**NAAN MUDHALVAN PROJECT REPORT**

**ON**

**“OPTIMIZING SPAM FILTERING WITH MACHINE LEARNING”**

Submitted in partial fulfillment of the requirements for the

award of the degree of

**BACHELOR OF SCIENCE IN**

**COMPUTER SCIENCE**

**SUBMITTED BY**

**TEAM LEADER**

**PUVANESH C**(Reg no. 20201371506127)

**TEAM MEMBERS**

**RAJA MUTHULAKSHMI T**(Reg no 20201371506128)

**SAKTHI MARI M(**Reg no. 20201371506132)

**SANGEETHA M(**Reg no.20201371506133)

****

**Department of Computer Science**

**Government Arts and Science College for Women – Alangulam**

**Tenkasi – 627851 April 2023**

1. **Introduction**
   1. **– Overview**

Optimizing spam filtering is a machine learning project that involves algorithms to automatically classify incoming SMS spam or legitimate messages, from reaching the user’s inbox. The goal is to accurately filter out unwanted messages and minimize false positives, while ensuring that important messages are not mistakenly labeled as spam.

* 1. **- Purpose**

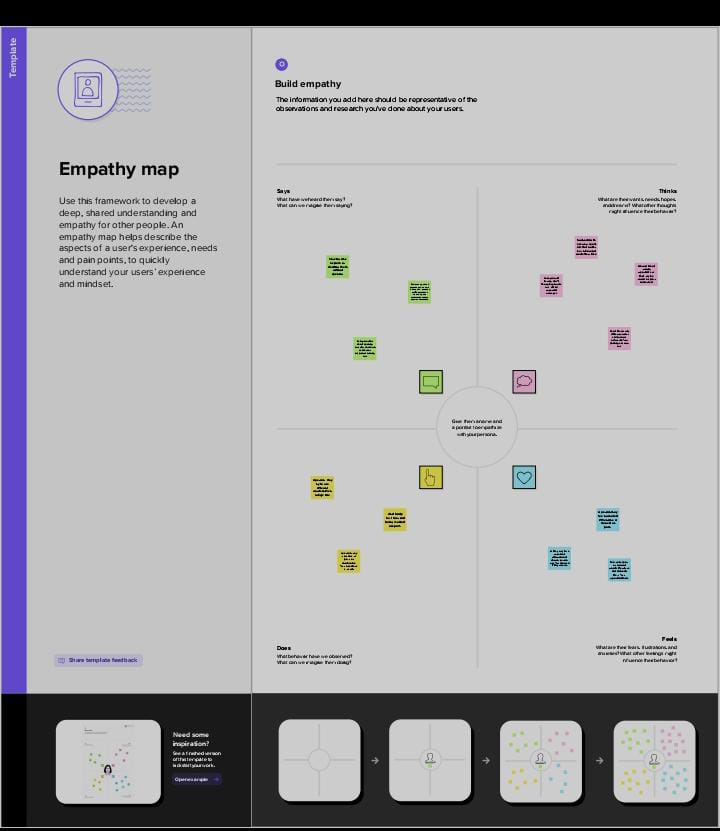
To achieve this, the project typically involves gathering a large dataset of messages that have already been classified as either spam or not-spam. This dataset is used to train a machine learning model, which can then classify new incoming messages based on their content and other features such as the sender's address, subject line, and attachments.

The machine learning model is typically trained using a variety of techniques, such as natural language processing (NLP), statistical modeling, and deep learning algorithms. The model is continuously updated and optimized based on feedback from users, which helps to improve its accuracy over time.

