# SMS SPAM DETECTION

AN INDUSTRY ORIENTED MINI PROJECT REPORT

Submitted to

**JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY,**

**HYDERABAD**

In Partial fulfilment of the requirements for the award of the degree of

**BACHELOR OF TECHNOLOGY**

**IN**

**COMPUTER SCIENCE AND ENGINEERING**

Submitted by

| | |
|---|---|
| **ALLA AKHILA** | **19UK1A0519** |
| **PALAKURTHI NITHIN** | **19UK1A0521** |
| **KUDURUPAKA ANUSHA** | **19UK1A0555** |
| **UPPULA SUSMITHA** | **19UK1A0523** |

Under the esteemed guidance of

**Mr. N. Sravan Kumar**

(Assistant Professor)

**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING**

**VAAGDEVI ENGINEERING COLLEGE**

(Affiliated to JNTUH, Hyderabad)

Bollikunta,Warangal-506005

**2019-2023**

**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING**
**VAAGDEVI ENGINEERING COLLEGE**
**BOLLIKUNTA, WARANGAL –506005**

**2019-2023**

## CERTIFICATE OF COMPLETION UG PROJECT PHASE-1

This is to certify that the UG Project Phase-1 entitled “**SMS SPAM DETECTION**” is being submittedby**A.AKHILA(H.NO:19UK1A0519),U.SUSMITHA(H.NO:19UK1A0 523),P.NITHIN(19UK1A0521),K.ANUSHA(19UK1A0555)** in partial fulfilment of the requirements for the award of the degree of Bachelor of Technology in Computer Science and Engineering to Jawaharlal Nehru Technological University Hyderabad during the academic year 2022-2023,is a record of work carried out by them under the guidance and supervision.

**Project Guide**
**Mr. N. Sravan Kumar**
(Assistant professor)

**Head of the Department**
**Dr. R. Naveen Kumar**
(Professor)

**External**

# ACKNOWLEDGEMENT

We wish to take this opportunity to express our sincere gratitude and deep sense of respect to our beloved **Dr.P.PRASAD RAO,** Principal, Vaagdevi Engineering College for making us available all the required assistance and for his support and inspiration to carry out this UG Project Phase-1 in the institute.

We extend our heartfelt thanks to **Dr.R.NAVEEN KUMAR**, Head of the Department of CSE, Vaagdevi Engineering College for providing us necessary infrastructure and thereby giving us freedom to carry out the UG Project Phase-1.

We express heartfelt thanks to Smart Bridge Educational Services Private Limited, for their constant supervision as well as for providing necessary information regarding the UG Project Phase-1 and for their support in completing the UG Project Phase-1.

We express heartfelt thanks to the guide, **Mr.N.SRAVAN KUMAR** Assistant professor, Department of CSE for his constant support and giving necessary guidance for completion of this UG Project Phase-1.

Finally, we express our sincere thanks and gratitude to my family members, friends for their encouragement and outpouring their knowledge and experience throughout the thesis.

| | |
|---|---|
| **ALLA AKHILA** | **(19UK1A0519)** |
| **PALAKURTHI NITHIN** | **(19UK1A0521)** |
| **KUDURUPAKA ANUSHA** | **(19UK1A0555)** |
| **UPPULA SUSMITHA** | **(19UK1A0523)** |

# ABSTRACT

In this technological era the use of gadgets such as cell phone has expanded, Short Message Service (SMS) has developed into a multi-billion dollar industry. Simultaneously, a decrease in the expense of informing administrations has brought about development in spontaneous business promotions (spams) being shipped off cell phones. In pieces of Asia, up to 30% of instant messages were spam in 2012.The absence of genuine information bases for SMS spam, a short length of messages and restricted highlights, and their casual language are the variables that may cause the setup email sifting calculations to fail to meet expectations in their order. In this undertaking, a data set of genuine SMS Spam store is utilized, and subsequent to preprocessing and highlight extraction, distinctive AI methods are applied to the information base. SMS spam filtering is a comparatively recent errand to deal such a problem. It inherits many concerns and quick fixes from Email spam filtering. However it fronts its own certain issues and problems at last, the outcomes are thought about and the best calculation for spam sifting for text informing is presented. Keywords- SMS, spam detection, machine learning, algorithms, Artificial intelligence.

