A

Mini Project On

**An Efficient Spam Detection Technique for IOT Devices using   
Machine Learning**

(Submitted in partial fulfillment of the requirements for the award of Degree) BACHELOR OF TECHNOLOGY

in

COMPUTER SCIENCE AND ENGINEERING

By

N.Nishanth Reddy (217R1A0539)

S.Nagaraju(227R5A0504) P.Sainath (217R1A0545)

Under the Guidance of

**G.PAVAN KUMAR**

(Assistant Professor)



## DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

**CMR TECHNICAL CAMPUS**

**UGC AUTONOMOUS**

(Accredited by NAAC, NBA, Permanently Affiliated to JNTUH, Approved by AICTE, New Delhi) Recognized Under Section 2(f) & 12(B) of the UGCAct.1956,

Kandlakoya (V), Medchal Road, Hyderabad-501401.

**2021-25**

## DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING



**CERTIFICATE**

This is to certify that the project entitled “**AN EFFICIENT SPAM DETECTION TECHNIQUE FOR IOT DEVICES USING MACHINE LEARNING**” being submitted by **N.NISHANTHREDDY (217R1A0539) , S.NAGARAJU(227R5A0504) & P.SAINATH (217R1A0545)** in partial fulfillment of the requirements for the award of the degree of B.Tech in Computer Science and Engineering to the Jawaharlal Nehru Technological University Hyderabad, is a record of bonafide work carried out by him/her under our guidance and supervision during the year 2023-24.

The results embodied in this thesis have not been submitted to any other University or Institute for the award of any degree or diploma.

#### Mr.G.Pavan Kumar Dr. A. Raji Reddy Assistant Professor DIRECTOR

**INTERNAL GUIDE**

**Dr. Nuthanakanti Bhaskar EXTERNAL EXAMINER**

**HOD**

**Submitted for viva voice Examination held on**

**ACKNOWLEGDEMENT**

Apart from the efforts of us, the success of any project depends largely on the encouragement and guidelines of many others. We take this opportunity to express our gratitude to the people who have been instrumental in the successful completion of this project. We take this opportunity to express my profound gratitude and deep regard to my guide

**Mr.G.Pavan kumar,** Assistant Professor for his exemplary guidance, monitoring and constant encouragement throughout the project work. The blessing, help and guidance given by him shall carry us a long way in the journey of life on which we are about to embark.  
 We also take this opportunity to express a deep sense of gratitude to Project Review Committee (PRC) Coordinators**,Dr. K. Maheswari, Dr. J. Narasimharao,Ms.K.Shilpa,  
Mr.K.Ranjith Reddy** for their cordial support, valuable information and guidance, which helped us in completing this task through various stages.

We are also thankful to **Dr. Nuthanakanti Bhaskar** Head, Department of Computer Science and Engineering for providing encouragement and support for completing this project successfully.

We are obliged to **Dr. A. Raji Reddy,** Director for being cooperative throughout the course of this project. We would like to express our sincere gratitude to Sri. **Ch. Gopal Reddy,** Chairman for providing excellent infrastructure and a nice atmosphere throughout the course of this project.

The guidance and support received from all the members of **CMR Technical Campus** who contributed to the completion of the project. We are grateful for their constant support and help.

Finally, we would like to take this opportunity to thank our family for their constant encouragement, without which this assignment would not be completed. We sincerely acknowledge and thank all those who gave support directly and indirectly in the completion of this project.

#### N.NISHANTH REDDY (217R1A0539) S.NAGARAJU (227R5A0504) P.SAINATH(217R1A0545)

**ABSTRACT**

The Internet of Things (IOT) is a group of millions of devices having sensors and actuators linked over wired or wireless channel for data transmission. IOT has grown rapidly over the past decade with more than 25 billion devices are expected to be connected by 2020. The volume of data released from these devices will increase many-fold in the years to come. In addition to an increased volume, the IOT devices produces a large amount of data with a number of different modalities having varying data quality defined by its speed in terms of time and position dependency. In such an environment, machine learning algorithms can play an important role in ensuring security and authorization based on biotechnology, anomalous detection to

Improve the usability and security of IOT systems. On the other hand, attackers often view learning algorithms to exploit the vulnerabilities in smart IOT-based systems. Motivated from these,in this paper, we propose the security of the IOT devices by detecting spam using machine learning. To achieve this objective,Spam Detection in IOT using Machine Learning framework is proposed. In this framework, five machine learning models are evaluated using various metrics with a large collection of inputs features sets. Each model computes a spam score by considering the refined input features. This score depicts the trustworthiness of IOT device under various parameters. REFIT Smart Home data set is used for the validation of proposed technique. The results obtained proves the effectiveness of the proposed scheme in comparison to the other existing schemes.

## LIST OF FIGURES

|  |  |  |
| --- | --- | --- |
| **FIGURE NO** | **FIGURE NAME** | **PAGE NO** |
| Figure 3.1 | Project Architecture | 6 |
| Figure 3.2 | Use case diagram | 8 |
| Figure 3.3 | Class diagram | 9 |
| Figure 3.4 | Sequence diagram | 10 |
| Figure 3.5 | Activity diagram | 11 |

|  |  |  |
| --- | --- | --- |
| **SCREENSHOT NO.** | **SCREENSHOT NAME** | **PAGE NO**. |
| Screenshot 5.1 | Web Interface | 15 |
| Screenshot 5.2 | Login Page | 16 |
| Screenshot 5.3 | Uploading Data | 17 |
| Screenshot 5.4 | Preview Data | 18 |
| Screenshot 5.5 | Prediction | 19 |
| Screenshot 5.6 | Output | 20 |
| Screenshot 5.7 | Performance | 22 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ABSTRACT** | |  |  | i |
| **LIST OF FIGURES** | | |  | ii |
| **LIST OF SCREENSHOTS** | | | | iii |
| **1.** | **INTRODUCTION** | | | 1 |
|  | 1.1 | PROJECT SCOPE | | 1 |
|  | 1.2 | PROJECT PURPOSE | | 1 |
|  | 1.3 | PROJECT FEATURES | | 1 |
| **2.** | **SYSTEM ANALYSIS** | | | 2 |
|  | 2.1 | PROBLEM DEFINITION | | 2 |
|  | 2.2 | EXISTING SYSTEM | | 2 |
|  |  | 2.2.1 | LIMITATIONS OF THE EXISTING SYSTEM | 2 |
|  | 2.3 | PROPOSED SYSTEM | | 3 |
|  |  | 2.3.1 | ADVANTAGES OF PROPOSED SYSTEM | 3 |
|  | 2.4 | FEASIBILITY STUDY | | 3 |
|  |  | 2.4.1 | ECONOMIC FESIBILITY | 4 |
|  |  | 2.4.2 | TECHNICAL FEASIBILITY | 4 |
|  |  | 2.4.3 | SOCIAL FEASIBILITY | 4 |
|  | 2.5 | HARDWARE & SOFTWARE REQUIREMENTS | | 5 |
|  |  | 2.5.1 | HARDWARE REQUIREMENTS | 5 |
|  |  | 2.5.2 | SOFTWARE REQUIREMENTS | 5 |
| **3.** | **ARCHITECTURE** | | | 6 |
|  | 3.1 | PROJECT ARCHITECTURE | | 6 |
|  | 3.2 | DESCRIPTION | | 7 |
|  | 3.3 | USECASE DIAGRAM | | 8 |
|  | 3.4 | CLASS DIAGRAM | | 9 |
|  | 3.5 | SEQUENCE DIAGRAM | | 10 |
|  | 3.6 | ACTIVITY DIAGRAM | | 11 |
| **4.** | **IMPLEMENTATION** | | | 12 |
|  | 4.1 | SAMPLE CODE | | 12 |
| **5.** | **SCREENSHOTS** | | | 15 |
| **6.** | **TESTING** | |  | 23 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 6.1 | INTRODUCTION TO TESTING | | 23 |
|  | 6.2 | TYPES OF TESTING | | 23 |
|  |  | 6.2.1 | UNIT TESTING | 23 |
|  |  | 6.2.2 | INTEGRATION TESTING | 23 |
|  |  | 6.2.3 | FUNCTIONAL TESTING | 24 |
|  | 6.3 | TEST CASES | | 24 |
|  |  | 6.3.1 | UPLOADING DATASET | 24 |
|  |  | 6.3.2 | CLASSIFICATION | 25 |
| **7.** | **CONCLUSION & FUTURE SCOPE** | | | 26 |
|  | 7.1 | PROJECT CONCLUSION | | 26 |
|  | 7.2 | FUTURE SCOPE | | 26 |
| **8.** | **BIBLIOGRAPHY** | |  | 27 |
|  | 8.1 | BIBLIOGRAPHY | | 27 |
|  |  |  | |  |

1. **INTRODUCTION**

**1.INTRODUCTION**

### PROJECT SCOPE

The project involves designing and implementing a framework for detecting spam in IoT devices using machine learning techniques. The framework uses a dataset that spans over a significant period, focusing on varying climatic conditions to enhance the accuracy of the spam detection in IoT devices.

### PROJECT PURPOSE The primary purpose is to improve the security and reliability of IoT devices by detecting and eliminating spam that may impact the effectiveness of smart homes and other IoT-driven systems. This is achieved through a machine learning-based approach that assigns a spam score to IoT devices based on their activity

### PROJECT FEATURES

* + - **Spam Detection Framework**: The framework uses five machine learning models to detect spam.
    - **Spamicity Score**: An algorithm computes the spamicity score for IoT devices based on input features.
    - **Dataset**: A comprehensive dataset from REFIT Smart Homes is used, ensuring a wide variety of input data to train and test the models.

1

# 2.SYSTEM ANALYSIS

## 2.SYSTEM ANALYSIS

**SYSTEM ANALYSIS** System Analysis is the important phase in the system development process. The System is studied to the minute details and analyzed. The system analyst plays an important role of an interrogator and dwells deep into the working of the present system. In analysis, a detailed study of these operations performed by the system and their relationships within and outside the system is done. A key question considered here is, “what must be done to solve the problem?” The system is viewed as a whole and the inputs to the system are identified. Once analysis is completed the analyst has a firm understanding of what is to be done.

### PROBLEM DEFINITION The problem addressed is detecting spam in IoT devices, which are vulnerable to spam or malicious activities due to the vast amount of data they produce and transmit. The existing systems use unsupervised machine learning techniques and reinforcement machine learning models to detect anomalies and DoS attacks but struggle with timely estimations due to resource constraints.

### EXISTING SYSTEM The current system leverages unsupervised machine learning for clustering and reinforcement learning for selecting security protocols, but it has challenges in processing IoT data effectively due to limited resources. It is prone to delays in detecting attacks and susceptible to various forms of compromise

#### LIMITATIONS OF EXISTING SYSTEM

* This job is challenging as it is usually difficult for an IoT system with limited resources to estimate the current network and timely attack status.
* Prone to attacks

### PROPOSED SYSTEM

The proposed system enhances IoT security by using a machine learning-based framework that computes a "spamicity score" to detect spam in IoT devices. It processes large, heterogeneous IoT data efficiently and evaluates models like Support Vector Machines and Random Forest for effective detection. The system is lightweight, energy-efficient, and improves device reliability by preventing malicious data. It also accounts for climatic variations to improve accuracy

### ADVANTAGES OF THE PROPOSED SYSTEM

The system is very simple in design and to implement. The system requires very low system resources and the system will work in almost all configurations. It has got following features

* + - * **Energy Efficiency**: The machine learning techniques used help build lightweight access  
         control protocols that conserve energy and extend the operational lifespan of IoT systems.
      * **Improved Data Management**: The system enhances the efficiency of IoT data   
        storage, processing, and retrieval, reducing the occurrence of spam and improving  
         data integrity.
      * **Enhanced Security**: By focusing on spam detection, the system significantly   
        reduces the risk of malicious information affecting IoT devices, thereby increasing  
         their reliability and trustworthiness.
      * **Adaptability**: The framework considers climatic variations, allowing it to adapt   
        to different environmental conditions, which enhances its effectiveness across  
         diverse scenarios.

### FEASIBILITY STUDY

The feasibility of the project is analyzed in this phase and business proposal is put forth with a very general plan for the project and some cost estimates. During system analysis the feasibility study of the proposed system is to be carried out. This is to ensure that the proposed system is not a burden to the company. Three key considerations involved in the feasibility analysis are

* Economic Feasibility
* Technical Feasibility
* Social Feasibility

### ECONOMIC FEASIBILITY

The developing system must be justified by cost and benefit. Criteria to ensure that effort is concentrated on project, which will give best, return at the earliest. One of the factors, which affect the development of a new system, is the cost it would require.

