methods they examined, Random Forest and Multi-layer Perceptron provided the best result. The results show that ML-based black-box malware detector was unable to detect most of the adversarial data.

S.n	**AUTHOR**	**METHOD**	**ATTACKS ADDRESSED**	**DATASET**	**RESULT**	**LIMITATION**
1	Shire	Angle-Based Outlier Detection,Principal Component Analysis, Minimum Covariance Determinant,ARIES GAN.	Man In The Middle attacks,Ping Distributed DoS attacks,	Modbus/TCP network flows,DNP3 network flows, operational data	The accuracy of the proposed mechanism reaches 99%.	The anomaly-based IDS suffer from a high number of False Positives
2	Saharkhizan	Modbus IoT environments,RNN Long-Short-Term-Memory,MENSA model.	TCP SYN DoS attacks ,Modbus query flood attacks.	Simoes, CICFlowMeter	Compared to the existing anomaly-based IDS, MENSA addresses efficiently the FP.	Signature-based IDS can detect only known cyberattack patterns and include only a limited set of signature rules
3	Shafi	Virtual Honeypot Devices, Markov models,BlackBox IDS	DoS attack,privacy,eavesdropping,backdoor attacks.	IoT testbed	Detects both known and unknown attacks with high detection rates&low false-positive alerts	A type of threat for fog computing who has gained impor- tance is DDoS attack which illegally appropriates resources of

						fog node
4	Shire	DL-based detection method, State Vector Estimator, DL-Based Identificatio,MENSA	False Data Injection, DoS attacks.	Modbus/TCP,DNP3	MENSA achieves the best performance either for detecting operational anomalies or discriminating the Modbus/TCP and DNP3 cyberattacks	adoption of the security standards is challenging, especially for adjustments that need to be taken place in real-time.
5	Imtiaz Ullah	Transfer learning,RNN,CNN	Replay, Flooding and DoS attacks	BoT-IoT, IoT Network Intrusion, MQTT-IoT-IDS2020,	Proposed binary and multiclass classification models showed high accuracy, precision, recall, and F1 score	A neural network that uses convolution has a possibly over- fitting issue
6	Qusay	multilabel classification method,Transfer learning,Random Forest	DoS,DDoS, Brute Force attack	IoT-23, IoT-DS-1, and IoT-DS-2	An efficient anomaly-based intrusion detection system for IoT networks that has both a high detection rate and a low false alarm rate was developed.	Intruders may carry out various attacks, resulting in issues with the privacy and security of IoT devices.

7	Irfan	DL,Backpropagation method, deep-autoencoder-based LSTM method.	BruteForce XXS, BruteForce WEB, DoS_Hulk_ Attack	NSL-KDD, KDDCup99, UNSW-NB15	identify the internal and external intruder's accurately in real-time	Due to adopted DL methods privacy and security concerns are critical.
8	Fayyaz	Deep-autoencoder-based LSTM, RNN, CNN,DNN	DOS_Gold Eyes_Attack, DoS_SlowLoris_ Attack	CSECIC-IDS2018 and the Bot-IoT datasets	DNNs give outstanding results on the performance metrics of true negative rate with an accuracy of 96.915%.	key issue is data movement, where data is transferred between encrypted forms in training and testing modules.
9	Miguel	Feature scaling,Feature extraction, S-IDS model,GAN	Zero day attack,Probing attack,DoS attack.	NSL KDD'99	Detection rates of most of the classes are improved	Datasets are imbalanced where different types of attack data are not available.

Chapter 3

PROBLEM STATEMENT

The aim of our project is to design a framework to detect cyber-attacks using Deep-Learning models.

3.1 Existing System

Much work has been done in building intrusion detection systems using a variety of machine learning and deep learning models. There was a limit to detecting various network attacks accurately using machine learning or deep learning algorithm in IOT networks. In the existing approach there is to detect attack is there or not which are not able to detect the types of attacks and accuracy is less.

3.2 Proposed System

The rapid growth of Internet of Things (IoT) is expected to add billions of IoT devices connected to the Internet. These devices represent a vast attack surface for cyberattacks. For example, these IoT devices can be infected with botnets to enable Distributed Denial of Service (DDoS) attacks. Signature-based intrusion detection systems are traditional countermeasures for such attacks. However, these methods rely on human experts and are time-consuming in terms of updates and may not exhaust all attack types especially zero-day attacks.

This project shows that it is possible to use generative deep learning methods like CNN-LSTM to detect intruders based on an analysis of the network data. The recently posted KDD dataset was used to train generative deep learning models to detect a variety of attacks like DDoS, and various botnets like Mirai, Okiruk and Torii. Over 1.8 million network flows were used to train the various models. The resulting generative models outperform traditional machine learning techniques like Random Forests. CNN-LSTM-based models were able to achieve an F1-Score of 0.99. In the proposed approach supports to detect different types of attacks and we are using the combination of two algorithms to increase accuracy.

Chapter 4

SYSTEM REQUIREMENTS

System Requirement Specification (SRS) is a central report, which frames the establishment of the product advancement process. It records the necessities of a framework as well as has a depiction of its significant highlight. An SRS is essentially an association's seeing (in composing) of a client or potential customer's frame work necessities and conditions at a specific point in time (generally) before any genuine configuration or improvement work. It's a two-way protection approach that guarantees that both the customer and the association comprehend alternate's necessities from that viewpoint at a given point in time.

The SRS talks about the item however not the venture that created it, consequently the SRS serves as a premise for later improvement of the completed item. The SRS may need to be changed, however it does give an establishment to proceed with creation assessment. In straightforward words, programming necessity determination is the beginning stage of the product improvement action.

The SRS means deciphering the thoughts in the brains of the customers – the information, into a formal archive – the yield of the prerequisite stage. Subsequently the yield of the stage is a situated of formally determined necessities, which ideally are finished and steady, while the data has none of these properties.

4.1 Functional Requirements

This section describes the functional requirements of the system for those requirements which are expressed in the natural language style.

1. Create a web application using flask framework which contains user.
2. User load dataset.
3. System will read ,preprocess and extract the features from the dataset.
4. System will use Deep Learning model to train
5. System will detects the attacks in network using Deep learning Model.

4.2 Non Functional Requirements

These are requirements that are not functional in nature, that is, these are constraints within which the system must work.

- The program must be self-contained so that it can easily be moved from one Computer to another. It is assumed that network connection will be available on the computer on which the program resides.
- **Capacity, scalability and availability.**

The system shall achieve 100 per cent availability at all times.The system shall be scalable to support additional clients and volunteers.

- **Maintainability.**

  The system should be optimized for supportability, or ease of maintenance as far as possible. This may be achieved through the use documentation of coding standards, naming conventions, class libraries and abstraction.

- **Randomness, verifiability and load balancing.**

  The system should be optimized for supportability, or ease of maintenance as far as possible. This may be achieved through the use documentation of coding standards, naming conventions, class libraries and abstraction. It should have randomness to check the nodes and should be load balanced.

4.3 HARDWARE REQUIREMENTS

• Processor Type	: Intel Core$^{\text{TM}-}$ i5
• Speed	: 2.4 GHZ
• RAM	:8 GB RAM
• Hard disk	: 80 GB HDD

4.3.1 CPU- INTEL CORE i5

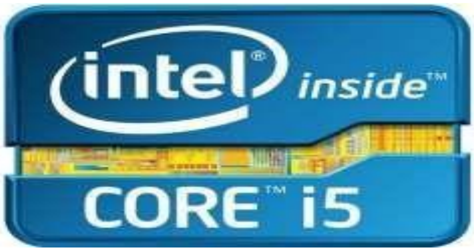


Fig 4.1 INTEL CORE i5

Intel Core is a brand name that Intel uses for various mid-range to high-end consumer and business microprocessors. As of 2015 the current line up of Core processors included the Intel Core i7, Intel Core i5, and Intel Core i3. 5th generation Intel® Core™ i5 processors empower new innovations like Intel® Real Sense™ technology—bringing you features such as gesture control, 3D capture and edit, and innovative photo and video capabilities to your devices. Enjoy stunning visuals, built-in security, and an automatic burst of speed when you need it with Intel® Turbo Boost Technology 2.0.

4.3.2 RAM

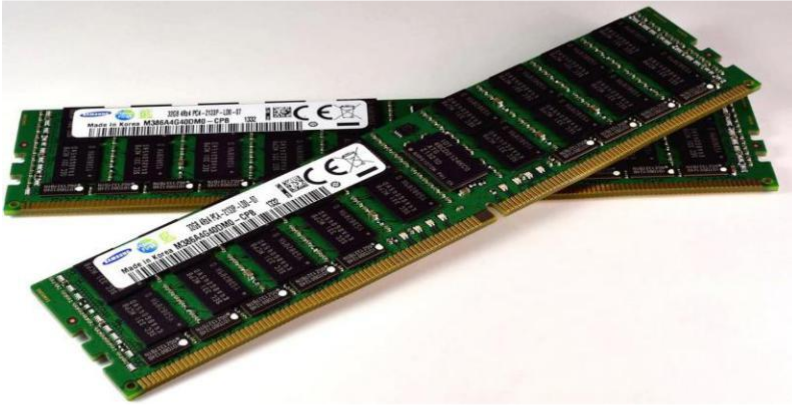


Fig 4.2 RAM 8 GB

When you load up an application on to your computer it loads into your available RAM memory. It is very quick type of memory. The more programs you load up, the more RAM is taken up. At the point where you have loaded up enough apps to take up all your free available physical RAM, your OS will create a swap-file on your hard drive. This file is used as a reserve for all additional apps you run.

The trouble with that is that hard drives are a lot slower to read and write from than RAM memory is. Therefore, your computer will perform much slower at that point. Although new generation of SSD hard drives are much faster than your traditional spinning drive, it is still best to have enough RAM available. If you are using Windows and want to want to know how much RAM you are using up, you can right click on task bar, then select start "Task Manager" and on the "performance" tab you will see a green bar indicating "Memory".

4.3.3 HARD DISK

Fig 4.3 Hard Disk Drive

A hard disk drive (HDD), hard disk, hard drive or fixed disk is a data storage device used for storing and retrieving digital information using one or more rigid ("hard") rapidly rotating disks (platters) coated with magnetic material. The platters are paired with magnetic heads arranged on a moving actuator arm, which read and write data to the platter surfaces. Data is accessed in a random-access manner, meaning that individual blocks of data can be stored or retrieved in any order rather than sequentially.

4.4 SOFTWARE REQUIREMENTS

• Operating System	: Windows 64-bit
• Technology	: Python
• IDE	: PythonIDLE
• Tools	: Anaconda
• Python Version	: Python 3.6

Chapter 5

SYSTEM DESIGN

5.1Data Flow Diagram:

A data flow diagram (DFD) is a graphical representation of the "flow" of data through an information system, modelling its process aspects. A DFD is often used as a preliminary step to create an overview of the system without going into great detail, which can later be elaborated. DFDs can also be used for the visualization of data processing.

Level:0

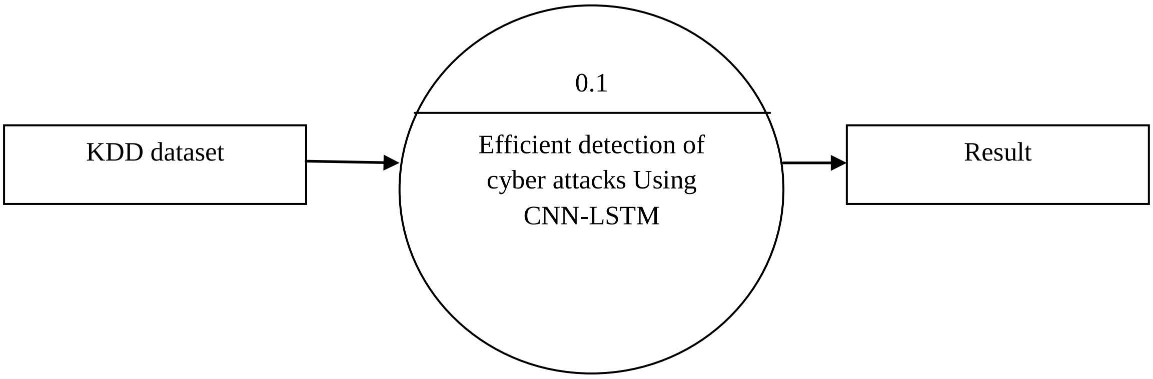


Fig 5.1 DFD-Level-0

Level 0 Describes the overall process of this project. we are passing KDD dataset as a input the system will efficiently process the dataset and apply CNN-LSTM algorithm to detect different types of cyber attacks and shows the performance comparison of those algorithms.