## TABLE OF CONTENTS:-

The areas where this solution can be applied.

## 9. CONCLUSION

Conclusion summarizing the entire work and findings.

## 10. FUTURE SCOPE

Enhancements that can be made in the future.

## 11. BIBILOGRAPHY

References of previous works or websites visited/books refered for analysis about the project , solution previous findings etc.

## APPENDIX

A Source Code

Attach the code for the solution built

# 1.INTRODUCTION

## 1.1 Overview

SMS is one of the most effective forms of communication. It is based on cellular communication system, just the cell phone needs to be in the network coverage area in order to send or receive the message. Almost everyone is using this service for communication. Various organizations deal with SMS for communicating with their clients/customers, banks and other government organization also use SMS for communication. Also, many business organizations use this service for advertising purposes. Thus, SMS is playing a vital role, as active internet connection is not required at all in this framework.

## 1.2 Purpose

The growth of mobile phone users has lead to a dramatic increasing of SMS spam messages. Recent reports clearly indicate that the volume of mobile phone spam is dramatically increasing year by year. In practice, fighting such plague is difficult by several factors, including the lower rate of SMS that has allowed many users and service providers to ignore the issue, and the limited availability of mobile phone spam-filtering software. Probably, one of the major concerns in academic settings is the scarcity of public SMS spam datasets, that are sorely needed for validation and comparison of different classifiers. Moreover, traditional content-based filters may have their performance seriously degraded since SMS messages are fairly short and their text is generally rife with idioms and abbreviations. In this paper, we present details about a new real, public and non-encoded SMS spam collection that is the largest one as far as we know. Moreover, we offer a comprehensive analysis of such dataset in order to ensure that there are no duplicated messages coming from previously existing datasets, since it may ease the task of learning SMS spam classifiers and could compromise the evaluation of methods. Additionally, we compare the performance achieved by several established machine learning techniques. Im summary, the results indicate that the procedure followed to build the collection does not lead to near-duplicates and, regarding the classifiers, the Support Vector Machines outperforms other evaluated techniques and, hence, it can be used as a good baseline for further comparison.

# 2.LITERATURE SURVEY

## 2.1 Existing problem

Most existing approaches to combating SMS spam were exported from successful email anti-spam solutions (Wang et al., 2010). However, not all solutions to email spam are applicable to SMS due to the small message size of 140 byte (160 English Alphabet characters), lack of some information such as edit format, header and Multi-purpose Internet Mail Exchanger (MIME), use of unstandardized abbreviation and acronyms and lastly, support for only textual representation. Spam filter have been deployed in either the client side (user mobile phone) or the server side (mobile network operators‟ side) or at both ends (client and server side approach). The basic idea of spam filtering is shown in figure.

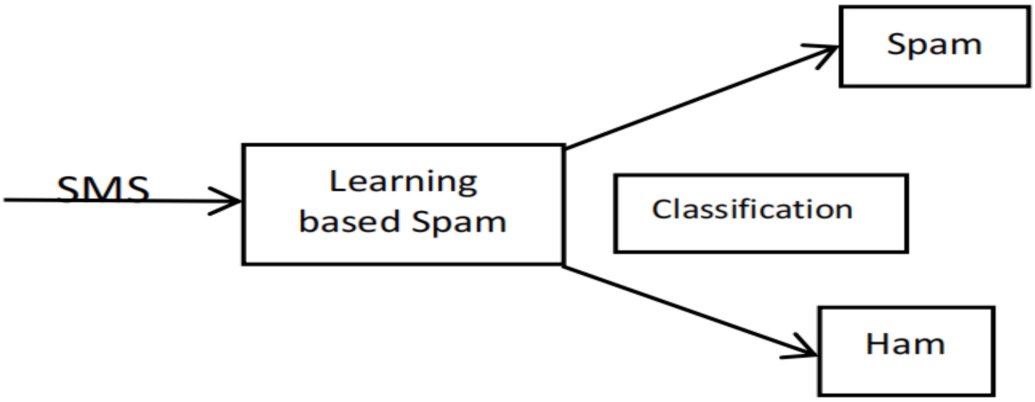


Figure : The Basic Idea of Spam Filtering ( Shahi and Yadav, 2014) There have been few surveys on SMS spam filtering, thus part of the goal of this work is to critically review the various approaches to SMS spam filtering in order to guide future research efforts.