The following are some of the important financial questions asked during preliminary investigation:

* + - * The costs conduct a full system investigation.
      * The cost of the hardware and software.
      * The benefits in the form of reduced costs or fewer costly errors.

Since the system is developed as part of project work, there is no manual cost to spend for the proposed system. Also all the resources are already available, it give an indication of the system is economically possible for development.

### TECHNICAL FEASIBILITY

This study is carried out to check the technical feasibility, that is, the technical requirements of the system. Any system developed must not have a high demand on the available technical resources. The developed system must have a modest requirement, as only minimal or null changes are required for implementing this system.

### BEHAVIORAL FEASIBILITY

This includes the following questions:

* + - * Is there sufficient support for the users?
      * Will the proposed system cause harm?

The project would be beneficial because it satisfies the objectives when developed and installed. All behavioral aspects are considered carefully and conclude that the project is behaviorally feasible.

### HARDWARE & SOFTWARE REQUIREMENTS

* + 1. **HARDWARE REQUIREMENTS:**

Hardware interfaces specifies the logical characteristics of each interface between the software product and the hardware components of the system. Thefollowing are some hardware requirements.

|  |  |  |
| --- | --- | --- |
| * Processor | : | Intel i5 and Above. |
| * Hard disk | : | 40 GB. |
| * RAM | : | 4GB and Above. |

### SOFTWARE REQUIREMENTS:

Software Requirements specifies the logical characteristics of each interface and software components of the system. The following are some software requirements

* Operating system : Windows 7
* Languages : Python 3.8
* IDE : Jupyter

# ARCHITECTURE

## 3.ARCHITECTURE

### PROJECT ARCITECTURE

This project architecture shows the procedure followed for Spam Detection using machine learning, starting from input to final prediction.

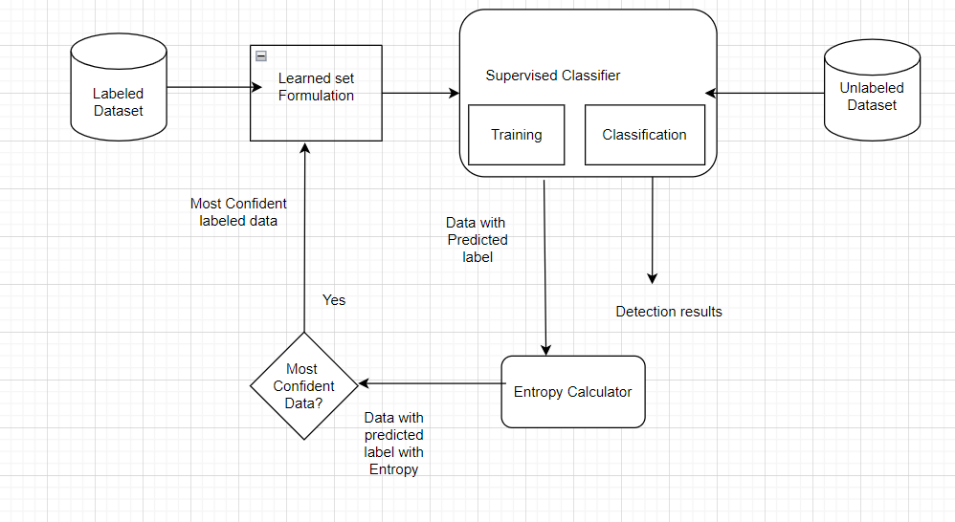


Figure 3.1: Project Architecture for efficient spam detection technique in IOT   
devices using ML.

### 3.2 DESCRIPTION

**Labeled Dataset Processing:**

* This module is responsible for handling the labeled dataset, where each data point is marked with a spam  
   classification (spam or no spam).
* **Input**: Labeled data containing features and corresponding spam labels.
* **Output**: A prepared dataset used for training the supervised classifier.

**Unlabeled Dataset Processing**:

* This module manages the unlabeled dataset, which includes data from IoT devices without predefined  
   spam classifications, enriching the learning context.
* **Input**: Unlabeled data from various IoT sources.
* **Output**: An integrated dataset that includes both labeled and unlabeled data for improved  
   detection capabilities.  
    
    
    
   **Supervised Classifier**:
* The supervised classifier module processes the labeled dataset to train the machine learning models,  
   learning to identify patterns indicative of spam activity.
* **Input**: Labeled dataset.
* **Output**: A trained model capable of classifying incoming data points.  
    
    
   **Entropy Calculator**:
* This module evaluates the confidence of the classifier's predictions. If the confidence score meets a  
   specified threshold, the prediction is deemed reliable.
* **Input**: Predictions from the supervised classifier.
* **Output**: Confidence scores that determine the reliability of the classifications.  
    
   **Learned Set Formulation**:
* This module integrates confident predictions into the model's knowledge base, enhancing its ability  
   to recognize spam in future data streams.
* **Input**: Confident predictions from the entropy calculator.
* **Output**: An updated learned set that improves the classifier's overall accuracy and adaptability.

### USE CASE DIAGRAM

The diagram illustrates the architecture of a spam detection system in IoT devices, highlighting key interactions and processes. The **User** interacts with two main modules: handling labeled and unlabeled datasets. The labeled data is used to train a **Supervised Classifier**, which classifies incoming data points. The classified data is then evaluated by the **Entropy Calculator** to assess the confidence of the predictions. Finally, confident predictions are sent to the **Learned Set Formulation**, where they are integrated into the model's knowledge base to enhance its accuracy in future spam detection.

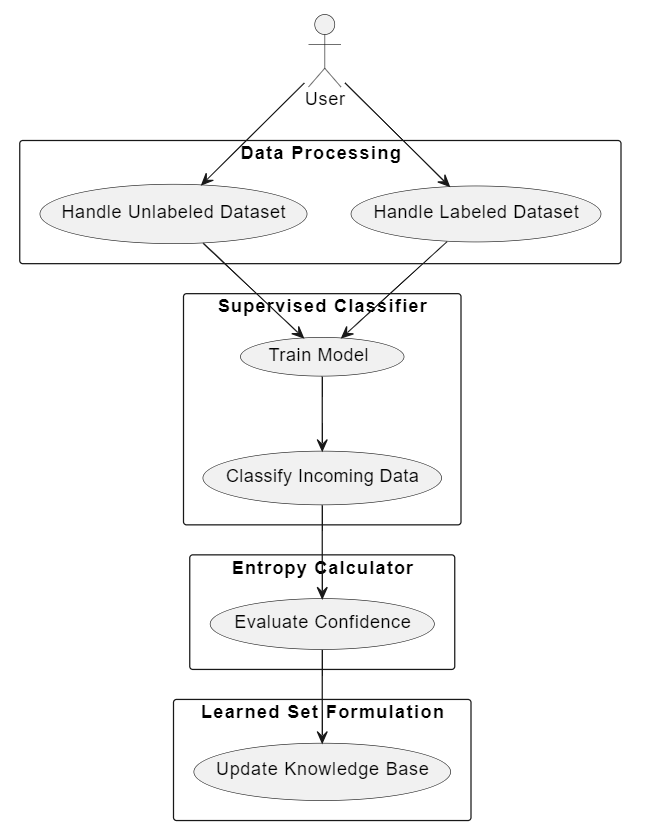


Figure 3.2: Use Case Diagram for Efficient spam detection technique in IOT devices using ML.

### CLASS DIAGRAM

Class Diagram is a collection of classes and objects.

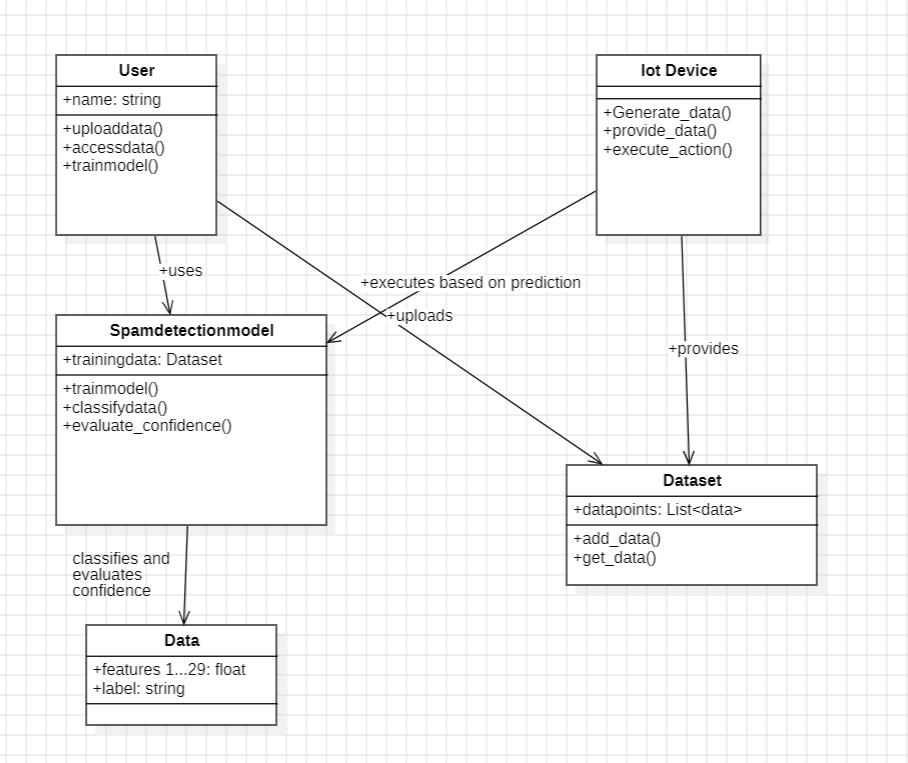


Figure 3.3:Class Diagram for Efficient spam detection technique in IOT devices using ML.

### SEQUENCE DIAGRAM

Figure 3.4:Sequence Diagram for Efficient spam detection technique in IOT devices using ML.

### ACTIVITY DIAGRAM

It describes about flow of activity states.

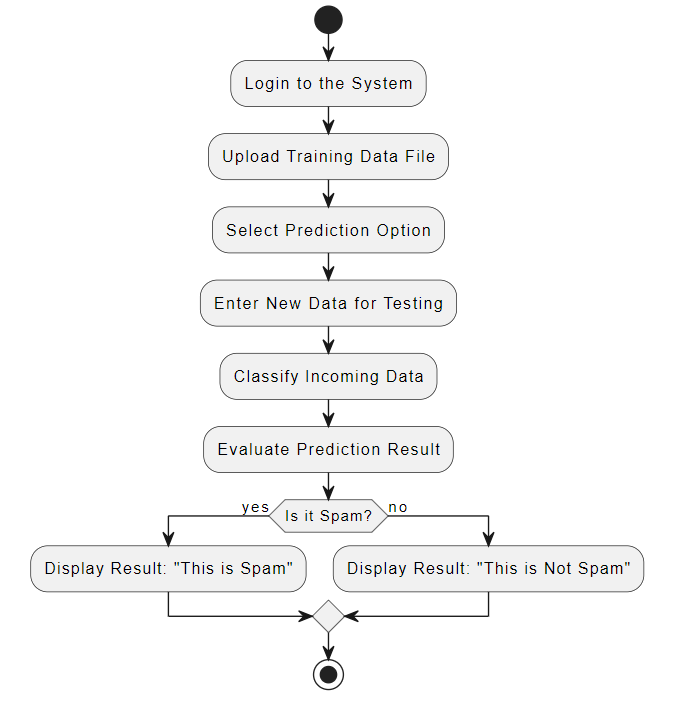


Figure 3.5: Activity Diagram for Efficient spam detection technique in IOT devices using ML.

# IMPLEMENTATION

### IMPLEMENTATION

**4.1 SAMPLE CODE  
  
app.py**import numpy as np

import pandas as pd

from flask import Flask, request, jsonify, render\_template, redirect, flash, send\_file

from sklearn.preprocessing import MinMaxScaler

from werkzeug.utils import secure\_filename

import pickle

import numpy as np

import pandas as pd

from sklearn.tree import DecisionTreeClassifier

from sklearn.ensemble import RandomForestClassifier, BaggingClassifier, AdaBoostClassifier, VotingClassifier

app = Flask(\_\_name\_\_) #Initialize the flask App

#forest = pickle.load(open('boosting.pkl','rb'))

model = pickle.load(open('spam.pkl', 'rb'))

@app.route('/')

@app.route('/index')

def index():

    return render\_template('index.html')

@app.route('/chart')

def chart():

    return render\_template('chart.html')

#@app.route('/future')

#def future():

#   return render\_template('future.html')

@app.route('/login')

def login():

    return render\_template('login.html')

@app.route('/upload')

def upload():

    return render\_template('upload.html')

@app.route('/preview',methods=["POST"])

def preview():

    if request.method == 'POST':

        dataset = request.files['datasetfile']

        df = pd.read\_csv(dataset,encoding = 'unicode\_escape')

        df.set\_index('Id', inplace=True)

        return render\_template("preview.html",df\_view = df)