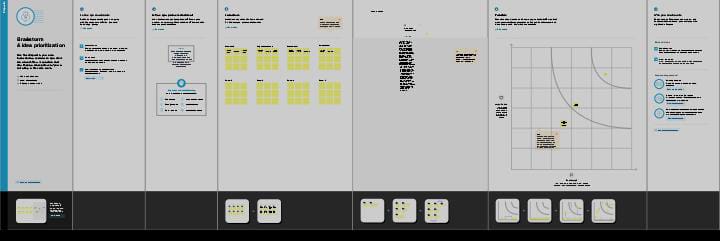
The ultimate goal of the project is to create a spam filter that is highly effective at identifying and blocking unwanted messages, while minimizing false positives and ensuring that important messages are not mistakenly flagged as spam. This can help to improve productivity and reduce the risk of security threats, such as phishing scams and malware infections.

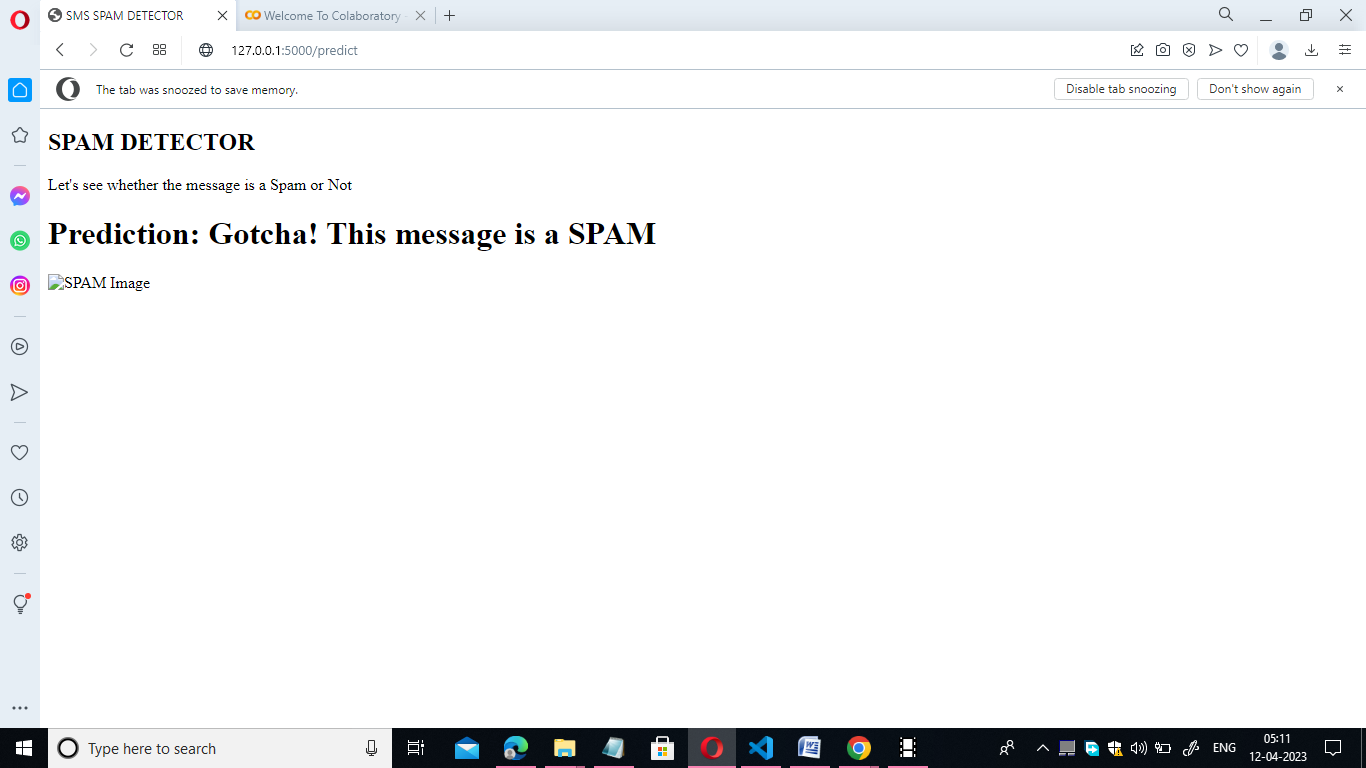
1. **PROBLEM DEFINITION & DESIGN THINKING**