## 2.2 Proposed solution

The proposed solution is categorized into Architecture, Approach and Feature set.

**Architecture**

The architectural sections are divided into three parts: client, server and the hybrid. The client side architecture involves the filtering or classification model being deployed on the user‟s mobile device while at the server side architecture, the filtering system is deployed at the mobile network operators‟ end or at the Short Message Service Centre (SMSC) which does the classification and forwards the messages into the appropriate folder on the client‟s device. The Hybrid architecture is based on both the client and server side, whereby the filtering system is deployed at both ends.

**Approaches**

Spam filtering approaches are classified into four types namely: listing, content-based, non-content based and collaborative approach.

**Listing Approach**

This technique is a conventional way of filtering SMS and its classification depends on two features called the whitelist (legitimate sender number) and blacklist (unwanted or unsolicited sender‟s number).

**Content based Approach**

This approach is a rule based classification that uses pattern recognition algorithm such as Bayesian, Support Vector Machines (SVM), Decision Tree, Hidden Markov Model (HMM) and K-Nearest Neighbor (KNN) to distinguish between spam and Ham messages.

**Non-Content based Approach**

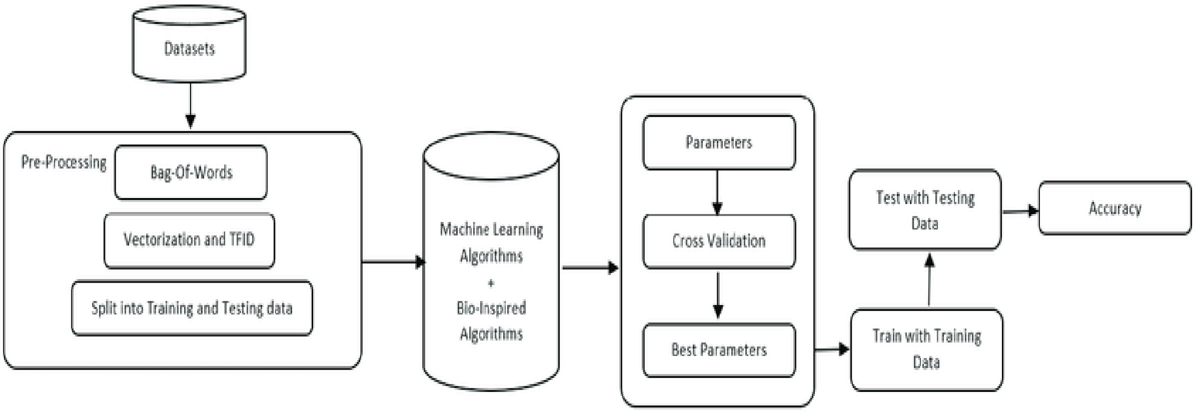
It is a behavioral-based detection system which uses the sending patterns such as temporal, static and network features of a spammer to classify SMS messages.

*Collaborative Filtering Approach*

Collaborative content filtering takes a server-based approach to combating SMS spam by collecting millions of messages of users around the globe or combining collective classifying power and accuracy from a community of users to form a super-classifier.