#@app.route('/home')

#def home():

 #   return render\_template('home.html')

@app.route('/prediction', methods = ['GET', 'POST'])

def prediction():

    return render\_template('prediction.html')

#@app.route('/upload')

#def upload\_file():

#   return render\_template('BatchPredict.html')

@app.route('/predict',methods=['POST'])

def predict():

    int\_feature = [x for x in request.form.values()]

    final\_features = [np.array(int\_feature)]

    result=model.predict(final\_features)

    if result == 1:

            result = "Spam detected"

    else:

        result = 'No spam'

    return render\_template('prediction.html', prediction\_text= result)

@app.route('/performance')

def performance():

    return render\_template('performance.html')

if \_\_name\_\_ == "\_\_main\_\_":

    app.run(debug=True)

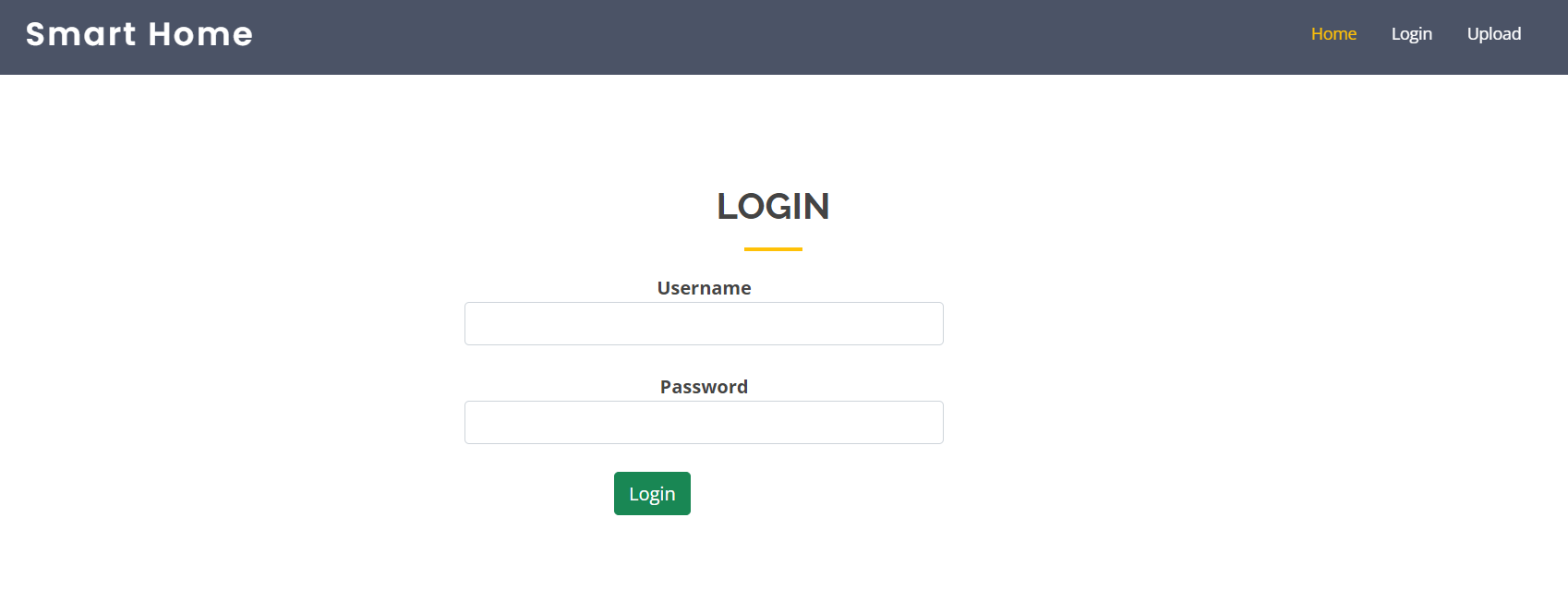
# SCREENSHOTS

### HOME PAGE



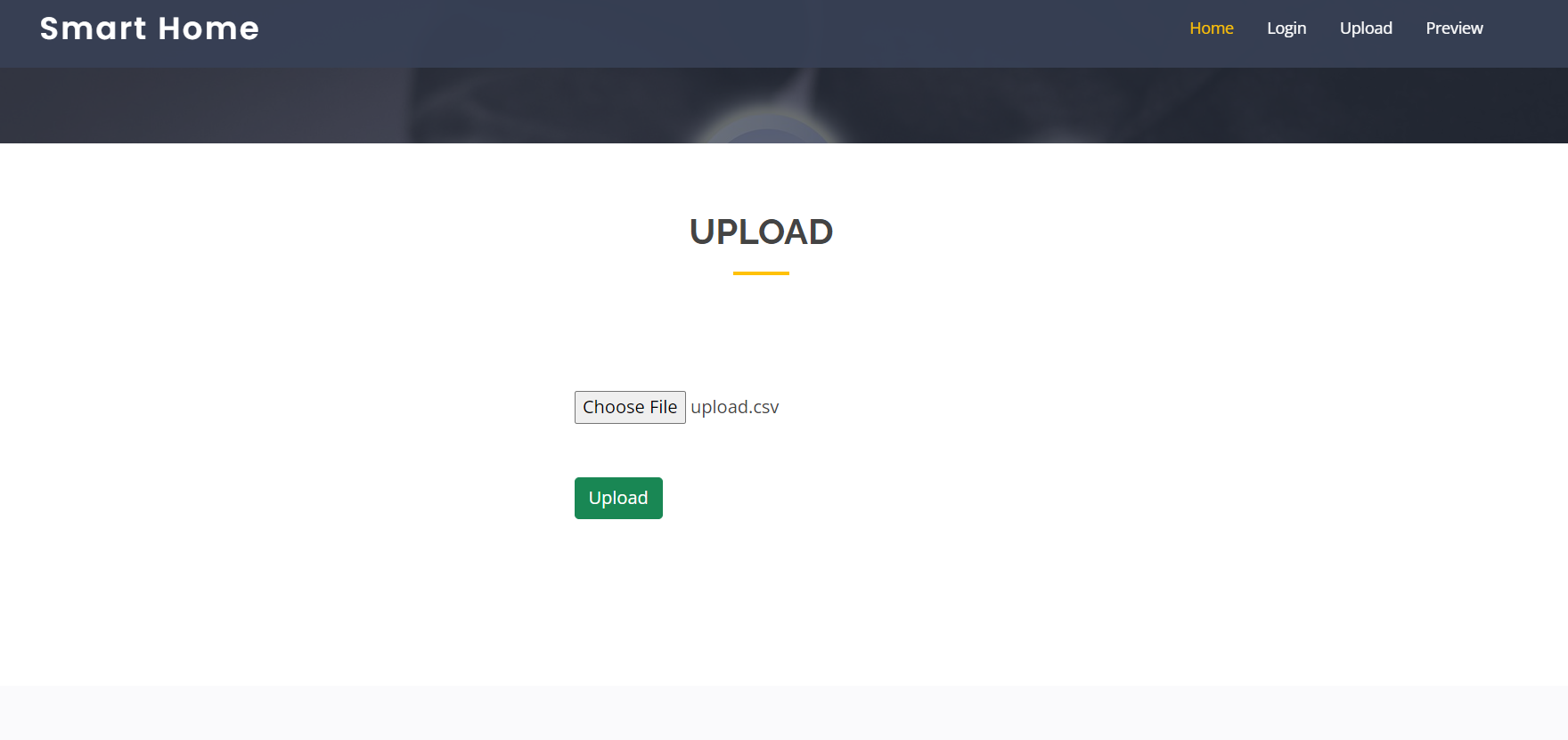
Screenshot 5.1: Home page of efficient Spam Detection technique for IOT devices  
 using ML.