Level: 1

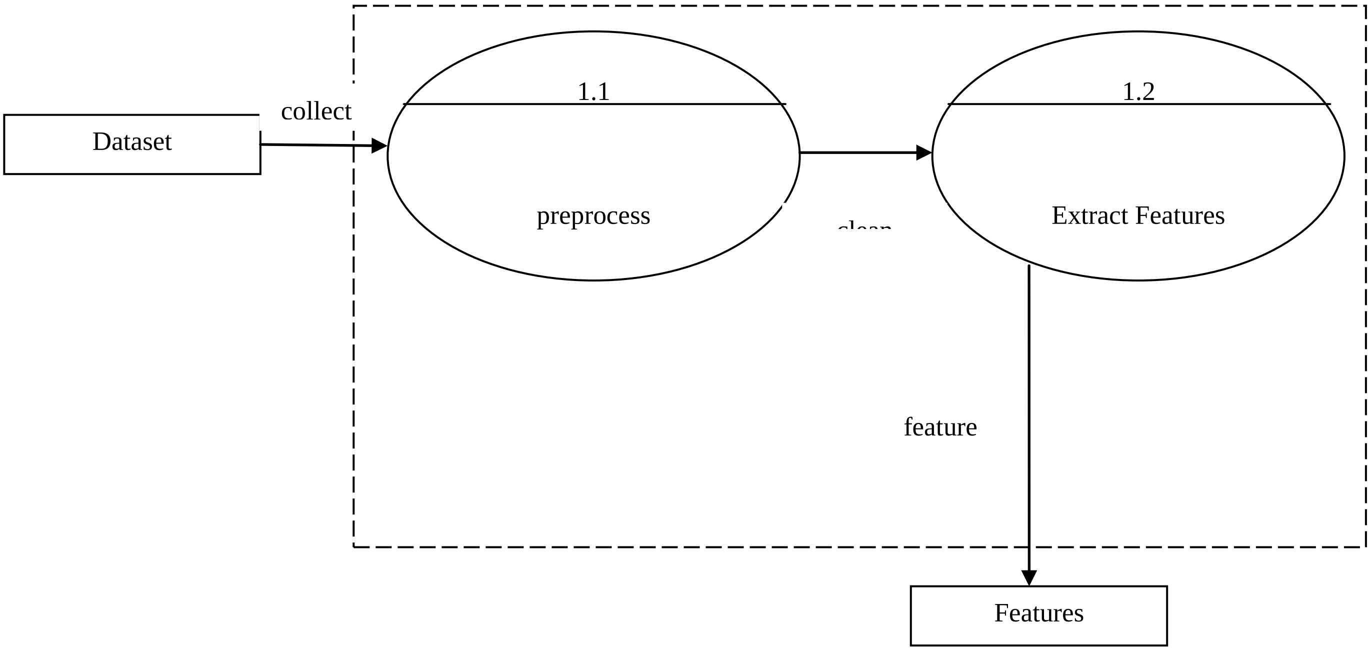


Fig 5.2 DFD-Level-1

Level 1 Describes the first stage process of this project. we are passing KDD network intrusion dataset as input to the system will preprocess and extract the important features using mutual information Correlation classification.

Level 2:

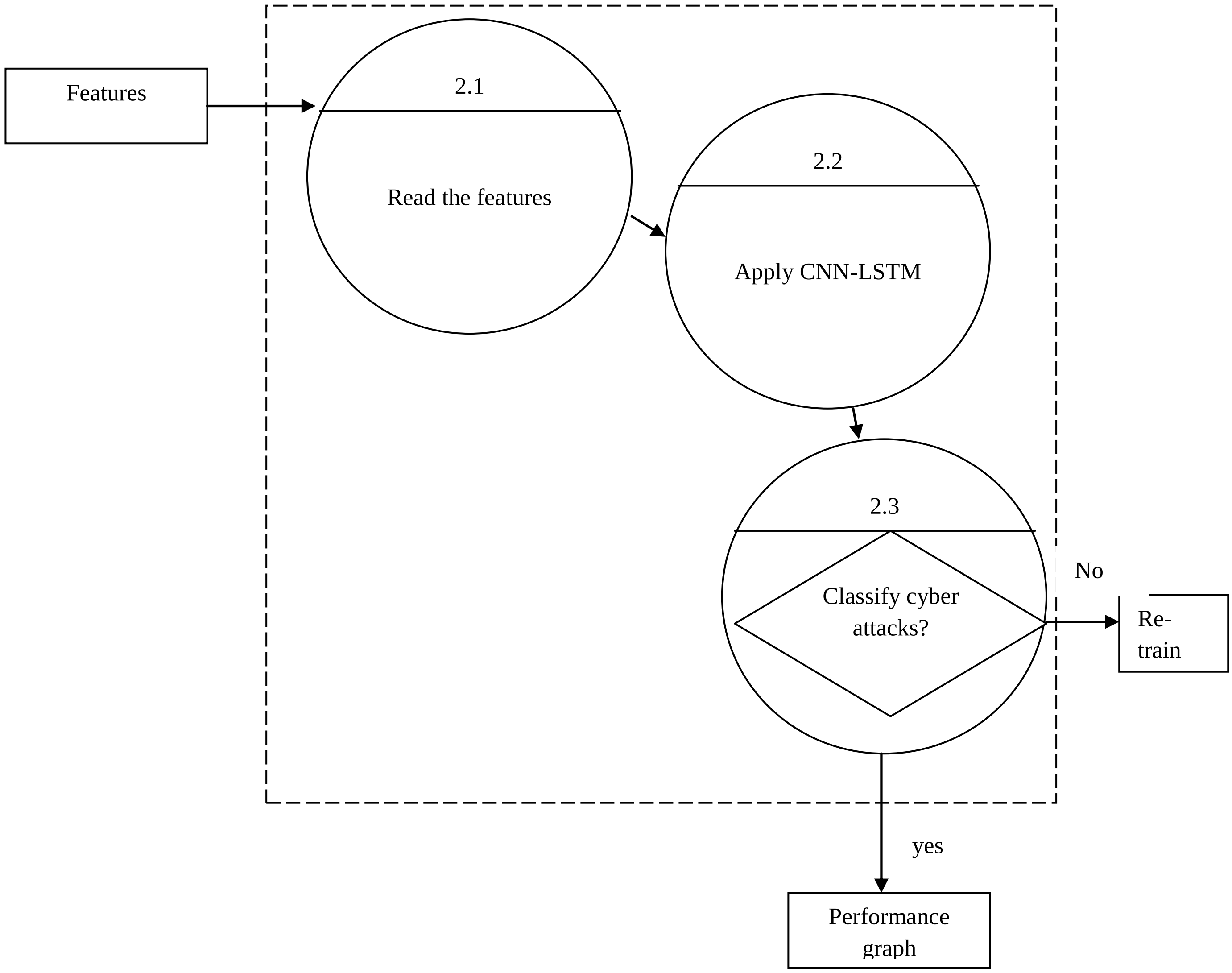


Fig 5.3 DFD-Level-2

Level 2 Describes the final stage process of this project. we are passing extracted features from level-1 by applying CNN-LSTM model system will detect the type of cyber attacks in IOT network.

5.2 Sequence Diagram

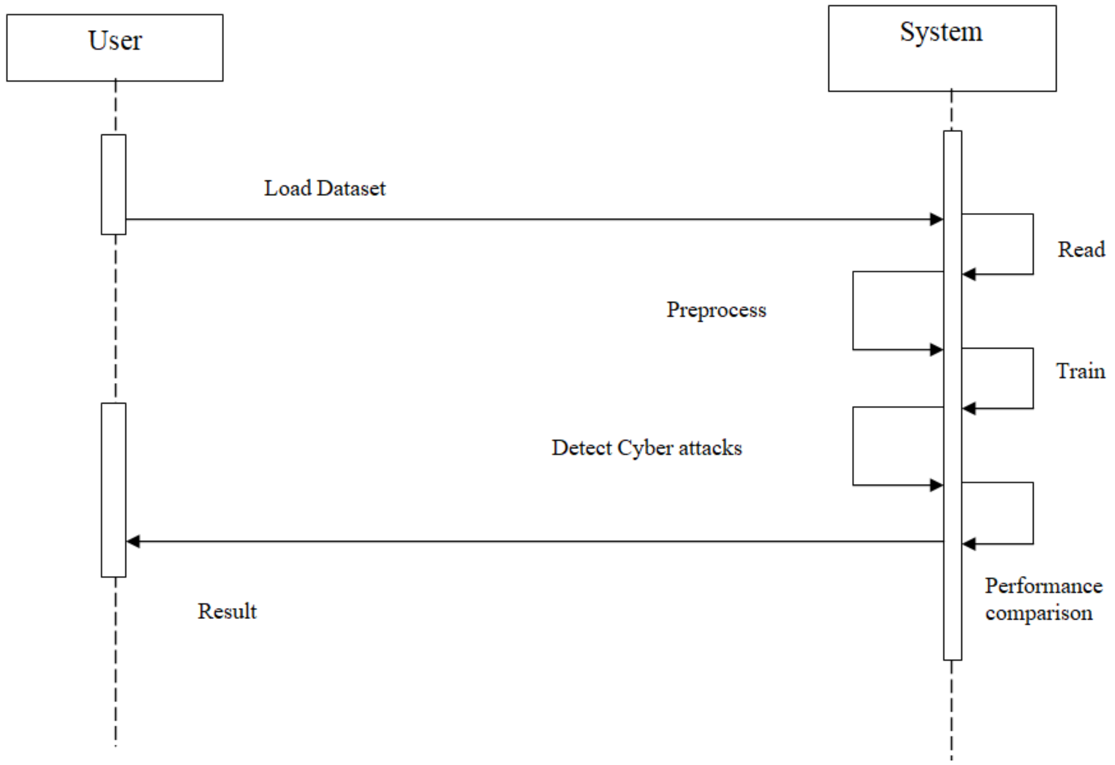


Fig 5.4 Sequence Diagram

Sequence diagram provides the detail about active and inactive states of the user.

Chapter 6

METHODOLOGY

6.1 System Architecture:

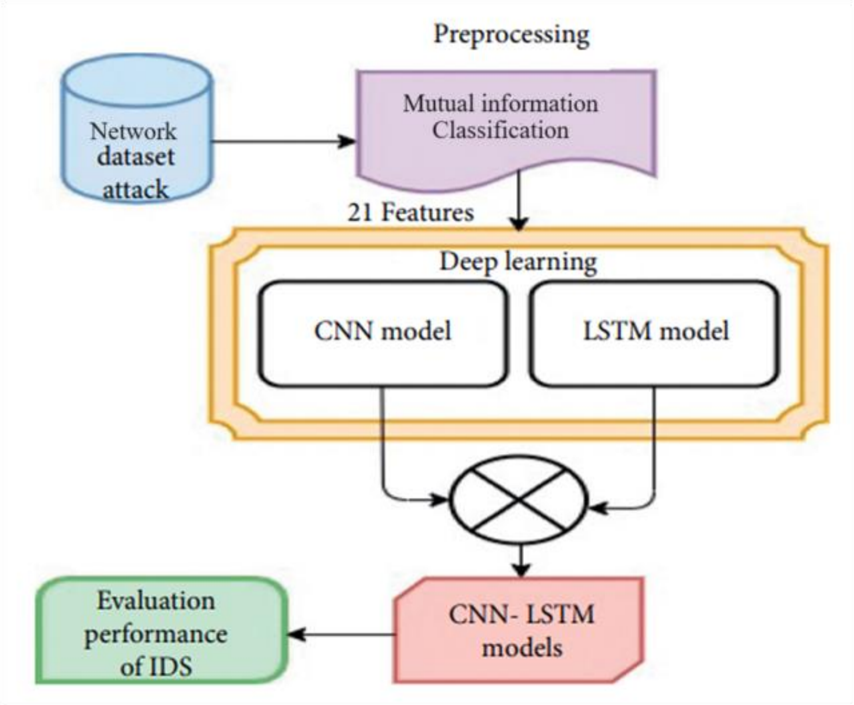


Fig 6.1 System Architecture

The newly developed KDD network intrusion dataset was adopted from csv files available online. The dataset contained 80 features and four main label dos,r2l,u2r and normal. The KDD network intrusion dataset attack was generated in 2020. Figure 5.1 shows the IoT environment of the generated KDD network intrusion dataset.

6.2 Modules:

In this system is used to detect and prevent the intrusion in network, this project is divided into following modules.

1. Collecting Dataset
2. Preprocess

3. Feature Selection Using Mutual information classification

4. Building Model

5. Performance Evaluation

6.3 Modular Description:

6.3.1. Collecting Dataset:

This data is based on the network traffic obtained from Internet of Things (IoT) devices with 20 malware and 3 benign captures. KDD network intrusion data set. We have collected from the UCI machine learning repository.

6.3.2. Data Pre-Processing

When the dataset is extracted, part of the data contains some noisy data, duplicate values, missing values, infinity values, etc. due to extraction errors or input errors. Therefore, we first perform data preprocessing. The main work is as follows.

(1) Duplicate values: delete the sample's duplicate value, only keep one valid data.

