HOPE FOUNDATION

FINOLEX ACADEMY OF MANAGEMENT AND TECHNOLOGY
DEPARTMENT OF INFORMATION TECHNOLOGY

EMAIL MONITORING SYSTEM

Presented By –

Mhadgut Asavari Pradeepkumar - 36

Nalawade Sayali Umesh - 46

Ranshur Pratiksha Dilip - 64

Guided By –

Prof. Atiya Kazi

CONTENTS

- ❖ **Problem Statement**
- ❖ **Literature Review**
- ❖ **Existing System**
- ❖ **Proposed System**
- ❖ **System Architecture**
- ❖ **Flowchart**
- ❖ **Algorithms**
- ❖ **System Requirement**
- ❖ **Conclusion**

PROBLEM STATEMENT

Email Spam has become a major problem nowadays , with rapid growth of internet users . Spam email are the messages sent to multiple addresses . People are using them for illegal and unethical conducts such as phishing and frauds .

So it is needed to identify those spam mails which are fraud .

Using Email Monitoring System , spam and non-spam emails are classified using ML algorithm like Naïve Bayes and KNN and Logistic Regression .

LITERATURE REVIEW

Paper	Features
Email based spam detection	In this spam classification is created using Bayes theorem and Naïve Bayes classifier and also IP addresses of the sender are often detected. And its accuracy is 97% .
Spam email using Naïve Bayes Classifier	In this, it creates spam Email classification using Naïve Bayes Algorithm and the accuracy is 99%. Also calculates error rate.
Existing Email Spam Filtering Method	In this the system Uses Machine Learning techniques like Naïve Bayes, KNN, SVM and summarizes overall scenario regarding Accuracy Rate.
Email spam filtering using ML	It compares implemented algorithm of XGboosting Classifier with existed classifier of SVM, Naïve Bayes and its accuracy is 95%
Machine Learning Techniques for spam Email	It implements spam detection by using Machine learning and deep Learning Techniques like Naïve Bayes, Decision Tree, Neural Networks and Random forest.

EXISTING SYSTEM

❖ **The Existing Email system has a weak spam detection Mechanism.**

        This results in segregation of important emails into spam emails.

        This can lead to misscommunication or delay of messages.

❖ **Sometimes some unimportant or phishing emails are not segregated into spam folder which leads unnecessary attention to unimportant emails .**
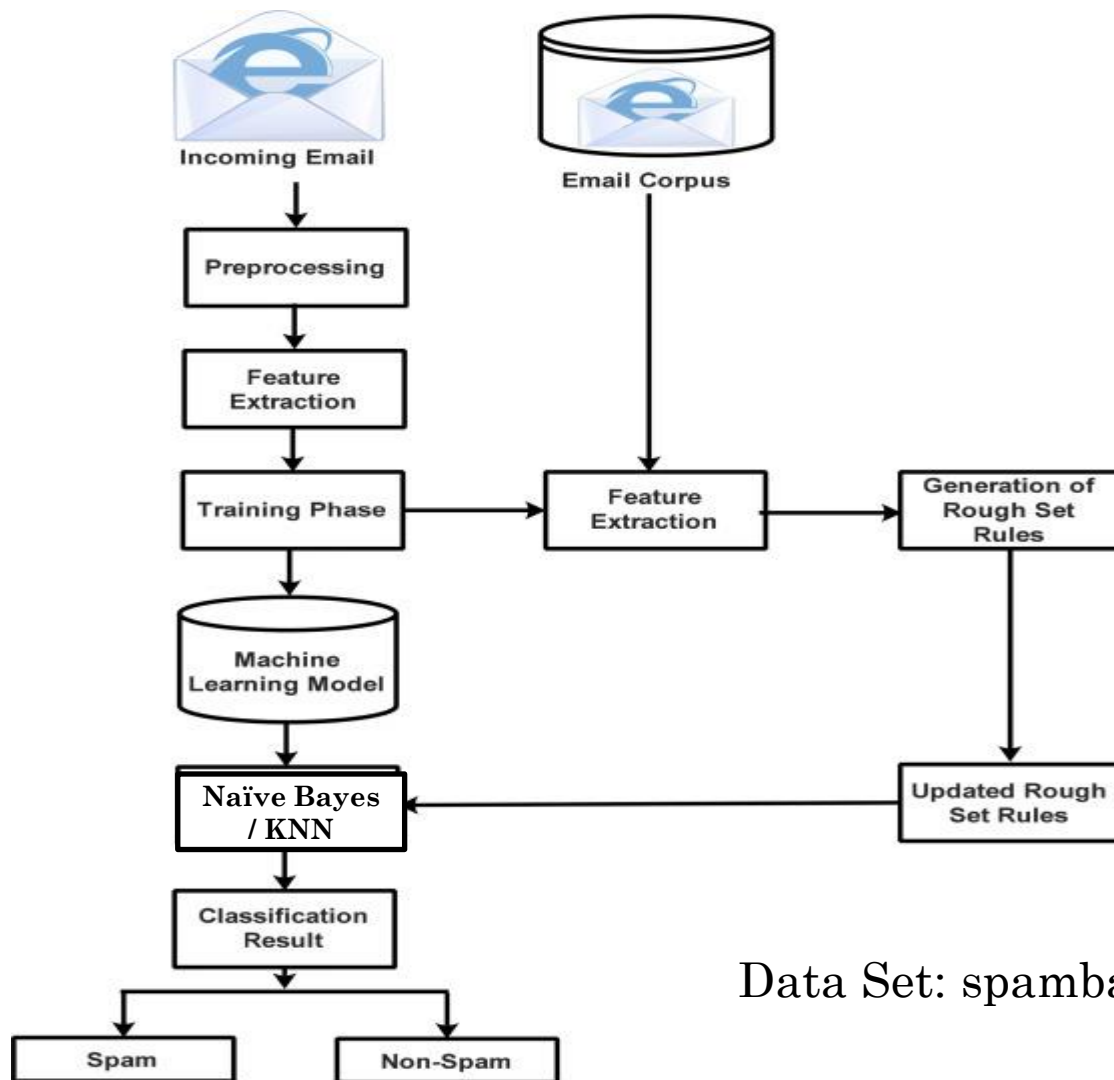
PROPOSED SYSTEM

