# Spam SMS filtering Using Machine Learning

## Problem Statement

Short Message Service (SMS) is one of the well-known communication services in which a message sends electronically. The lessening in the cost of SMS benefits by telecom organizations has prompted the expanded utilization of SMS. This ascent pulled in assailants, which have brought about SMS Spam problem. Spam messages include advertisements, free services, promotions, awards, etc. People are using the ubiquity of mobile phone devices is expanding day by day as they give a vast variety of services by reducing the cost of services. Short Message Service (SMS) is one of the broadly utilized communication service. In any case, this has prompted an expansion in mobile phones attacks like SMS Spam. In this problem, preliminary results are mentioned or explained herein based on Singapore based publically available datasets. This problem is further expanded using multiple background datasets.

## Background

Many SMS Spam messages detection techniques are available these days to block spam messages and filtering spam messages. Few of which are mentioned below: - Gómez Hidalgoet. al. assessed a few Bayesian based classifiers to identify mobile phone spam. In this problem, the researchers proposed the first two surely understood SMS spam datasets: the Spanish (199 spam and 1,157 ham) and English (82 spam and 1,119 ham) test databases. They have tried on them various messages portrayal techniques and machine learning calculations, as far as viability. The outcomes show that Bayesian separating methods can be successfully utilized to group SMS spam.

Hidalgo et al have analyzed that how Bayesian filtering technique can be used to detect SMS Spam. They have built two datasets one in English and another in Spanish. Their analysis shows that Bayesian filtering techniques that were earlier used in detecting email spam can also be used to block SMS Spam.

## Methodology

Our framework is a combination of various techniques or methods like: - data collection, data pre-processing, and finally applying classifications methods on available SMS labeled dataset.
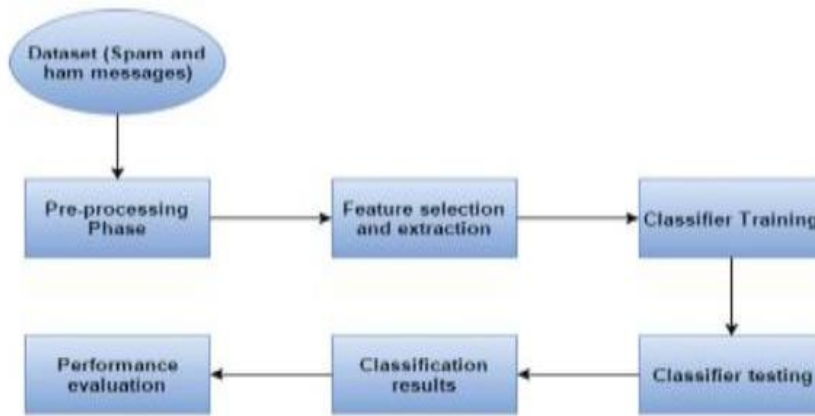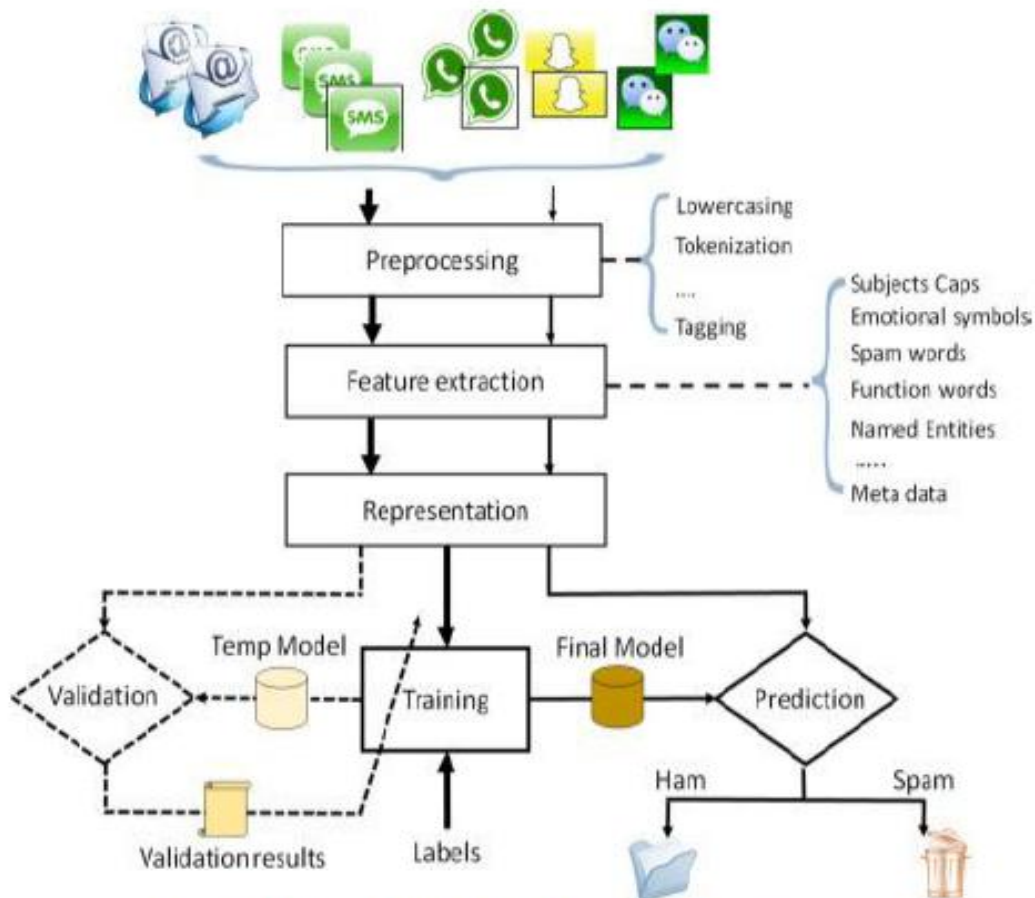
Fig1: System Architecture



Fig 2: Flow Chart of SMS spam filtering [1]

**Experimental Design**

The SMS Spam Collection v.1 is a public set of SMS (text) labeled messages that have been collected for mobile phone spam research. It has one dataset composed by 5,574 English, real and non-encoded messages, tagged as legitimate (ham) or spam. The collection is free for all purposes, and it is publicly available at:

**Links: 1.** www.dt.fee.unicamp.br/~tiago/smsspamcollection/

2. https://archive.ics.uci.edu/ml/datasets/sms+spam+collection

**Name: -**SMS Spam Collection v. 1 and SMS Spam Collection Data Set

When testing has been done by some researchers on the similar number of instances but written in Indian English our accuracy is degraded because of Indian writing style. Singapore English is different from Indian English because of different writing and speaking style. Our main objective following existing research is to develop such generalized model that could predict or filter the datasets on multiple backgrounds with a better accuracy level.

Our future goal should be test the results on large spam dataset on multiple backgrounds like (Singapore, American, Indian English etc.).

## References

[1] Mobile Commons Blog.
https://www.mobilecommons.com/blog/2016/01/how-textmessaging-will-change-for-the-better-in-2016/

[2]http://www.academia.edu/2987380/SMS_Spam_Filtering_Methods_and_Data