(2) Outliers: in the sample data, the sample size of missing values(Not a Number, NaN) and Infinite values(Inf) is small, so we delete this.

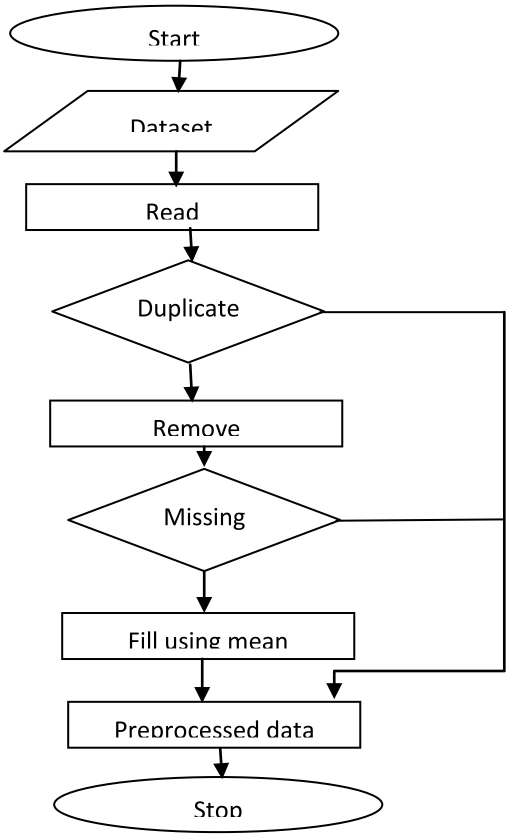
(3) Numerical standardization: In order to eliminate the dimensional influence between indicators and accelerate the gradient descent and model convergence, the data is standardized, that is, the method of obtaining Z-Score, so that the average value of each feature becomes 0 and the standard deviation becomes 1, converted to a standard normal distribution, which is related to the overall sample distribution, and each sample point can have an impact on standardization

Pseudocode:

```
• Procedure preprocess
• Step 1: Read the dataset
• Step 2: for all records in dataset
        o Find nan values
        o If any nan values
                ▪ Drop the record
                ▪ Else
                        • Find repeated values
                ▪ if any duplicate
                        • drop the record
```

Return preprocessed dataset

Flow chart:



6.3.3. Feature selection using mutual information classification

Mutual Information estimates mutual information for fixed categories like in a classification problem or a continuous target variable in regression problems. Mutual Information works on the entropy of the variables.

Let us take two random variables there mutual information between them will be zero if and only if the variables are completely independent otherwise the mutual information between them would be symmetric and non-negative.

The mutual information between two random variables *X* and *Y* can be stated formally as follows:

- I(X ; Y) = H(X) — H(X | Y)

Where *I(X; Y)* is the mutual information for *X* and *Y*, *H(X)* is the entropy for *X*, and *H(X | Y)* is the conditional entropy for *X* given *Y*. The result has the units of bits(zero to one).

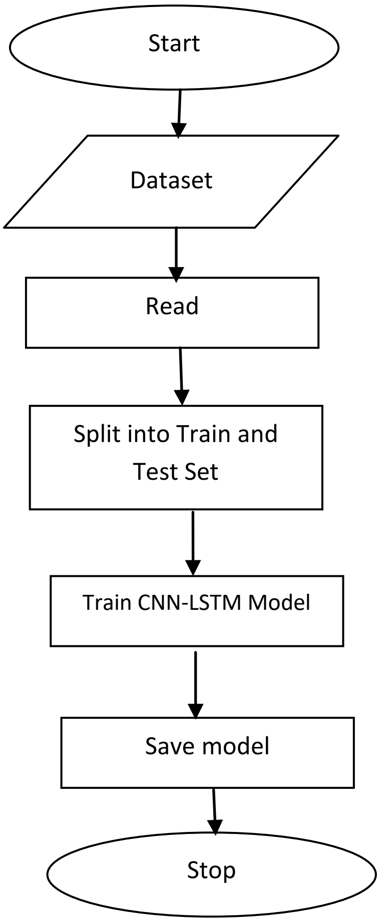
Mutual information is a measure of dependence or "*mutual dependence*" between two random variables. As such, the measure is symmetrical, meaning that *I(X; Y) = I(Y; X)*.

Entropy in chemistry is defined as randomness. Here Entropy quantifies how much information there is in a random variable. So mutual information helps in reducing the entropy.

6.3.4. BUILDING MODELS:

After feature selection we are planning to use CNN-LSTM model to perform the classification to detect the various types of cyber attacks.

Flow Chart:



6.3.5. PERFORMANCE ANALYSIS

We use the Accuracy, Prediction, Recall, and F1-Score to evaluate the experimental model's performance. These evaluation criteria reflect the performance of the intrusion detection system's flow recognition accuracy rate, and false alarm rate. The combination of the model prediction results and the true label is divided into four types: False Negative(FN), a positive sample, which is mistakenly judged as a negative sample. False Positive(FP), negative samples are misjudged as positive samples. True Negative(TN), actually negative samples, are correctly judged as negative samples. True Positive(TP), actually positive samples, are judged as the positive sample.

Pseudo code:

Performance Evaluation

Step 1: Load the test set

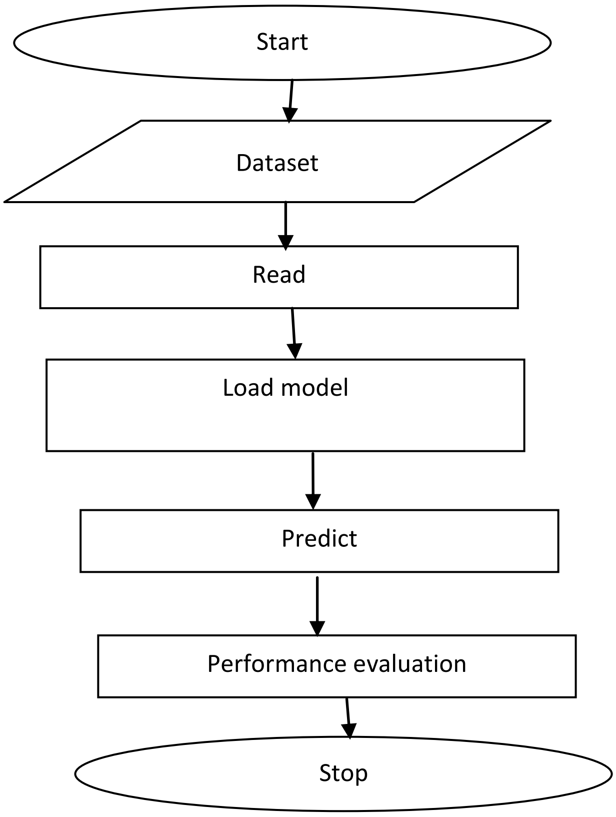
Step 2: Load the pre train model

Step 3: Evaluate the model using predict()

Step 4: Get the accuracy

Step 5: Show performance in the graph

Flow Chart:



6.4 Algorithms

In this project we are using following algorithms to detect cyber attacks in IOT network data

1. For selecting the important features mutual information correlation classification is used.
2. For detecting types of attacks CNN-LSTM is used.

- **MUTUAL INFORMATION CORRELATION:**

Mutual Information estimates mutual information for fixed categories like in a classification problem or a continuous target variable in regression problems. Mutual Information works on the entropy of the variables.

Let us take two random variables there mutual information between them will be zero if and only if the variables are completely independent otherwise the mutual information between them would be symmetric and non-negative.

The mutual information between two random variables *X* and *Y* can be stated formally as follows:

- $I(X ; Y) = H(X) — H(X \mid Y)$

Where *I(X; Y)* is the mutual information for *X* and *Y*, *H(X)* is the entropy for *X*, and *H(X | Y)* is the conditional entropy for *X* given *Y*. The result has the units of bits(zero to one).

Mutual information is a measure of dependence or "*mutual dependence*" between two random variables. As such, the measure is symmetrical, meaning that *I(X; Y) = I(Y; X)*.

Entropy in chemistry is defined as randomness. Here Entropy quantifies how much information there is in a random variable. So mutual information helps in reducing the entropy.

Pseudo Code:

```
X = multi_data.drop(["intrusion"],axis =1)
y = multi_data["intrusion"]
from sklearn.feature_selection import SelectKBest, SelectPercentile, mutual_info_classif

selector = SelectPercentile(mutual_info_classif, percentile=35)
X_reduced = selector.fit_transform(X, y)
X_reduced.shape
cols = selector.get_support(indices=True)
selected_columns = X.iloc[:,cols].columns.tolist()
selected_columns
```

- **CNN-LSTM** We proposed combining two advanced deep learning algorithms to detect intrusion from an IoT network dataset. A hybrid model was designed to automatically detect the attacks, and the structure of the proposed model is presented in following figure. the architecture was developed by combining two deep learning models, namely, the CNN and LSTM networks, whereas the CNN algorithm was used to process the significant features obtained from the mutual_info_classif method with the size of 20 × 625,783 to extract new complex features. A convolutional layer size of three kernels was used to extract the complex features, and tanh activation was proposed to transfer the data. A two kernel max pool was used for dimension reduction, and we mapped the features to the LSTM model for the extraction of new time information. After the LSTM time information was extracted, the fusion features were fully connected for use in the classification process. the softmax was proposed to detect attacks from the IoT network data.

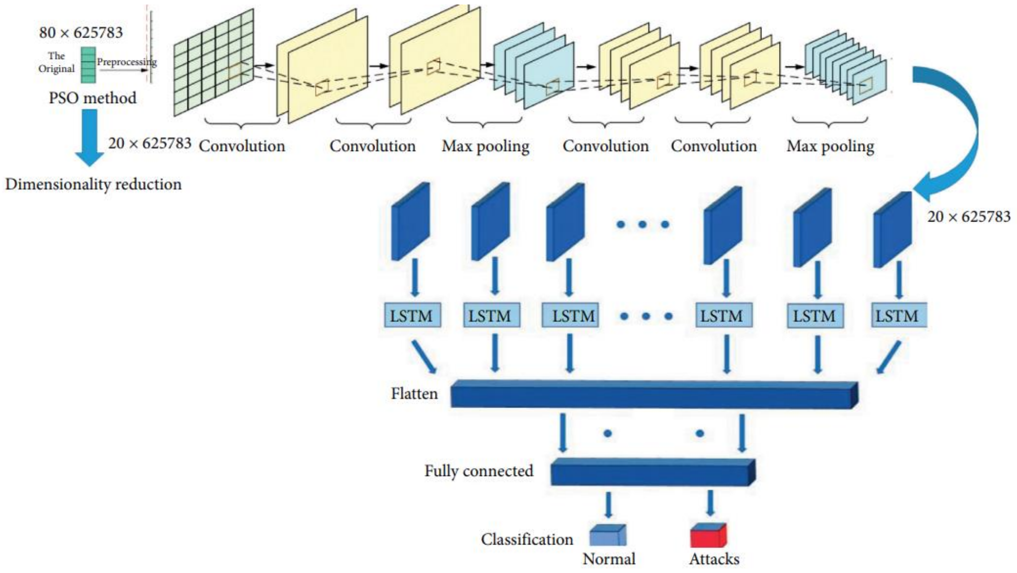


Fig 6.2 CNN-LSTM Architecture

Chapter 7

SYSTEM TESTING

The purpose of testing is to discover errors. Testing is the process of trying to discover every conceivable fault or weakness in a work product. It provides a way to check the functionality of components, sub assemblies, assemblies and/or a finished product It is the process of exercising software with the intent of ensuring that the

Software system meets its requirements and user expectations and does not fail in an unacceptable manner. There are various types of test. Each test type addresses a specific testing requirement.

7.1 TYPES OF TESTS

7.1.1 Unit testing

Unit testing involves the design of test cases that validate that the internal program logic is functioning properly, and that program inputs produce valid outputs. All decision branches and internal code flow should be validated. It is the testing of individual software units of the application .it is done after the completion of an individual unit before integration. This is a structural testing, that relies on knowledge of its construction and is invasive. Unit tests perform basic tests at component level and test a specific business process, application, and/or system configuration. Unit tests ensure that each unique path of a business process performs accurately to the documented specifications and contains clearly defined inputs and expected results.

7.1.2 Integration testing

Integration tests are designed to test integrated software components to determine if they actually run as one program. Testing is event driven and is more concerned with the basic outcome of screens or fields. Integration tests demonstrate that although the components were individually satisfaction, as shown by successfully unit testing, the combination of components is correct and consistent. Integration testing is specifically aimed at exposing the problems that arise from the combination of components.

7.1.3Functional test

Functional tests provide systematic demonstrations that functions tested are available as specified by the business and technical requirements, system documentation, and user manuals.

Functional testing is centered on the following items:

Valid Input : identified classes of valid input must be accepted.

Invalid Input : identified classes of invalid input must be rejected.

Functions : identified functions must be exercised.

Output : identified classes of application outputs must be exercised.

Systems/Procedures: interfacing systems or procedures must be invoked.

Organization and preparation of functional tests is focused on requirements, key functions, or special test cases. In addition, systematic coverage pertaining to identify Business process flows; data fields, predefined processes, and successive processes must be considered for testing. Before functional testing is complete, additional tests are identified and the effective value of current tests is determined.

7.1.4 System Test

System testing ensures that the entire integrated software system meets requirements. It tests a configuration to ensure known and predictable results. An example of system testing is the configuration oriented system integration test. System testing is based on process descriptions and flows, emphasizing pre-driven process links and integration points.

7.1.5 White Box Testing

White Box Testing is a testing in which in which the software tester has knowledge of the inner workings, structure and language of the software, or at least its purpose. It is purpose. It is used to test areas that cannot be reached from a black box level.

7.1.6 Black Box Testing

Black Box Testing is testing the software without any knowledge of the inner workings, structure or language of the module being tested. Black box tests, as most other kinds of tests, must be written from a definitive source document, such as specification or requirements document, such as specification or requirements document. It is a testing in which the software under test is treated, as a black box .you cannot "see" into it. The test provides inputs and responds to outputs without considering how the software works.

7.1.7 Unit Testing:

Unit testing is usually conducted as part of a combined code and unit test phase of the software lifecycle, although it is not uncommon for coding and unit testing to be conducted as two distinct phases.

Test strategy and approach

Field testing will be performed manually and functional tests will be written in detail.

Test objectives

- All field entries must work properly.
- Pages must be activated from the identified link.
- The entry screen, messages and responses must not be delayed.

Features to be tested

- Verify that the entries are of the correct format
- No duplicate entries should be allowed
- All links should take the user to the correct page.

7.1.8 Integration Testing

Software integration testing is the incremental integration testing of two or more integrated software components on a single platform to produce failures caused by interface defects.

The task of the integration test is to check that components or software applications, e.g. components in a software system or – one step up – software applications at the company level – interact without error.

Test Results: All the test cases mentioned above passed successfully. No defects encountered.

7.1.9 Acceptance Testing

User Acceptance Testing is a critical phase of any project and requires significant participation by the end user. It also ensures that the system meets the functional requirements.

Test Results: All the test cases mentioned above passed successfully. No defects encountered.

7.2 Test cases

Test Case#	UTC01
Test Name	User input format

Test Description	To test user input as dataset
Input	Dataset
Expected Output	The file should be read by the program and display on the monitor
Actual Output	The file is read and display accordingly
Test Result	Success

Test Case#	UTC02
Test Name	User input format
Test Description	To test user input dataset
Input	Dataset as null
Expected Output	Show alert message select dataset
Actual Output	Show alert message select dataset

Test Result	Success
Test Case#	UTC03
Test Name	Prediction of Intrusion
Test Description	To test whether predicting network Intrusion or not?
Input	Dataset
Expected Output	It Should predict Intrusion
Actual Output	Predicted intrusion as per the trained data
Test Result	Success

Test Case#	UTC04
Test Name	Test case for importing valid python libraries
Test Description	To test whether an algorithm to implement congestion nodes works without sklearn and keras models
Input	Import all valid libraries sklearn, tkinter and keras libraries
Expected Output	An error should be thrown specifying “error importing libraries sklearn, tkinter and keras libraries”
Actual Output	An error is thrown
Test Result	Success

Chapter 8

IMPLEMENTATION

8.1 Signup

```
<!DOCTYPE html>
<html lang="zxx">
<head>
<meta charset="UTF-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<title>Home</title>
<link rel="apple-touch-icon" sizes="57x57" href="static/images/favicons/apple-icon-
57x57.png">
<link rel="apple-touch-icon" sizes="60x60" href="static/images/favicons/apple-icon-
60x60.png">
<link rel="apple-touch-icon" sizes="72x72" href="static/images/favicons/apple-icon-
72x72.png">
<link rel="apple-touch-icon" sizes="76x76" href="static/images/favicons/apple-icon-
76x76.png">
<link rel="apple-touch-icon" sizes="114x114" href="static/images/favicons/apple-
icon-114x114.png">
<link rel="apple-touch-icon" sizes="120x120" href="static/images/favicons/apple-
icon-120x120.png">
<link rel="apple-touch-icon" sizes="144x144" href="static/images/favicons/apple-
icon-144x144.png">
<link rel="apple-touch-icon" sizes="152x152" href="static/images/favicons/apple-
icon-152x152.png">
<link rel="apple-touch-icon" sizes="180x180" href="static/images/favicons/apple-
icon-180x180.png">
<link rel="icon" type="image/png" sizes="192x192"
 href="static/images/favicons/android-icon-192x192.png">
<link rel="icon" type="image/png" sizes="32x32"
href="static/images/favicons/favicon-32x32.png">
<link rel="icon" type="image/png" sizes="96x96"
href="static/images/favicons/favicon-96x96.png">
<link rel="icon" type="image/png" sizes="16x16"
href="static/images/favicons/favicon-16x16.png">
<link rel="manifest" href="static/images/favicons/manifest.json">
<meta name="msapplication-TileColor" content="#ffffff">
<meta name="msapplication-TileImage" content="static/images/favicons/ms-icon-
144x144.png">
<meta name="theme-color" content="#ffffff">
<link rel="stylesheet" href="static/css/bootstrap.min.css">
<link rel="stylesheet" href="./static/css/style.css">
```

```
<link rel="stylesheet" href="./static/css/mobile.css">
<link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/font-
awesome/5.9.0/css/all.min.css"
integrity="sha512-
q3eWabyZPc1XTCmF+8/LuE1ozpg5xxn7iO89yfSOd5/oKvyqLngoNGsx8jq92Y8eXJ/IRxQbEC+FGSYxtk2o
iw=="
crossorigin="anonymous" referrerpolicy="no-referrer">
<link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/font-
awesome/6.1.1/css/all.min.css">
<link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/font-
awesome/6.1.2/css/all.min.css">
<link href="https://unpkg.com/aos@2.3.1/dist/aos.css" rel="stylesheet">
<link rel="stylesheet" href="static/css/owl.carousel.min.css">
<link rel="stylesheet" href="static/css/owl.theme.default.min.css">
</head>
<body>
    <!-- HEADER-SECTION -->
<div class="home-header-section">
        <figure class="banner-right-img left_icon img">
            <img src="static/images/header-right-img.png" alt="" class="star">
        </figure>
        <header class="header">
            <div class="main-header">
                <div class="container-fluid">
                    <nav class="navbar navbar-expand-lg navbar-light p-0">
                        <a class="navbar-brand pt-0" href="/"><img
src="static/images/cyber.png" alt="" class="img-fluid diverge-logo"></a>
                            <button class="navbar-toggler collapsed" type="button"
data-toggle="collapse"
                            data-target="#navbarSupportedContent" aria-
controls="navbarSupportedContent"
                            aria-expanded="false" aria-label="Toggle navigation">
                            <span class="navbar-toggler-icon"></span>
                            <span class="navbar-toggler-icon"></span>
                            <span class="navbar-toggler-icon"></span>
                            </button>
                                <div style="margin-left: 35%;" class="collapse
navbar-collapse" id="navbarSupportedContent">
                                    <ul  class="navbar-nav">
                                        <li  class="nav-item active">
                                            <a class="nav-link text-decoration-none
navbar-text-color home-margin-top" href="/">Home<span class="sr-
only">(current)</span></a>
                                        </li>

                                        <!-- <li class="nav-item navbar-text-
color"><a class="nav-link text-decoration-none contact-us-margin navbar-text-color"
href="pricing.html">Pricing</a></li> -->
```

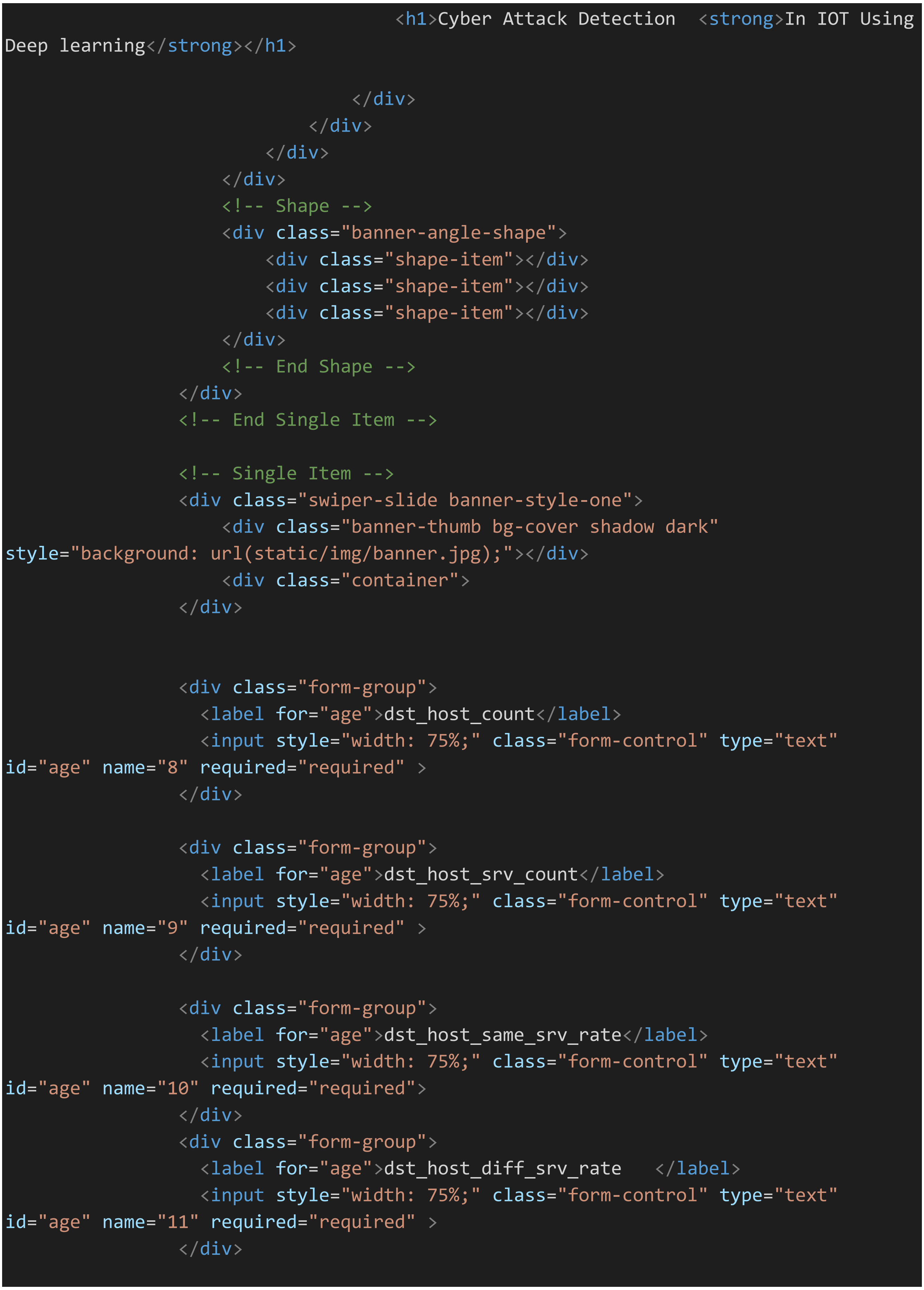
```
                  </ul>
                  <div class="btn-talk ml-auto">
                    <ul class="m-0 p-0">
                      <li class="list-unstyled d-lg-inline-
block"><a class="nav-link contact" href="/logon">Signup</a></li>
                    </ul>
                  </div>
                </div>
          </nav>
        </div>
      </div>
    </header>
    <!-- BANNER-SECTION -->
    <div class="home-banner-section overflow-hidden position-relative">
      <div class="banner-container-box">
        <div class="container-fluid">
          <div class="row">
            <div class="col-xl-6 col-lg-7 col-md-12 col-sm-12 mb-md-0
mb-4 text-md-left text-center order-lg-1 order-2">
              <div class="social-icons position-absolute">
                <ul class="list-unstyled">
                  <li><a class="text-decoration-none"><i
class="fa-brands fa-facebook-f social-networks"></i></a></li>
                  <li><a class="text-decoration-none"><i
class="fa-brands fa-twitter social-networks"></i></a></li>
                  <li><a class="text-decoration-none"><i
class="fa-brands fa-instagram social-networks"></i></a></li>
                </ul>
              </div>
              <div class="home-banner-text" data-aos="fade-up"
id="myContentDIV">
                <h1>Welcome <span class="h1-text">to </span> Cyber
Security</h1>
                <p class="banner-paragraph">
                  Cyber Attack Detection Using IOT</p>

              </div>
            </div>
            <div class="col-xl-6 col-lg-5 col-md-12 col-sm-12 order-lg-2
order-1">
              <div class="banner-img-content position-relative">
                <figure class="banner-img mb-0">
                  <img class="img-fluid banner-img-width"
src="static/images/cyber-security-left-img.png" alt="">
                </figure>
              </div>
            </div>
```

```
                    </div>
                </div>
            </div>
        </div>
    </div>
    <!-- About-Us-SECTION -->
<section class="about-us-section overflow-hidden position-relative">
    <figure class="about-left-back-img">
        <img src="static/images/about-left-background.png" alt="" class="star">
    </figure>
        <div class="container">
            <div class="row">

                <div class="col-xl-6 col-lg-6 col-md-12 col-sm-12 order-lg-2 order-
2">
                    <div class="about-us-content aos-init aos-animate" data-
aos="fade-up">
                        <h6 class="autorix-text"  data-aos="fade-up">About us</h6>

                        <p class="aboutus-p" data-aos="fade-up-right">The
technological advancements of Internet of Things (IoT) has revolutionized
traditional Consumer Electronics (CE) into next-generation CE with higher
connectivity and intelligence. This connectivity among sensors, actuators,
appliances, and other consumer devices enables improved data availability, and
provides automatic control in CE network. </p>


                    </div>
                </div>
        </div>
    </div>
</section>
    <!--partners-section -->

<!-- Form-Section -->

    <!-- Footer-Section -->
    <div class="footer-section">

        <div class="footer-bar text-center">
            <div class="row">
                <div class="footer-bar-content w-100">
                    <p class="text-size-16 mb-0">Whizcyber copyright © 2023. All
Rights Reserved.</p>
                </div>
            </div>
       </div>
    </div>
    <script src="https://code.jquery.com/jquery-1.12.1.min.js"></script>
    <script src="static/js/animations.js"></script>
    <script src="static/js/bootstrap.min.js"></script>
    <script src="static/js/jquery-3.6.0.min.js"></script>
    <script src="static/js/popper.min.js"></script>
    <script src="static/js/owl.carousel.js"></script>
    <script src="https://unpkg.com/aos@2.3.1/dist/aos.js"></script>
    <script src="static/js/text-animations.js"></script>
    <script src="static/js/carousel.js"></script>
    <script src="static/js/showhide.js"></script>
    <script src="https://cdnjs.cloudflare.com/ajax/libs/magnific-popup.js/1.1.0/jquery.magnific-popup.js"></script>
    <script src="https://unpkg.com/ityped@0.0.10"></script>
    <script src="./static/js/type.js"></script>
    <script src="static/js/custom-script.js"></script>
</body>
</html>
```

8.2 Home Page

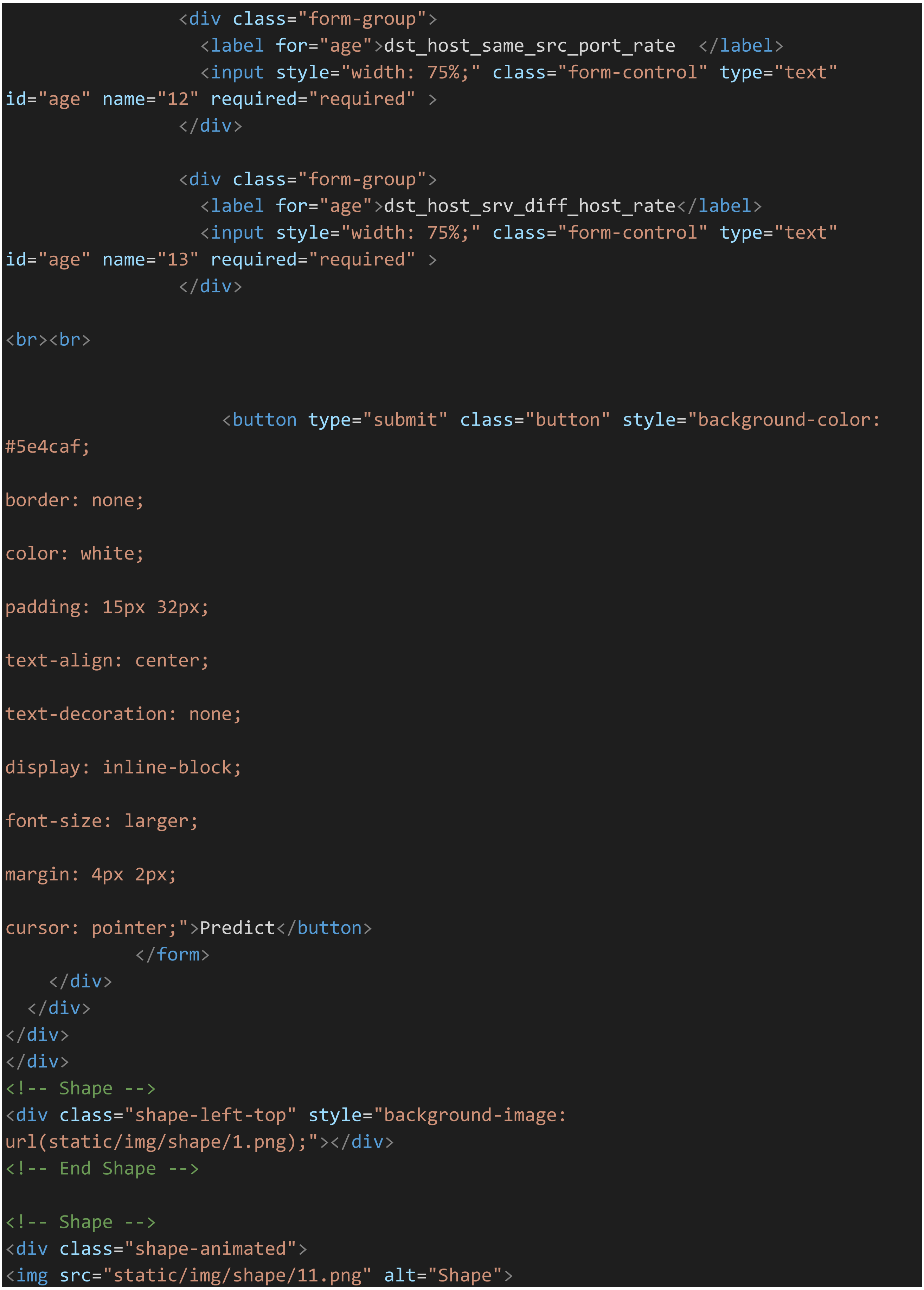
```
<!DOCTYPE html>
<html lang="en">

<head>
    <!-- ========== Meta Tags ========== -->
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale=1">
    <meta name="description" content="Crysa - It Solution Template">

    <!-- ========== Page Title ========== -->
    <title>Form</title>

    <!-- ========== Favicon Icon ========== -->
    <link rel="shortcut icon" href="static/img/favicon.png" type="image/x-icon">

    <!-- ========== Start Stylesheet ========== -->
    <link href="static/css/bootstrap.min.css" rel="stylesheet" />
    <link href="static/css/font-awesome.min.css" rel="stylesheet" />
    <link href="static/css/themify-icons.css" rel="stylesheet" />
    <link href="static/css/elegant-icons.css" rel="stylesheet" />
    <link href="static/css/flaticon-set.css" rel="stylesheet" />
    <link href="static/css/magnific-popup.css" rel="stylesheet" />
    <link href="static/css/swiper-bundle.min.css" rel="stylesheet" />
    <link href="static/css/animate.css" rel="stylesheet" />
    <link href="static/css/validnavs.css" rel="stylesheet" />
    <link href="static/css/helper.css" rel="stylesheet" />
    <link href="static/css/style.css" rel="stylesheet" />
    <link href="static/style.css" rel="stylesheet">
    <!-- ========== End Stylesheet ========== -->

</head>

<body>

    <!--[if lte IE 9]>
        <p class="browserupgrade">You are using an <strong>outdated</strong>
browser. Please <a href="https://browsehappy.com/">upgrade your browser</a> to
improve your experience and security.</p>
    <![endif]-->

    <!-- Preloader Start -->
    <div class="se-pre-con"></div>
    <!-- Preloader Ends -->

    <!-- Start Header Top
    ============================================= -->
    <div class="top-bar bg-dark text-light top-style-one">
        <div class="container-fill pr">
            <div class="row align-center">

                <div class="col-xl-3 col-lg-4 text-right item-flex">


                        <span class="input-group-addon close-search"><i class="fa
fa-times"></i></span>
                    </div>
                </div>
            </div>
            <!-- End Top Search -->

            <div class="container-fill pr">


                <div class="row align-center">
                    <!-- Start Header Navigation -->
                    <div class="col-xl-2 col-lg-2 col-md-2 col-sm-1 col-1">
                        <div class="navbar-header">
                            <button type="button" class="navbar-toggle" data-
toggle="collapse" data-target="#navbar-menu">
                                <i class="fa fa-bars"></i>
                            </button>
                            <a class="navbar-brand" href="#">
                                <img src="static/img/logo.png" class="logo logo-
display" alt="Logo">
```

```
                                <img src="static/img/logo.png" class="logo logo-
scrolled" alt="Logo">
                            </a>
                        </div>
                    </div>
                    <!-- End Header Navigation -->

                    <!-- Collect the nav links, forms, and other content for
toggling -->
                    <div class="col-xl-7 col-lg-8 col-md-4 col-sm-4 col-4">
                        <div class="collapse navbar-collapse" id="navbar-menu">

                            <img src="static/img/logo.png" alt="Logo">
                            <button type="button" class="navbar-toggle" data-
toggle="collapse" data-target="#navbar-menu">
                                <i class="fa fa-times"></i>
                            </button>

                            <ul class="nav navbar-nav navbar-right" data-
in="fadeInDown" data-out="fadeOutUp">

                              <li><a href="/home">Home</a></li>
                                <li class="dropdown">
        </nav>
        <!-- End Navigation -->

    </header>
    <!-- End Header -->

    <!-- Start Banner Area
    ============================================= -->
    <div class="banner-area banner-style-one content-right navigation-custom-large
zoom-effect overflow-hidden text-light">
        <!-- Slider main container -->
        <div class="banner-fade">
            <!-- Additional required wrapper -->
            <div class="swiper-wrapper">

                <!-- Single Item -->
                <div class="swiper-slide banner-style-one">
                    <div class="banner-thumb bg-cover shadow dark"
style="background: url(static/img/banner.jpg);"></div>
                    <div class="container">
                        <div class="row align-center">
                            <div class="col-xl-7 offset-xl-5">
                                <div class="content">
                                    <h4>Welcome To Dashboard</h4>
```



```
                                    <h1>Cyber Attack Detection  <strong>In IOT Using
Deep learning</strong></h1>

                                </div>
                            </div>
                        </div>
                    </div>
                    <!-- Shape -->
                    <div class="banner-angle-shape">
                        <div class="shape-item"></div>
                        <div class="shape-item"></div>
                        <div class="shape-item"></div>
                    </div>
                    <!-- End Shape -->
                </div>
                <!-- End Single Item -->

                <!-- Single Item -->
                <div class="swiper-slide banner-style-one">
                    <div class="banner-thumb bg-cover shadow dark"
style="background: url(static/img/banner.jpg);"></div>
                    <div class="container">
                </div>


                <div class="form-group">
                  <label for="age">dst_host_count</label>
                  <input style="width: 75%;" class="form-control" type="text"
id="age" name="8" required="required" >
                </div>

                <div class="form-group">
                  <label for="age">dst_host_srv_count</label>
                  <input style="width: 75%;" class="form-control" type="text"
id="age" name="9" required="required" >
                </div>

                <div class="form-group">
                  <label for="age">dst_host_same_srv_rate</label>
                  <input style="width: 75%;" class="form-control" type="text"
id="age" name="10" required="required">
                </div>
                <div class="form-group">
                  <label for="age">dst_host_diff_srv_rate   </label>
                  <input style="width: 75%;" class="form-control" type="text"
id="age" name="11" required="required" >
                </div>
```

```
<img src="static/img/logo.png" class="logo logo-scrolled" alt="Logo">
                            </a>
                        </div>
                    </div>
                    <!-- End Header Navigation -->

                    <!-- Collect the nav links, forms, and other content for
toggling -->
                    <div class="col-xl-7 col-lg-8 col-md-4 col-sm-4 col-4">
                        <div class="collapse navbar-collapse" id="navbar-menu">

                            <img src="static/img/logo.png" alt="Logo">
                            <button type="button" class="navbar-toggle" data-
toggle="collapse" data-target="#navbar-menu">
                                <i class="fa fa-times"></i>
                            </button>

                            <ul class="nav navbar-nav navbar-right" data-
in="fadeInDown" data-out="fadeOutUp">

                              <li><a href="/home">Home</a></li>
                                <li class="dropdown">
        </nav>
        <!-- End Navigation -->

    </header>
    <!-- End Header -->

    <!-- Start Banner Area
    ============================================= -->
    <div class="banner-area banner-style-one content-right navigation-custom-large
zoom-effect overflow-hidden text-light">
        <!-- Slider main container -->
        <div class="banner-fade">
            <!-- Additional required wrapper -->
            <div class="swiper-wrapper">

                <!-- Single Item -->
                <div class="swiper-slide banner-style-one">
                    <div class="banner-thumb bg-cover shadow dark"
style="background: url(static/img/banner.jpg);"></div>
                    <div class="container">
                        <div class="row align-center">
                            <div class="col-xl-7 offset-xl-5">
                                <div class="content">
                                    <h4>Welcome To Dashboard</h4>
```



```
                <div class="form-group">
                  <label for="age">dst_host_same_src_port_rate  </label>
                  <input style="width: 75%;" class="form-control" type="text" 
id="age" name="12" required="required" >
                </div>

                <div class="form-group">
                  <label for="age">dst_host_srv_diff_host_rate</label>
                  <input style="width: 75%;" class="form-control" type="text" 
id="age" name="13" required="required" >
                </div>

<br><br>


                    <button type="submit" class="button" style="background-color: 
#5e4caf;

border: none;

color: white;

padding: 15px 32px;

text-align: center;

text-decoration: none;

display: inline-block;

font-size: larger;

margin: 4px 2px;

cursor: pointer;">Predict</button>
            </form>
    </div>
  </div>
</div>
</div>
<!-- Shape -->
<div class="shape-left-top" style="background-image: 
url(static/img/shape/1.png);"></div>
<!-- End Shape -->

<!-- Shape -->
<div class="shape-animated">
<img src="static/img/shape/11.png" alt="Shape">
```

```
</div>
<!-- End Shape -->

<!-- Shape -->
<div class="blur-bg"></div>
<!-- End Shape -->


</div>
<!-- End About -->


<!-- End Footer Bottom -->
</footer>
<!-- End Footer -->

<!-- jQuery Frameworks
============================================= -->
<script src="static/js/jquery-3.6.0.min.js"></script>
<script src="static/js/bootstrap.bundle.min.js"></script>
<script src="static/js/jquery.appear.js"></script>
<script src="static/js/jquery.easing.min.js"></script>
<script src="static/js/jquery.magnific-popup.min.js"></script>
<script src="static/js/modernizr.custom.13711.js"></script>
<script src="static/js/swiper-bundle.min.js"></script>
<script src="static/js/wow.min.js"></script>
<script src="static/js/progress-bar.min.js"></script>
<script src="static/js/circle-progress.js"></script>
<script src="static/js/isotope.pkgd.min.js"></script>
<script src="static/js/imagesloaded.pkgd.min.js"></script>
<script src="static/js/jquery.nice-select.min.js"></script>
<script src="static/js/count-to.js"></script>
<script src="static/js/jquery.scrolla.min.js"></script>
<script src="static/js/YTPlayer.min.js"></script>
<script src="static/js/TweenMax.min.js"></script>
<script src="static/js/validnavs.js"></script>
<script src="static/js/main.js"></script>

</body>
</html>
```

8.3 KDD-CUP

```
import warnings
warnings.filterwarnings('ignore')
# importing required libraries
import numpy as np
import pandas as pd
import pickle # saving and loading trained model
from os import path

# importing required libraries for normalizing data
from sklearn import preprocessing
from sklearn.preprocessing import (StandardScaler, OrdinalEncoder,LabelEncoder, MinMaxScaler, OneHotEncoder)
from sklearn.preprocessing import Normalizer, MaxAbsScaler , RobustScaler, PowerTransformer
# importing library for plotting
import matplotlib.pyplot as plt
import seaborn as sns
from sklearn import metrics
from sklearn.metrics import accuracy_score # for calculating accuracy of model
from sklearn.model_selection import train_test_split # for splitting the dataset for training and testing
from sklearn.metrics import classification_report # for generating a classification report of model

from sklearn.metrics import precision_score
from sklearn.metrics import recall_score
from sklearn.metrics import f1_score

from sklearn.metrics import roc_auc_score
from sklearn.metrics import roc_curve, auc
import tensorflow as tf
from tensorflow.keras.utils import to_categorical

from keras.layers import Dense, Conv1D, MaxPool1D, Flatten, Dropout # importing dense layer
from keras.models import Sequential #importing Sequential layer
from keras.layers import Input
from keras.models import Model
# representation of model layers
from keras.utils.vis_utils import plot_model
import tensorflow as tf
gpus = tf.config.list_physical_devices('GPU')
if gpus:
  # Create 2 virtual GPUs with 1GB memory each
  try:
    tf.config.set_logical_device_configuration(
        gpus[0],
        [tf.config.LogicalDeviceConfiguration(memory_limit=1024),
         tf.config.LogicalDeviceConfiguration(memory_limit=1024)])
    logical_gpus = tf.config.list_logical_devices('GPU')
    print(len(gpus), "Physical GPU,", len(logical_gpus), "Logical GPUs")
  except RuntimeError as e:
    # Virtual devices must be set before GPUs have been initialized
    print(e)
```

Chapter 9

RESULTS

9.1 Snapshots

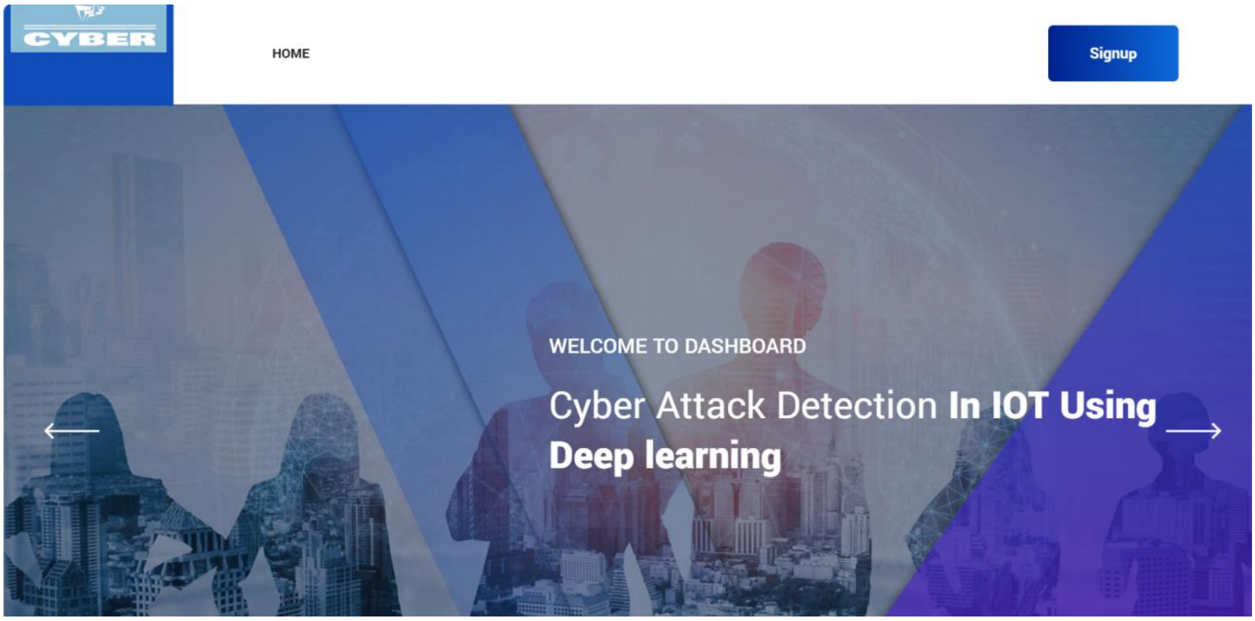


Fig 9.1 Home Page

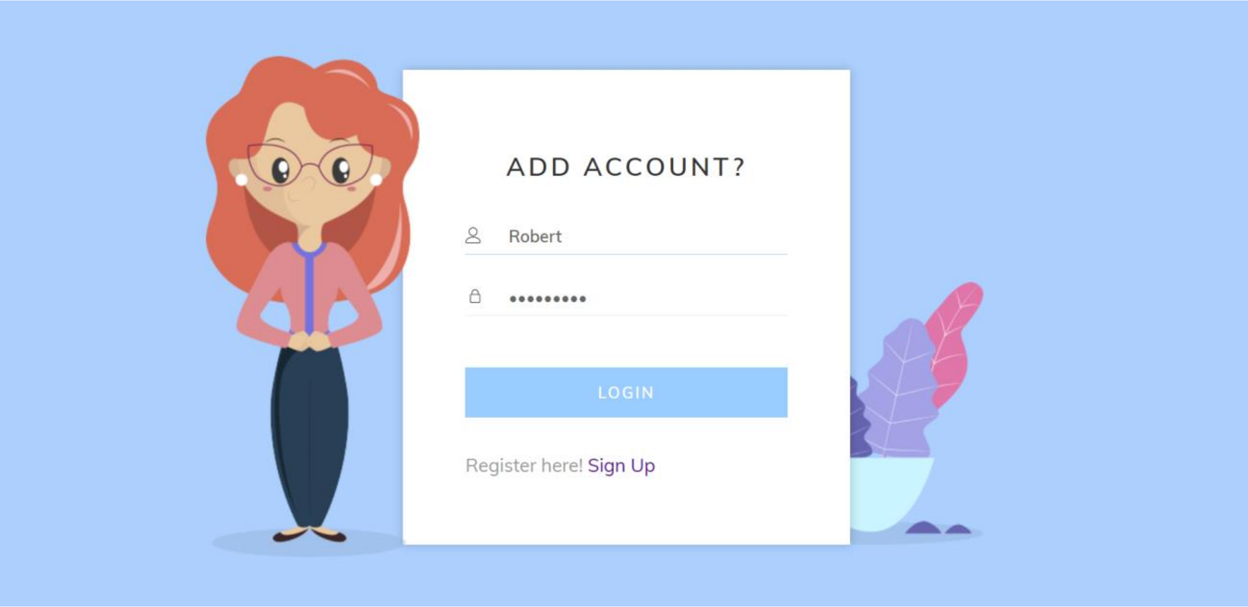
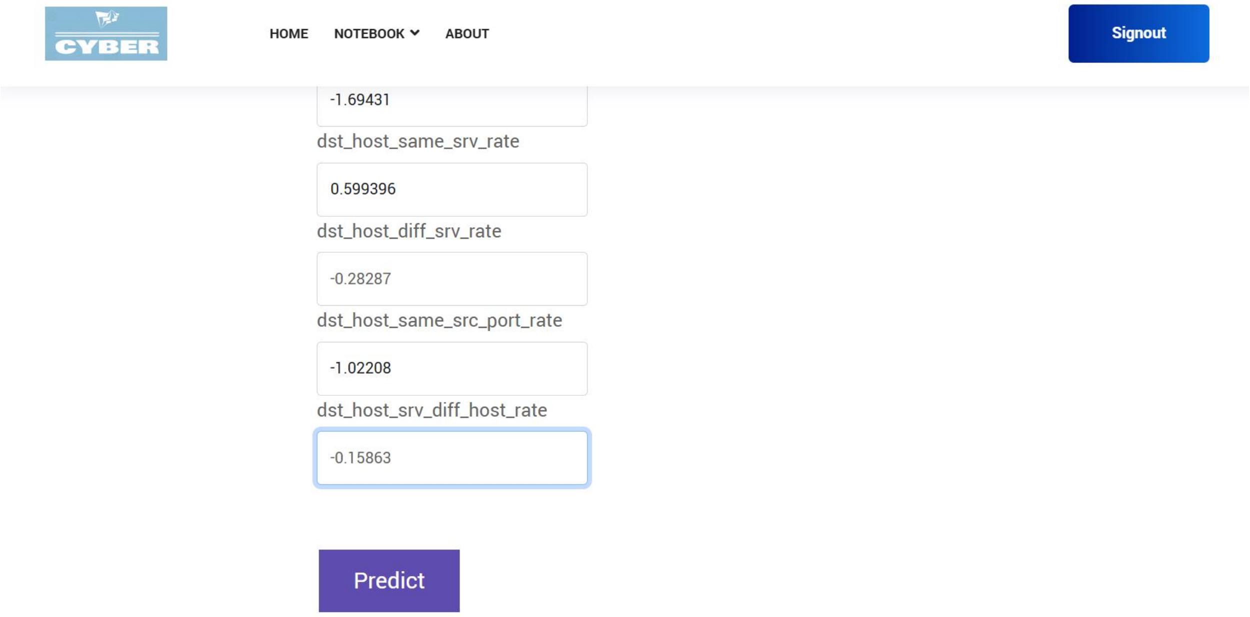
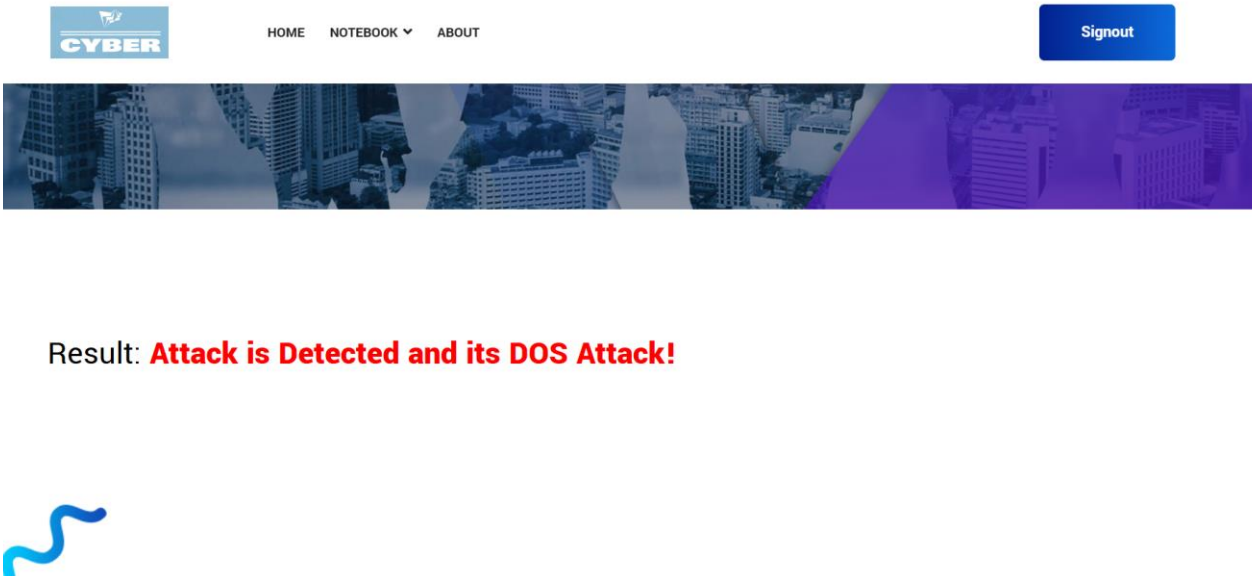