In this system to solve the problem of spam , email monitoring system is implemented using machine learning algorithms like Naive Bayes and KNN and accuracy of both these algorithms is compared .

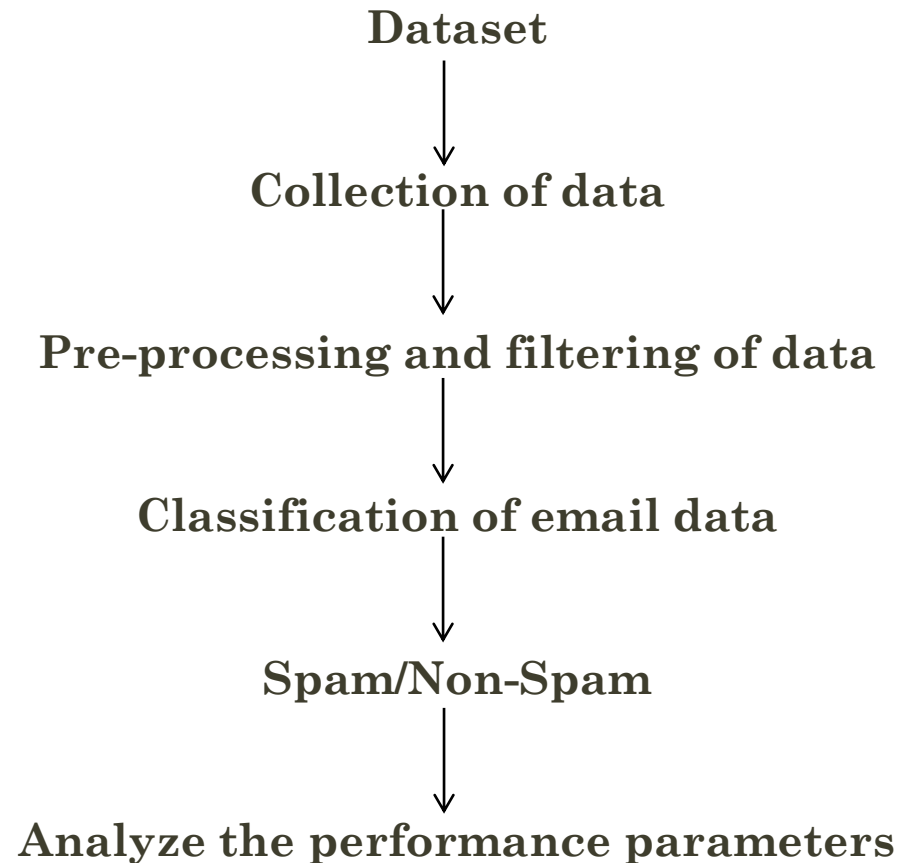Using this system the problem of existing system is been solved.

SYSTEM ARCHITECTURE

Data Set: spambase.csb

FLOWCHART

Dataset

↓

Collection of data

↓

Pre-processing and filtering of data

↓

Classification of email data

↓

Spam/Non-Spam

↓

Analyze the performance parameters

ALGORITHMS

- ❖ Naïve Bayes
- ❖ KNN (K – Nearest Neighbor)
- ❖ Logistic Regression

These are supervised ML algorithm used for classification problems .

Naïve Bayes is based on Bayes theorem which uses probability formula :

$$P(A|B) = \frac{P(B|A) \cdot P(A)}{P(B)}$$

KNN is based on similarity which uses Euclidean distance formula :

$$\sqrt{(X1 - X2)^2 + (Y1 - Y2)^2}$$

Logistic regression represent by the following formula :

Logit(pi) = 1/(1+ exp(-pi)) ln(pi/(1-pi)) = Beta_0 + Beta_1*X_1 + … + B_k*K_k

SYSTEM REQUIREMENT

❖ **HARDWARE REQUIREMENTS :**

Operating system : Windows

RAM : 8 GB(minimum requirement)

Hard Disk : 1GB working space (minimum requirement)

❖ **SOFTWARE REQUIREMENT:**

Languages : Python

Tools : Google Colab / PyCharm, VS code , Flask

CONCLUSION

We will implement email monitoring system using Machine Learning Algorithms such as Naive Bayes Algorithm and KNN (K-Nearest Neighbor) and Linear Regression Algorithm and compare which is better .

THANK YOU