# 3.THEORITICAL ANALYSIS

## 3.1 Block diagram



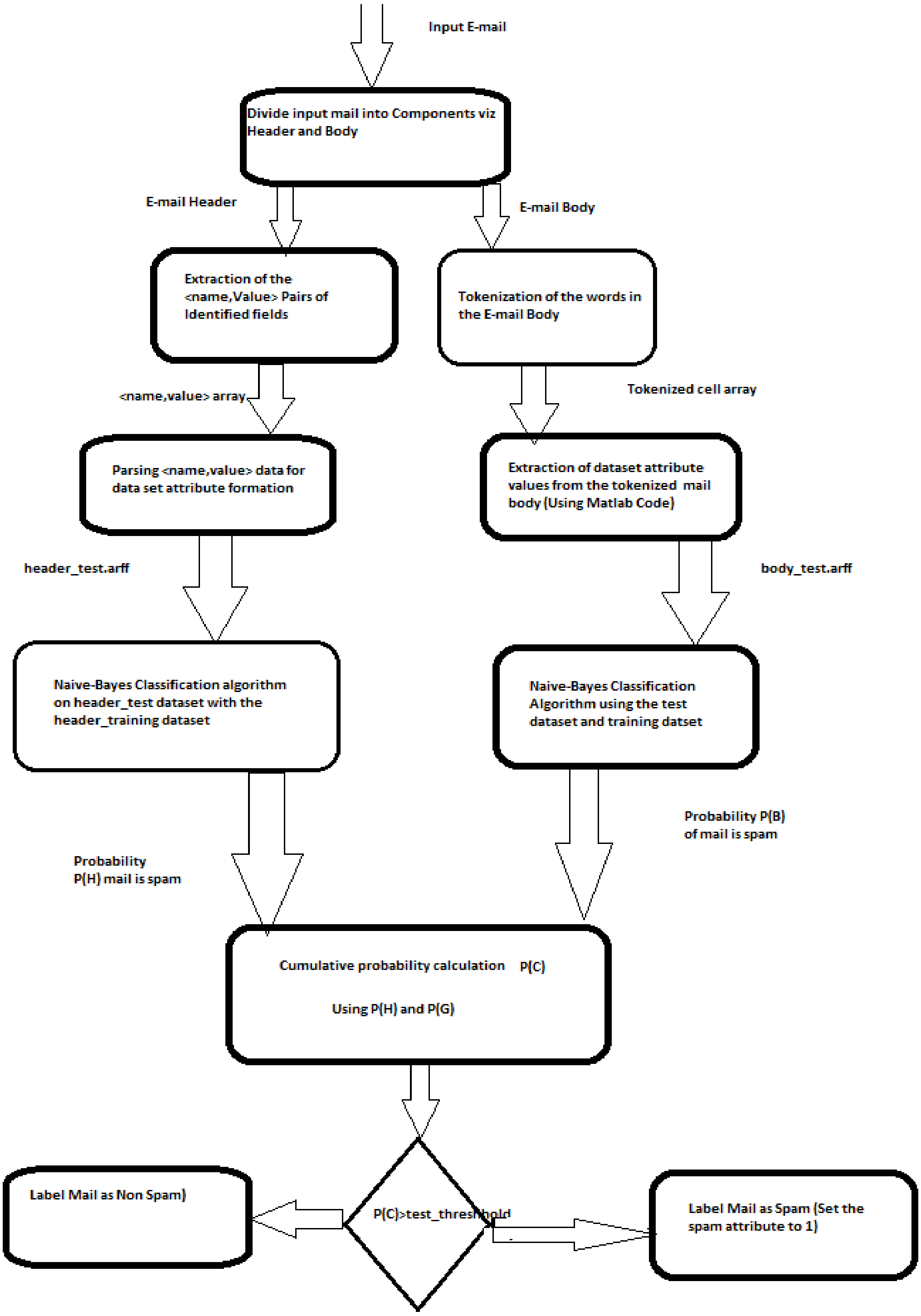
## 3.2 Hardware and Software designing

SMS spamming is an activity of sending ‘unwanted messages’ through text messaging or other communication services; normally using mobile phones. Nowadays there are many methods for SMS spam detection, ranging from the list-based, statistical algorithm, IP-based and using machine learning. However, an optimum method for SMS spam detection is difficult to find due to issues of SMS length, battery and memory performances. Hoping to minimize the aforementioned problems, this paper introduces another detection variance that is based on common characters used when sending SMS (i.e. numbers and symbols), SMS length and keywords. To verify our work, the proposed features were stipulated into five different algorithms and then, tested with three different datasets for their ability to detect spam. From the conduct of experiments, it can be suggested that these three features are reasonable to be used for detecting SMS spam as it produced positive results. In the future, it is anticipated that the proposed algorithm will perform better when combined with machine learning techniques.