Fig 9.2 Login Page



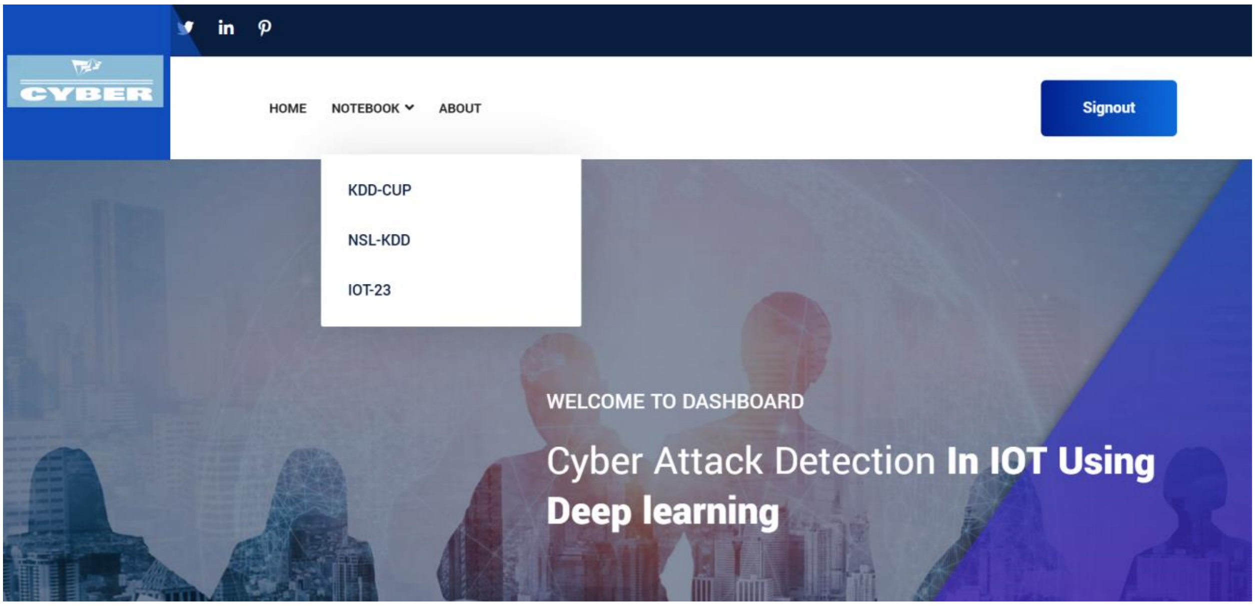
-1.69431
dst_host_same_srv_rate
0.599396
dst_host_diff_srv_rate
-0.28287
dst_host_same_src_port_rate
-1.02208
dst_host_srv_diff_host_rate
-0.15863

Fig 9.3 Prediction Page



Result: Attack is Detected and its DOS Attack!

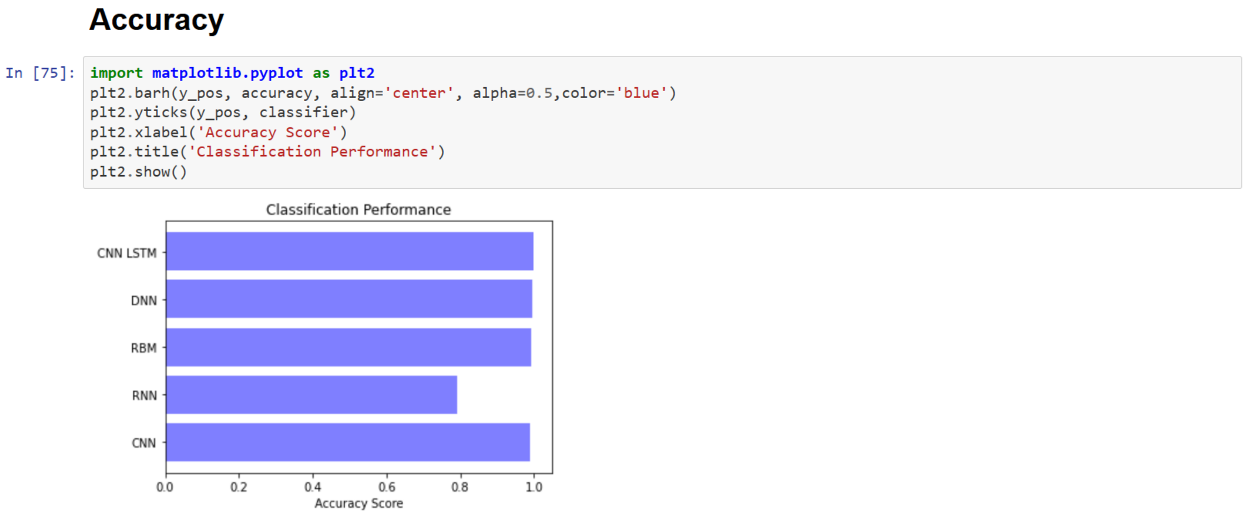
Fig 9.4 Result Page showing name of attack detected



WELCOME TO DASHBOARD

Cyber Attack Detection **In IOT Using Deep learning**

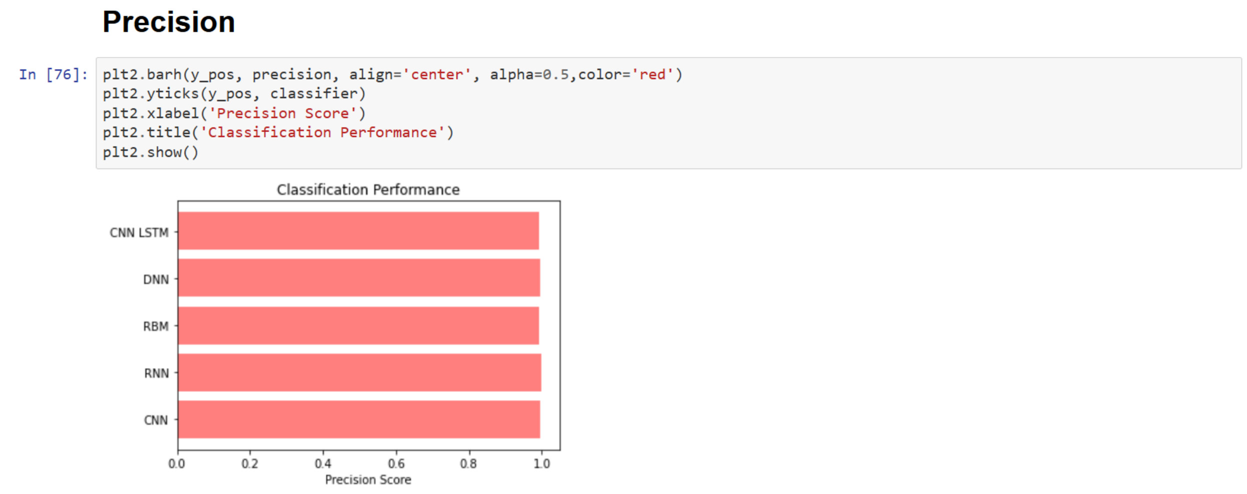
Fig 9.5 Dashboard



Accuracy

```
In [75]: import matplotlib.pyplot as plt2
         plt2.barh(y_pos, accuracy, align='center', alpha=0.5,color='blue')
         plt2.yticks(y_pos, classifier)
         plt2.xlabel('Accuracy Score')
         plt2.title('Classification Performance')
         plt2.show()
```

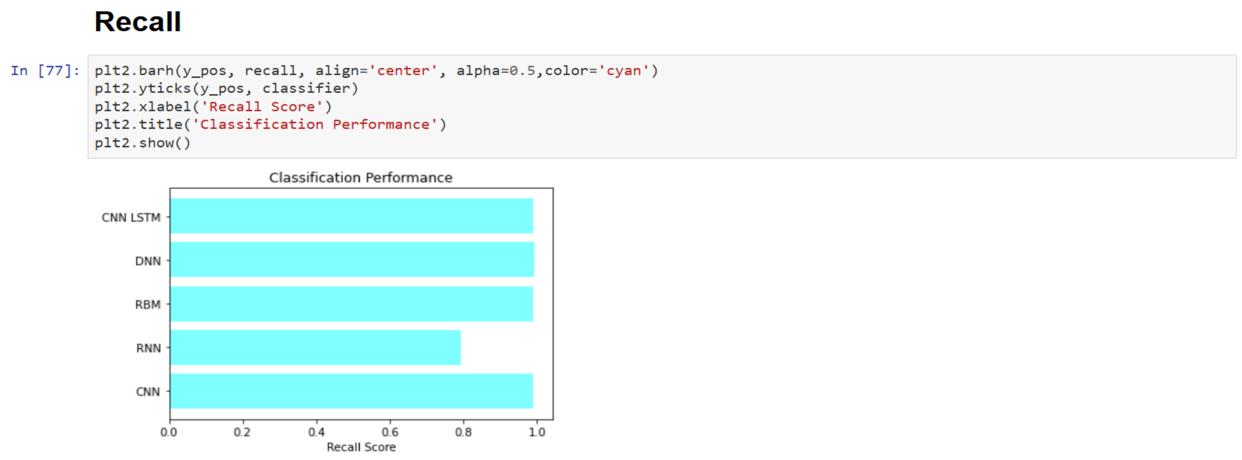
Fig 9.6 Accuracy score



Precision

```
In [76]: plt2.barh(y_pos, precision, align='center', alpha=0.5,color='red')
         plt2.yticks(y_pos, classifier)
         plt2.xlabel('Precision Score')
         plt2.title('Classification Performance')
         plt2.show()
```

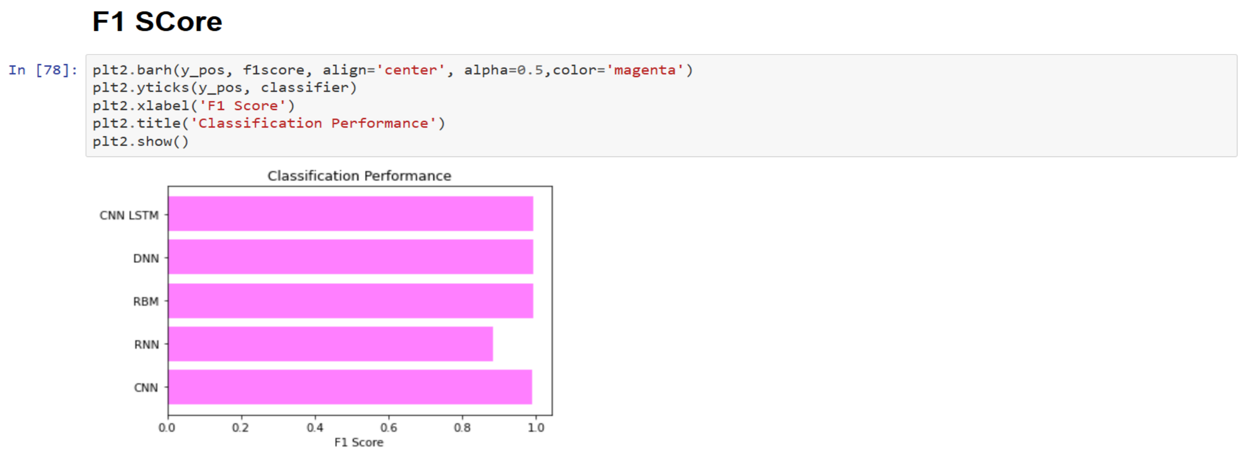
Fig 9.7 Precision Score



Recall

```
In [77]: plt2.barh(y_pos, recall, align='center', alpha=0.5,color='cyan')
         plt2.yticks(y_pos, classifier)
         plt2.xlabel('Recall Score')
         plt2.title('Classification Performance')
         plt2.show()
```