### LOGIN PAGE



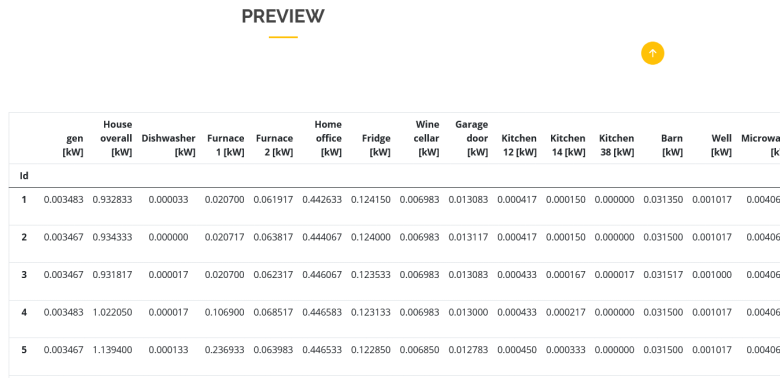
Screenshot 5.2: Login page of efficient Spam Detection technique for IOT devices

### UPLOADING DATA

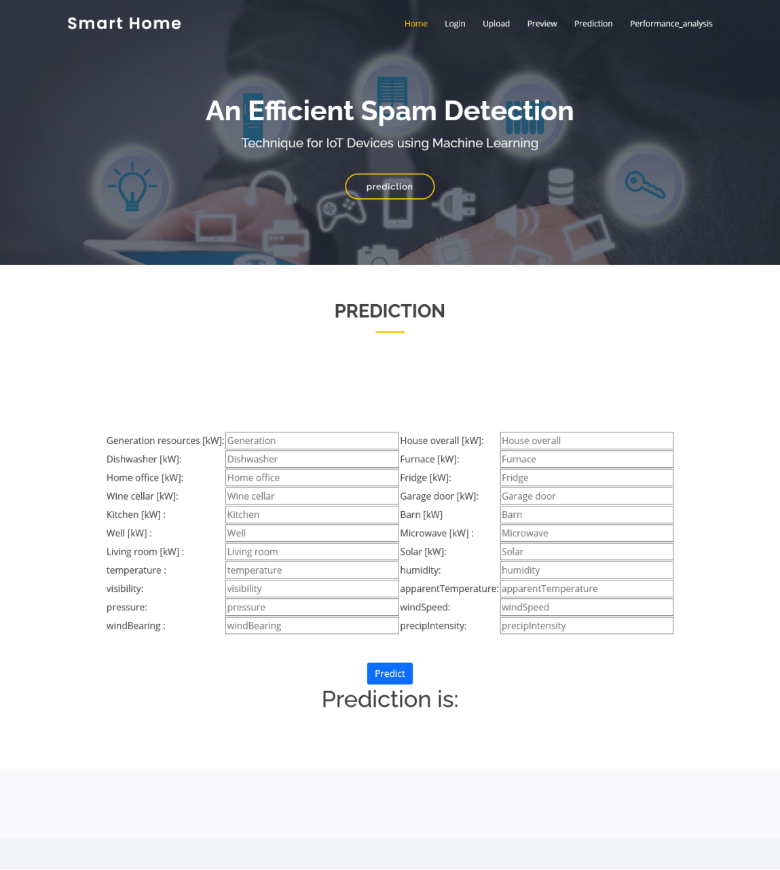


Screenshot 5.3: uploading dataset for training the model.