## 4.EXPERIMENTAL INVESTIGATION

In the literature, spam problems and its influence have been investigated and discussed from different perspectives. Several researchers have looked into the influence of spam on economy, finance, marketing, business and management, while other researchers studied the impact of spam on security, privacy and date protections. Moreover, there were many researches that spotted a light on anti-spam filter techniques such as machine learning and IP blocks. In addition to that, there were several researches that were conducted to illustrate the impact of spam on the society, spam and law, and spam and e-mail reliability. There are two main objectives in this research. First, the theoretical part where the impact of spam on economy, finance, marketing and business will be studied; secondly, the practical part where multi-functions of document processing such as word stemming, short message form, stop words and tokenizing will be created. Moreover, an adapted machine learning (Bayesian method) working together with the study’s document processing to implement an accurate anti-spam engine will be used.

# 5.FLOWCHART


Input E-mail
Divide input mail into Components viz Header and Body
E-mail Header
E-mail Body
Extraction of the <name,Value> Pairs of Identified fields
Tokenization of the words in the E-mail Body
<name,value> array
Tokenized cell array
Parsing <name,value> data for data set attribute formation
Extraction of dataset attribute values from the tokenized mail body (Using Matlab Code)
header_test.arff
body_test.arff
Naive-Bayes Classification algorithm on header_test dataset with the header_training dataset
Naive-Bayes Classification Algorithm using the test dataset and training datset
Probability P(B) of mail is spam
Probability P(H) mail is spam
Cumulative probability calculation P(C)
Using P(H) and P(G)
Label Mail as Non Spam)
P(C)>test_threshold
Label Mail as Spam (Set the spam attribute to 1)

## 6.RESULT

At first we manually searched on google using the topic Spam Detection to gain an overview in spam detection field. It resulted in many email, twitter, web and SMS spam detection related papers. Then we customized our search using only SMS spam detection. It resulted in a few papers. Although there are SLR for other spam detection techniques but none of the search strings produces a SLR for SMS Spam detection. Through our study selection procedure we have chosen 17(S1-S17) papers published in different conferences and journals relating only to SMS spam detection. Among the 17 studies S1 and S11 are from same authors and S11 is an extension of S1. The ref. [20] is a journal which is an extension of the conference paper S10. S12 is an extension of [8]. As a result, in total we have studied 19 studies. Table 4 summarizes the reviewed papers Study ID with the reference no given in reference section, publication years, name of the conferences and journals where the papers published and the research questions they answered. The SMS spam collection data set is used for testing the method. The dataset is split into two categories for training and testing the research. The result of the experiments demonstrated that the classification performance of LR is high as compared with K-NN and DT, and the LR achieved a high accuracy of 99%.