Fig 9.8 Recall Score

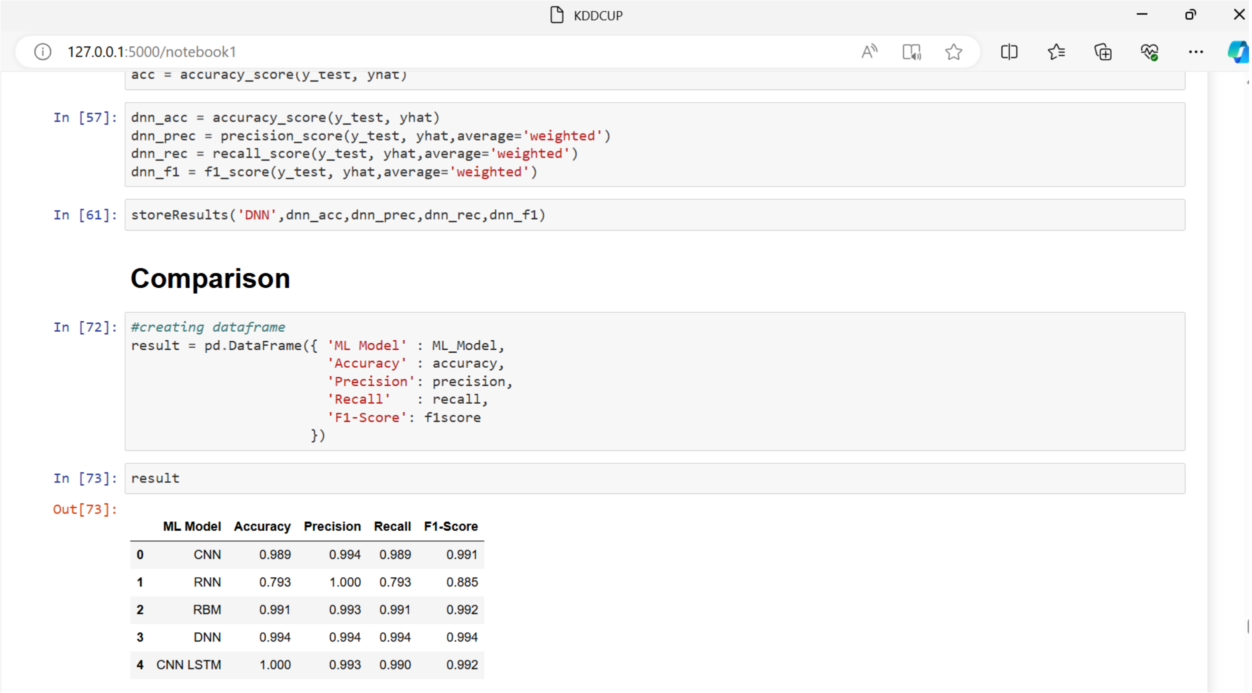


F1 SCore

```
In [78]: plt2.barh(y_pos, f1score, align='center', alpha=0.5,color='magenta')
         plt2.yticks(y_pos, classifier)
         plt2.xlabel('F1 Score')
         plt2.title('Classification Performance')
         plt2.show()
```

Fig 9.9 F1 Score

9.2 Comparison of Results



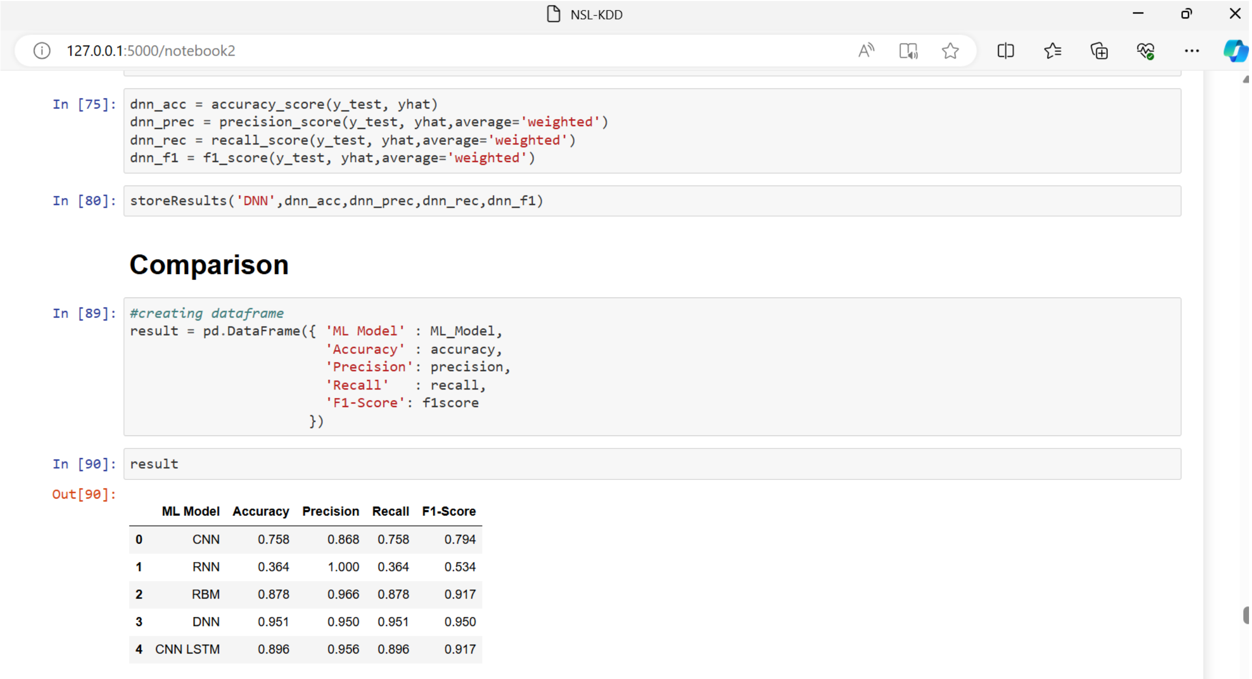
```
acc = accuracy_score(y_test, yhat)

In [57]: dnn_acc = accuracy_score(y_test, yhat)
         dnn_prec = precision_score(y_test, yhat,average='weighted')
         dnn_rec = recall_score(y_test, yhat,average='weighted')
         dnn_f1 = f1_score(y_test, yhat,average='weighted')

In [61]: storeResults('DNN',dnn_acc,dnn_prec,dnn_rec,dnn_f1)
```

Comparison

```
In [72]: #creating dataframe
         result = pd.DataFrame({ 'ML Model' : ML_Model,
                                 'Accuracy' : accuracy,
                                 'Precision': precision,
                                 'Recall'   : recall,
                                 'F1-Score': f1score
                               })

In [73]: result

Out[73]:
```

	ML Model	Accuracy	Precision	Recall	F1-Score
0	CNN	0.989	0.994	0.989	0.991
1	RNN	0.793	1.000	0.793	0.885
2	RBM	0.991	0.993	0.991	0.992
3	DNN	0.994	0.994	0.994	0.994
4	CNN LSTM	1.000	0.993	0.990	0.992

Fig 9.10 Results of KDDCUP



```
In [75]: dnn_acc = accuracy_score(y_test, yhat)
         dnn_prec = precision_score(y_test, yhat,average='weighted')
         dnn_rec = recall_score(y_test, yhat,average='weighted')
         dnn_f1 = f1_score(y_test, yhat,average='weighted')

In [80]: storeResults('DNN',dnn_acc,dnn_prec,dnn_rec,dnn_f1)
```

Comparison

```
In [89]: #creating dataframe
         result = pd.DataFrame({ 'ML Model' : ML_Model,
                                 'Accuracy' : accuracy,
                                 'Precision': precision,
                                 'Recall'   : recall,
                                 'F1-Score': f1score
                               })

In [90]: result

Out[90]:
```

	ML Model	Accuracy	Precision	Recall	F1-Score
0	CNN	0.758	0.868	0.758	0.794
1	RNN	0.364	1.000	0.364	0.534
2	RBM	0.878	0.966	0.878	0.917
3	DNN	0.951	0.950	0.951	0.950
4	CNN LSTM	0.896	0.956	0.896	0.917

Fig 9.11 Results of NSL-KDD

CONCLUSION

This project has shown that for a limited set of attacks and IoT devices, it is possible to use generative deep learning methods like mutual information classification and CNN-LSTM to classify attacks with a very high accuracy. Although there are several datasets regarding intrusion detection, it is better to use a dataset which was generated from IoT devices. Hence, in this project we used a recent dataset called KDD network attack dataset. We implemented baseline models, mutual information classification and CNN-LSTM. Our results show that the LSTM based models are more effective at identifying attacks and classifying them. We also tried randomizing the test set in a way that we can inject new information and the model was able to consider it as an anomaly.

PROJECT OUTCOME

Project Title: Deep Learning Framework to Detect Cyber-Attacks in IoT Network

Year: 2023-24

SL. No	Factors addressed through this project	Applicable PO's and PSO's	Justification
1.	Network Protection	PO1,PO2,PO3,PO4, PO5,PO7,PO8,PO9,PO10, PO11,PO12,PSO1,PSO2,PSO3	Applied engineering knowledge to analyze the problems in IoT networks using Deep-Learning Models to achieve significance performance improvements in classifying malware by handling various issues.

REFERENCES

[1] R. Shire, S. Shiaeles, K. Bendiab, B. Ghita, and N. Kolokotronis, “Malware squid: A novel IoT malware traffic analysis framework using convolutional neural network and binary visualisation,” in Internet of Things, Smart Spaces, and Next Generation Networks and Systems. Cham, Switzerland: Springer, 2019, pp. 65–76.

[2] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, ‘‘DDoS in the IoT: Mirai and other Botnets,’’ Computer, vol. 50, no. 7, pp. 80–84, 2020, doi: 10.1109/MC.2020.201.

[3] S. Kwon, H. Yoo, and T. Shon, “IEEE 1815.1-based power system security with bidirectional RNN-based network anomalous attack detection for cyber-physical system,” IEEE Access, vol.8, pp. 77572–77586, 2020.

[4] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, ‘‘Fog computing and its role in the Internet of Things,’’ in Proc. 1st Ed. MCC Workshop Mobile cloud Comput. (MCC), 2012, p. 13.

[5] J. Pacheco and S. Hariri, ‘‘Anomaly behavior analysis for IoT sensors,’’ Trans. Emerg. Telecommun. Technol., vol. 29, no. 4, p. e3188, Apr. 2018.

[6] G. Kaur, A. H. Lashkari, and A. Rahali, ‘‘Intrusion traffic detection and characterization using deep image learning,’’ in Proc. IEEE Dependable, Autonomic Secure Comput., Aug. 2020, pp. 55–62, doi: 10.1109/DASC-PICom-CBDCom-CyberSciTech49142.2020.00025

[7] M. A. Ferrag, L. Maglaras, S. Moschoyiannis, and H. Janicke, ‘‘Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study,’’ J. Inf. Secur. Appl., vol. 50, Feb. 2020, Art. no. 102419, doi: 10.1016/j.jisa.2019.102419.

[8] D. Li, L. Deng, M. Lee, and H. Wang, ‘‘IoT data feature extraction and intrusion detection system for smart cities based on deep migration learning,’’ Int. J. Inf. Manage., vol. 49, pp. 533–545, Oct. 2019, doi: 10.1016/j.ijinfomgt.2019.04.006.

[9] B. Alqahtani and B. AlNajrani, ‘‘A study of Internet of Things protocols and communication,’’ in Proc. 2nd Int. Conf. Comput. Inf. Sci. (ICCIS), Oct. 2020, pp. 1–6, doi: 10.1109/ICCIS49240.2020.9257652.

[10] I. Andrea, C. Chrysostomou, and G. Hadjichristofi, ‘‘Internet of Things: Security vulnerabilities and challenges,’’ in Proc. IEEE Symp. Comput. Commun. (ISCC), Jul. 2019, pp. 180–187, doi: 10.1109/ISCC.2015.7405513.

[11] R. Ahmad and I. Alsmadi, ‘‘Machine learning approaches to IoT security: A systematic literature review,’’ Internet Things, vol. 14, Jun. 2021, Art. no. 100365, doi: 10.1016/j.iot.2021.100365.