### PREVIEW DATA

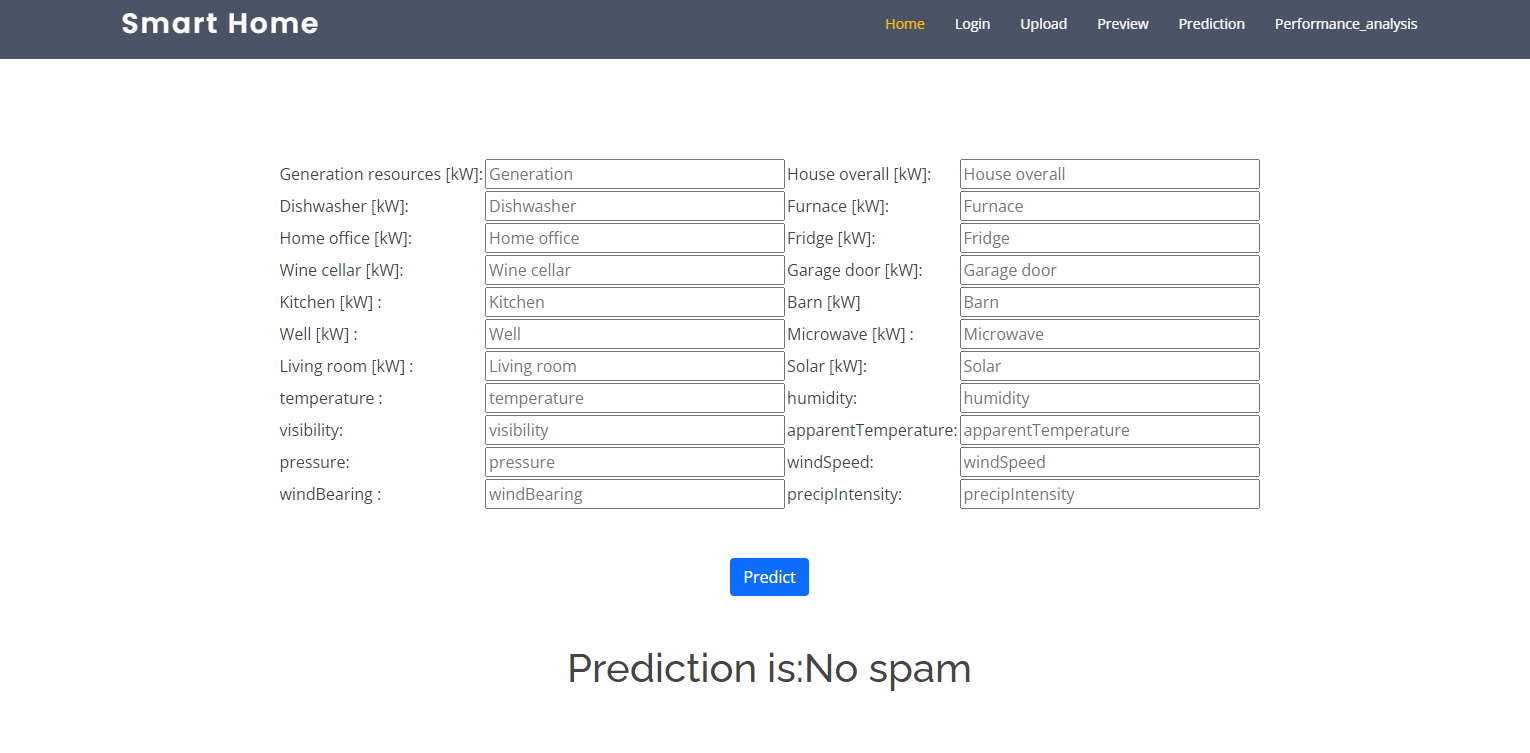


Screenshot 5.4:Previewing the inserted data.

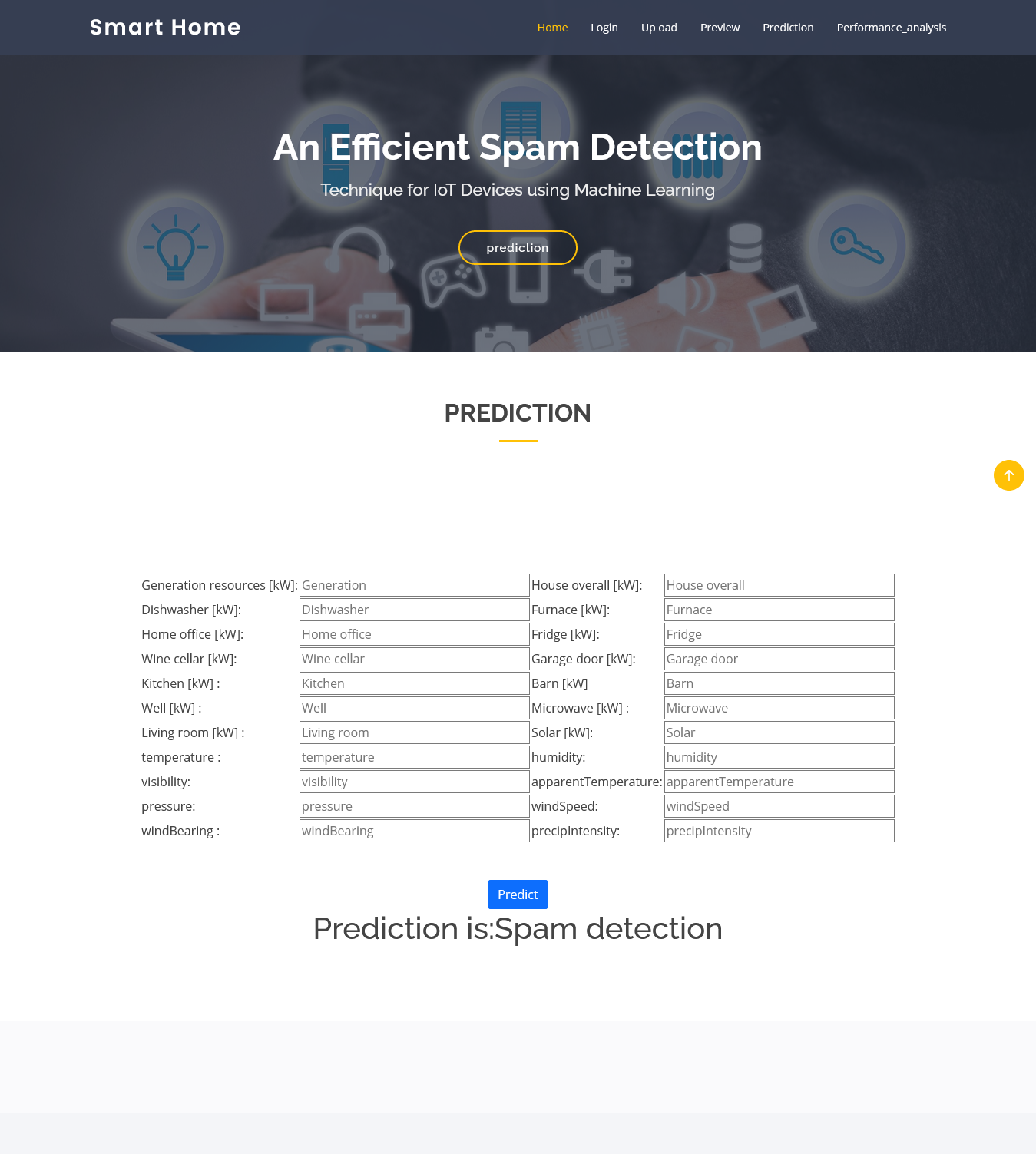
5.5 PREDICTION

Screenshot 5.5: Prediction of data

5.6 OUTPUT

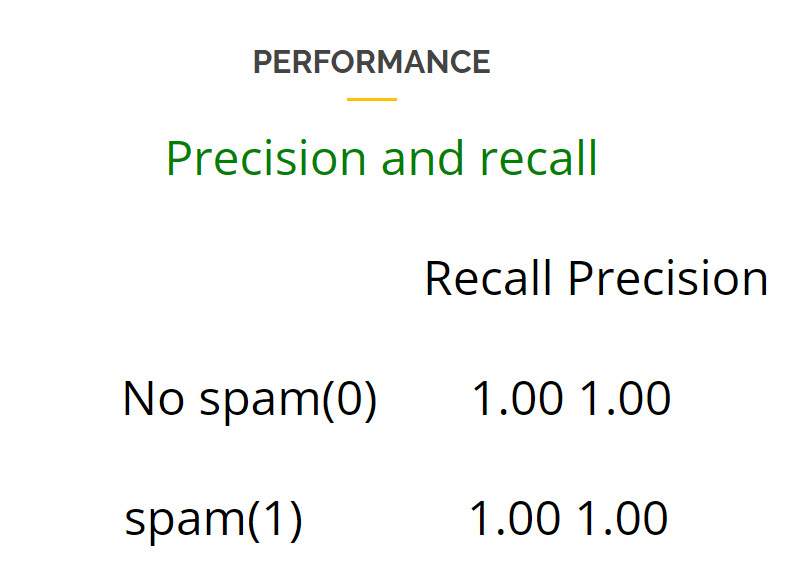


Screenshot5.6.1:output for no spam

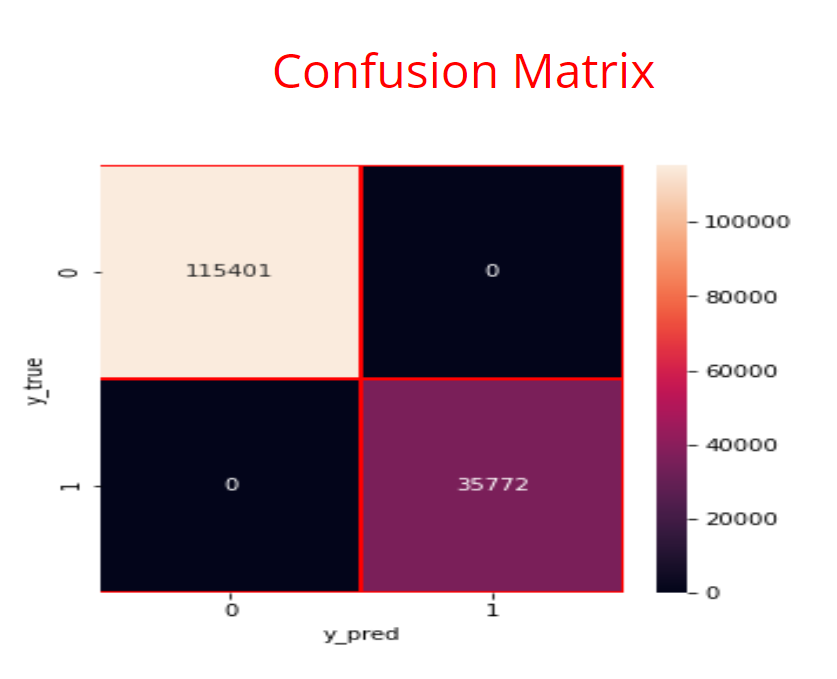


Screenshot5.6.2:output for spam.

5.7:Performance



Screenshot5.7.1:precision and recall

  
   
 Screenshot5.7.2:Confusion matrix

# TESTING

## TESTING

### INTRODUCTION TO 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.

### TYPES OF TESTING

* + 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.

### 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.

### FUNCTIONAL TESTING

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.

### TEST CASES

* + 1. **UPLOADING DATASET**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Test case ID | Test case name | Purpose | Test Case | Output |
| 1 | User uploads dataset | Use it for Train and predict | The user uploads the dataset | Uploaded successfully |
| 2 | User clicks on train and test the model | Use it to split the data into training and testing | The user splits the data into two parts one is for training and other for testing | Train Test Model successfully created |

* + 1. **CLASSIFICATION**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Test case ID | Test case name | Purpose | Input | Output |
| 1 | Classification test 1 | To check if the classifier performs its task | A data with Spam is givan | Spam is predicted. |
| 2 | Classification test 2 | To check if the classifier performs its task | A Normal data is given | It predicted as Not Spam. |

**CONCLUSION**

**CONCLUSION & FUTURE SCOPE**

* 1. **PROJECT CONCLUSION**

The spam detection system for IoT devices successfully implements machine learning algorithms to identify and mitigate spam activity. By leveraging labeled and unlabeled datasets, the system enhances the reliability of IoT devices, ensuring the integrity of data transmission. The integration of various machine learning models, coupled with robust evaluation mechanisms, has demonstrated a significant improvement in the accuracy of spam detection. The user-friendly interface allows for seamless interaction, empowering users to upload data, initiate predictions, and access results efficiently.

### FUTURE SCOPE

The future scope of the spam detection system includes implementing real-time data processing to provide instant feedback on spam detection as IoT devices generate data. Enhancing the model with advanced machine learning techniques, such as deep learning, will improve classification accuracy and adaptability to new spam types. Additionally, developing dynamic learning capabilities will allow the system to continuously update its knowledge base based on incoming data. Integration with broader IoT security frameworks will provide a comprehensive solution, while user customization options for spam detection thresholds will enhance flexibility and user experience.

# BIBLIOGRAPHY

## 8. BIBLIOGRAPHY

### REFERENCES

* Z.-K. Zhang, M. C. Y. Cho, C.-W.Wang, C.-W.Hsu, C.-K. Chen, and S. Shieh, “Iot security: ongoing challenges and research opportunities,”in 2014 IEEE 7th international conference on service-oriented computing and applications. IEEE, 2014, pp. 230–234.
* A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, “Blockchain for iot security and privacy: The case study of a smart home,” in 2017 IEEE international conference on pervasive computing and IEEE, 2017, pp. 618–623.
* E. Bertino and N. Islam, “Botnets and internet of things security,”Computer, no. 2, pp. 76–79, 2017.
* C. Zhang and R. Green, “Communication security in internet of thing:preventive measure and avoid ddos attack over iot network,” in Proceedings of the 18th Symposium on Communication

**8.2**  **GITHUB LINK  
  
 [https://github.com/Theachiever05/An-Efficient-Spam- detectection-techniques-for-IOT-devices-using- MachineLearning/upload/main](https://github.com/Theachiever05/An-Efficient-Spam-detectection-techniques-for-IOT-devices-using-MachineLearning/upload/main)**