RANI CHANNAMMA UNIVERSITY

"Vidhya Sangama", P B R H – 4, BELGAVI-591 156

BLDEA'S

S B ARTS AND K C P SCIENCE COLLEGE, VIJAYAPUR

A Project Synopsis

ON

"SPAM SMS DETECTION USING AI"

A Project Synopsis submitted in partial fulfillment for the award of the degree

Bachelor Of Computer Application

Submitted By

Sakshi Ambali

Shruti Badagandi

Project Guide

Prof. S.D. PATIL

CONTENTS

Abstract

The number of people using mobile devices increasing day by day. **SMS** (short message service) is a text message service available in smartphones as well as basic phones. So, as the traffic of SMS increased drastically, the spam messages also increased. **Spam** is unsolicited and unwanted messages sent electronically and whose content may be malicious. SMS messages are usually very cheap (if not free) for the user to send, making it appealing for unrightful exploitation. The dangers of spam messages for the users are many: undesired advertisement, exposure of private information, becoming a victim of a fraud or financial scheme, being lured into malware and phishing websites etc. So, spam classification has special attention. At the same time, reduction in the cost of messaging services has resulted in growth in unsolicited commercial advertisements (spams) being sent to mobile phones. In parts of Asia, up to **30%** of text messages were spam in 2012. In this project different artificial intelligence techniques are applied to the database. Finally, the results are compared and the best algorithm for spam filtering for text messaging is introduced.

Introduction

SMS spam is used for commercial advertising and spreading phishing links. Commercial spammers use malware to send SMS spam because sending SMS spam is illegal in most countries. Sending spam from a compromised machine reduces the risk to the spammer because it obscures the provenance of the spam. SMS can have a limited number of characters, which includes alphabets, numbers, and a few symbols. A look through the messages shows a clear pattern. Almost all of the spam messages ask the users to **call a number, reply by SMS, or visit some URL**. This pattern is observable by the results obtained by a simple SQL query on the spam. The low price and the high bandwidth of the SMS network have attracted a large amount of SMS spam.

SMS spam detection is an important task where spam SMS messages are identified and filtered. As more significant numbers of SMS messages are communicated every day, it is challenging for a user to remember and correlate the newer SMS messages received in context to previously received SMS. Thus, using the knowledge of artificial intelligence with the amalgamation of machine learning, and data mining we will try to develop web-based SMS text spam detector. Algorithms used in this technique are**: Logistic regression (LR), K-nearest neighbor (K-NN) and Decision Tree (DT).**

Existing System

Artificial Intelligence (AI) has changed many aspects of our digital lives, including how we handle and filter spam. Spam has always been a big problem for many. To detect these messages, it is necessary to have a **Spam detector.** It is a crucial part of maintaining the privacy and usability of our digital tools. AI tools like **Mail-Meteor, Spam Arrest and algorithms like K-Nearest Neighbors (KNN) and Random Forest (RF) algorithm** have been developed to fight against this issue with very accurate accuracy and efficiency. These, like any other AI tool, have been trained on a different data set of billions of data to learn from it and catch the spam quickly within a few seconds.

Proposed Approach

We notice that the length of the text message (number of characters used) is a very good feature for the classification of spams. Sorting features based on their **mutual information (MI) criteria** shows that this feature has the highest MI with target labels. Additionally, going through the misclassified samples, we notice that text messages with length below a certain threshold are usually hams, yet because of the tokens 22 corresponding to the alphabetic words or numeric strings in the message they might be classified as spams.

Advantages

Enhanced security: Out of all the SMS received by an individual throughout the day, the possibility of a phishing attack or cyber threat is never zero. With the benefits of SMS spam filters, the security risk can be reduced

Time efficient: By filtering out the important SMS and sending to the spam box the junk SMS, spam filter saves time for the user and keeps the business communications going by streamlining the user inbox.

Improved performance: Along the lines of the time-saving benefit of SMS spam filters, these tools facilitate increased productivity of the user by keeping away unwanted SMS.

It Saves You Money: Every day, someone falls prey to a phishing scam, a particular kind of spam-based scheme where someone thinks they are getting a legitimate SMS and ends up divulging credit card information. Sometimes it is a personal credit card, sometimes it is a company credit card. In both instances, the end result is losing valuable time and money to a scam.

Challenges

- There are no **publicly available large datasets** of spam SMS. Even if there were, it is not at all expected that training on those datasets would translate into a good performance within our context. Therefore, there is no choice but to build a custom dataset from real data that streams into the system.
- **Absence of a pipeline** to transform SMS logs into a structured and clean dataset.
- The app is available in many countries and languages, adding **another layer of complexity.**
- **Message ambiguity**: it can even be hard for a human to distinguish between real messages and spam.

Requirements

OS – Windows 7 and above

Language – Python (NumPy and Pandas)

IDE – VS CODE

Expected Outcomes

The SMS spam message problem is plaguing almost every country and keeps increasing without a sign of slowing down as the number of mobile users increase in addition to cheap rates of SMS services. Therefore, this paper presents the spam filtering technique using various machine learning algorithms. Different algorithms will provide different performances and results based on the features used. For future works, adding more features such as message lengths might help the classifiers to train data better and give better performance. Present Work is useful to identify Spam SMS from SMS dataset. Experimental work shows that **98.12%** SMS are identified correctly as Spam SMS from the dataset.