## 7.ADVANTAGES AND DISADVANTAGES

### Advantages:

1.It Streamlines Inboxes

2.Protect Against Malware

3. Keeps You Compliant

4.It Saves You Money

### Disadvantages:

1.Lkelihood of unresponsiveness

2.Ineffective resource untilization

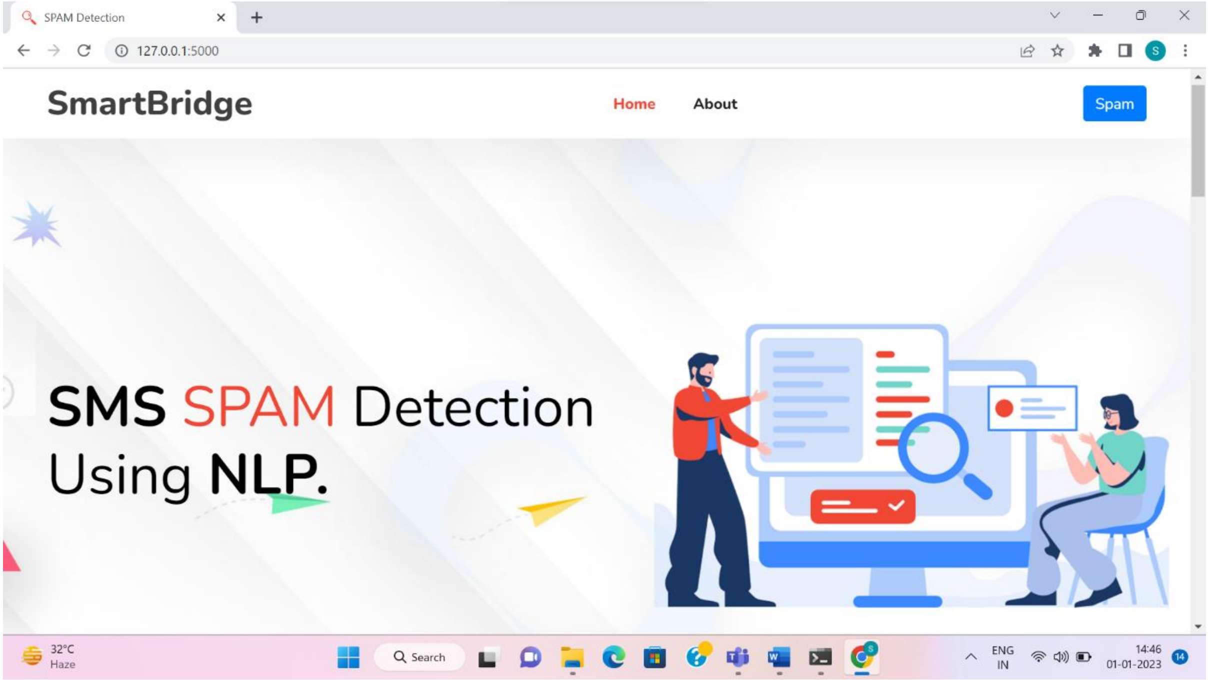
3.Undelivered emails

4.Website blocking

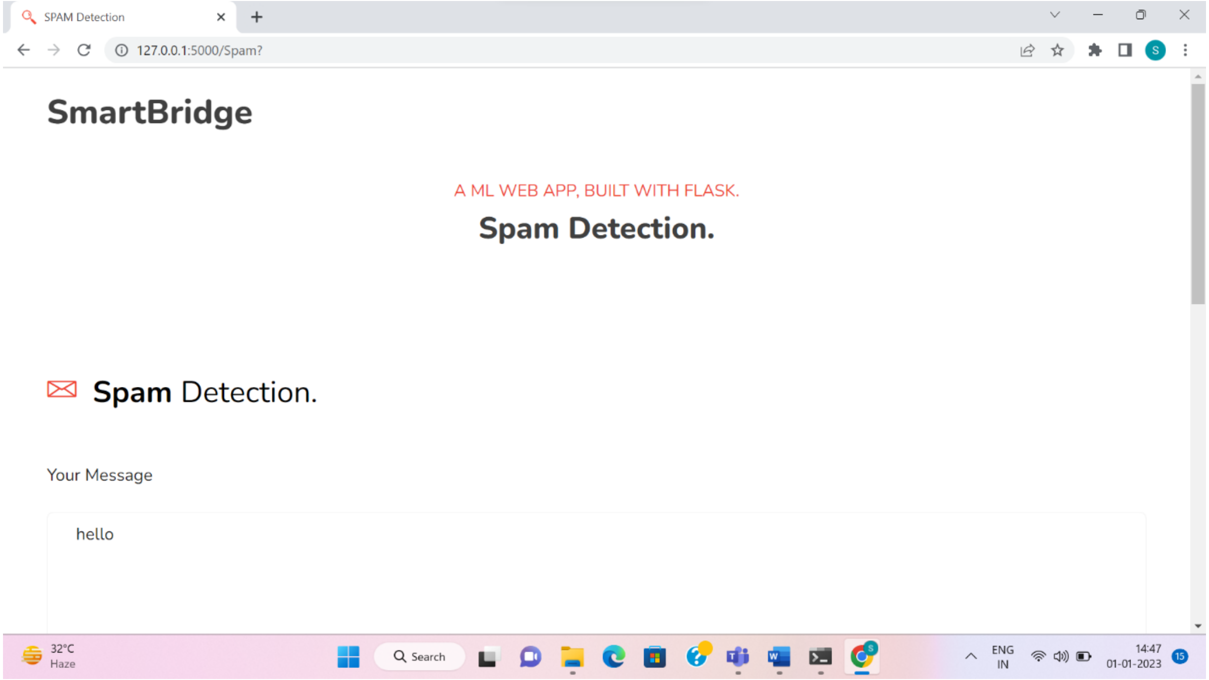
## 8.APPLICATIONS

- Authentication
- Challenge/response systems
- Checksum-based filtering
- Country-based filtering
- DNS-based blacklists
- URL filtering
- Strict enforcement of RFC standards
- Honeypots
- Hybrid filtering
- Outbound spam protection
- PTR/reverse DNS checks
- Rule-based filtering
- SMTP call back verification
- SMTP proxy
- Spam trapping
- Statistical content filtering
- Tarpits
- Collateral damage

## OUTPUT IMAGES



SMS SPAM Detection
Using NLP.



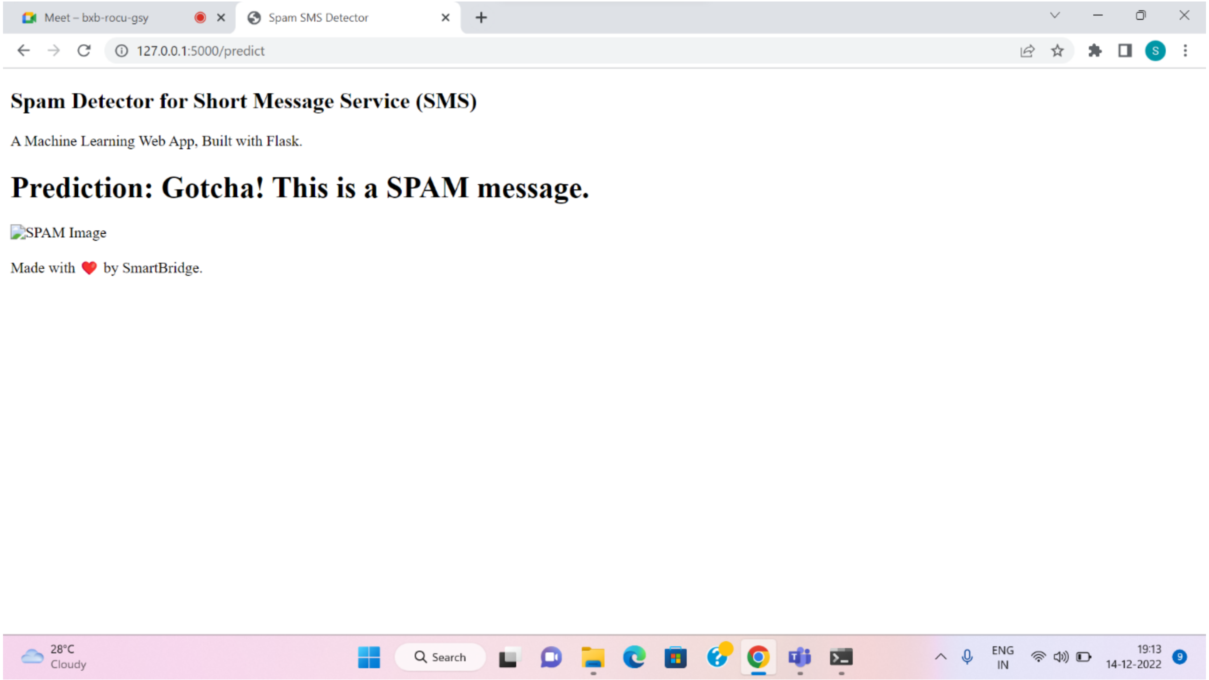
A ML WEB APP, BUILT WITH FLASK.

Spam Detection.

✉ Spam Detection.

Your Message

hello



Spam Detector for Short Message Service (SMS)

A Machine Learning Web App, Built with Flask.

Prediction: Gotcha! This is a SPAM message.

SPAM Image

Made with ❤ by SmartBridge.

## 9.CONCLUSION

In this paper the existing spam detection techniques, their current applications and their limitations have been highlighted.It has been seen that even the existing techniques consist of certain loop holes and none of the methods is completely effective in itself. Review spam detection is indeed a hard task but it requires continuous research and development in this field.

## 10.FUTURE SCOPE

Review spam detection is essential since it can ensure justice for the sellers and retain the trust of the buyer on the online stores. The algorithms developed so far have not been able to remove the requirement of manual checking of the reviews. Hence there is scope for complete automation of spam detection systems with maximum efficiency. With growing popularity of online stores, the competition also increases. The spammers get smarter day by day and spam reviews become untraceable. It is necessary to identify the spamming techniques in order to produce counter algorithms.

## 11.BIBILOGRAPHY

[1] Nitin Jindal and Bing Liu, Review Spam Detection, *WWW 2007*.

[2] Sihong Xie, Guan Wang, Shuyang Lin, Philip S. Yu, Review Spam Detection via Time Series Pattern Discovery, *WWW 2012*.

[3] Atefeh Heydari, Mohammad ali Tavakoli, Naomie Salim, Zahra Heydari, Detection of review spam: A survey, *Science Direct Expert Systems with Applications*, 42 (7) (2015).

[4] Ee Peng Lim, Viet-An Nguyen, Nitin Jindal, Bing Liu, Hady Wirawan Lauw, Detecting Product Review Spammers using Rating Behaviors, *CIKM 2010*. [5] Nitin Jindal and Bing Liu, Opinion Spam and Analysis, *WSMD 2008*.

[6] Guan Wang, Sihong Xie, Bing Liu, Philip S. Yu, Review Graph based Online Store Review Spammer Detection, *IEEE 2011*.

[7] Bing Liu, Sentiment analysis and Opinion mining, Morgan & Claypool Publishers, May 2012.

[8] Somayeh Shojaee, Masrah Azrifah Azmi Murad, Azreen

Bin Azman, Nurfadhlina Mohd Sharef and Samaneh Nadali, Detecting Deceptive Reviews Using Lexical and Syntactic Features, *IEEE 2013*.

[9] Shebuti Rayana, Leman Akoglu Stony, Collective Opinion Spam Detection: Bridging Review Networks and Metadata, *KDD 2015*.

[10] Guan Wang, Sihong Xie, Bing Liu, Philip S. Yu, Identify Online Store Review Spammers via Social Review Graph, *ACM Transactions On Intelligent Systems and Technology*, 3 (4) (September 2012).

[11] Yiqun Liu, Min Zhang, Shaoping Ma, Liyun Ru, User Behavior Oriented Web Spam Detection, *WWW 2008.*

[12] Fangtao Li, Minlie Huang, Yi Yang and Xiaoyan Zhu, Learning to Identify Review Spam, *IJCAI 2011*.

[13] Arjun Mukherjee, Bing Liu, Junhui Wang, Natalie Glance, Detecting Group Review Spam, *WWW 2011*.

https://stories.flipkart.com/flipkart-fake-reviews/, 2016.

## APPENDIX:-

## app.py

```
# Importing essential libraries

from flask import Flask, render_template, request

import pickle



# Load the Multinomial Naive Bayes model and CountVectorizer object from disk

filename = 'spam-sms-mnb-model.pkl'

classifier = pickle.load(open(filename, 'rb'))
```

```
cv = pickle.load(open('cv-transform.pkl','rb'))

app = Flask(__name__)



@app.route('/')

def home():

    return render_template('index.html')



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

def prediction(): # route which will take you to the prediction page

   return render_template('spam.html')



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

def predict():

   if request.method == 'POST':

    message = request.form['message']

    data = [message]

    vect = cv.transform(data).toarray()
    my_prediction = classifier.predict(vect)

    return render_template('result.html', prediction=my_prediction)



if __name__ == '__main__':

    app.run(debug=True)
```