**2.1. Empathy Map**

****

**2.2. Ideation & Brainstorming Map**

**3. Result**

****

1. **Advantage and Disadvantages**

**Advantages:**

* Saves time and resources by automating the process of identifying and filtering unwanted messages which can be time-consuming and tedious for humans to do manually.
* Helps to protect against phishing scams, malware, and other security threats that can be delivered through spam messages and emails.
* Improves the user experience by reducing the amount of unwanted messages that the users have to sort through.

**Disadvantages:**

* There is always a risk of false positives or false negatives, which can result in legitimate messages being incorrectly filtered as spam messages .
* Over-aggressive spam filtering can lead to legitimate messages being incorrectly flagged as spam, resulting in important messages being missed.
* Some users may find spam filtering to be intrusive or may be concerned about privacy issues related to the automated analysis of their messages .

**5. APPLICATIONS**

Spam filtering algorithms are used in a variety of applications to automatically identify and remove unwanted or unsolicited messages, emails, or other types of communication.

1. **SMS:** Spam filtering algorithms are used in SMS messaging services to identify and block unsolicited or fraudulent text messages.
2. **Email:** Spam filtering algorithms are commonly used in email clients and servers to automatically filter out unwanted or unsolicited emails, such as promotional emails or phishing scams.
3. **Social media:** Social media platforms use spam filtering algorithms to detect and remove spammy comments or messages that violate community guidelines.
4. **Network security:** Spam filtering algorithms are used in network security applications to identify and block emails and other communication that may contain viruses or malware.
5. **Online advertising:** Spam filtering algorithms are used in online advertising platforms to detect and remove fraudulent or low-quality ads that may be misleading or harmful.
6. **Mobile apps:** Spam filtering algorithms are used in mobile apps to identify and remove spammy or low-quality user-generated content.

**6.CONCLUSION**

In this project, I have used the Kaggle Spam dataset . I have used four models to find the accuracy. The models are Decision tree, Random forest, Naïve Bayes and ANN. Among these models ANN gives the best accuracy rate of 99% . So, I have used ANN to predict my Message as spam or non spam. And then I have build the python code and imported flask to direct the webpages.

Home and Result are the two html file that I have Created. And atlast, my model has predicted its correct output.

**7.FEATURE SCOPE :**

* **Machine learning algorithms**: One effective approach to spam filtering is to use machine learning algorithms to detect patterns in spam messages. By analyzing large amounts of spam data, these algorithms can learn to recognize common characteristics of spam messages and filter them out.
* **Natural Language Processing (NLP):** NLP techniques can be used to identify the semantic structure of messages and detect any indications of spam messages. It can also be used to recognize patterns in the text that may indicate whether or not a message is spam.
* **Email header analysis**: Analyzing the email header information can provide important clues as to whether a message is spam or not. By examining the sender’s IP address, email domain, and other header information, it is possible to identify and block known spam sources.
* **Real-time blacklists**: A real-time blacklist (RBL) is a list of known spamming sources that is constantly updated. By incorporating an RBL into a spam filter, the system can quickly identify and block messages from known spammers.
* **Bayesian filtering**: Bayesian filtering is a statistical technique that can be used to filter spam based on the probability that a message is spam. By analyzing the text and other characteristics of a message, Bayesian filtering can calculate the probability that it is spam and block it accordingly.
* **Sender reputation:** Sender reputation is a measure of the trustworthiness of an email sender. By analyzing the history of emails sent by a particular sender, it is possible to identify and block messages from senders with a history of sending spam.
* **User feedback:** User feedback can be used to improve the effectiveness of a spam filter over time. By allowing users to mark messages as spam or not spam, the system can learn from these ratings and improve its accuracy..

8.APPENDIX:

