International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 06 | June - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

Spam SMS Detection Using Machine Learning

Atharva Kale,Vaibhav Katake, Gaurav Despande,Rugved Gavali

Dept of Computer Engineering, SVPM'S College of Engineering, Malegaon (Pune), India

---

Abstract - In today's digital communication era, unsolicited and malicious text messages, commonly known as spam, pose a significant threat to user privacy and mobile security. This project aims to develop an intelligent and automated system for SMS spam detection using machine learning techniques, with a focus on the Support Vector Machine (SVM) algorithm. The objective is to classify incoming messages as either "spam" or "ham" (non-spam) with high accuracy and efficiency.

The system is trained on a labeled SMS dataset containing a mixture of spam and ham messages. Text preprocessing techniques such as tokenization, lowercasing, stop-word removal, and TF-IDF vectorization are applied to convert raw text into numerical features suitable for machine learning. The SVM classifier, known for its robustness in high-dimensional spaces, is trained on the transformed dataset to find the optimal decision boundary between the two classes.

The model's performance was tested using widely accepted metrics such as accuracy, precision, recall, and F1-score to ensure reliable results. Experimental results demonstrate that SVM provides a reliable and effective method for spam detection with strong generalization capabilities.

.

1.INTRODUCTION

With the explosive growth of mobile communication, Short Message Service (SMS) has become one of the most widely used forms of personal and business communication. However, this convenience is often disrupted by the increasing number of spam messages that are either promotional, fraudulent, or malicious in nature. These unsolicited messages not only waste users' time but also pose serious security threats, including phishing attacks, identity theft, and financial fraud.

Spam detection, therefore, has become a crucial task in ensuring secure and effective communication. Manual filtering of messages is neither efficient nor scalable. To overcome this challenge, machine learning offers a powerful solution that can automatically learn patterns from data and classify messages as spam or ham (non-spam) with high accuracy.

In this project, we implement a machine learning-based SMS spam detection system using the **Support Vector Machine (SVM)** algorithm. SVM is a supervised learning model that is particularly well-suited for text classification problems due to its ability to handle high-dimensional feature spaces and find optimal separating hyperplanes between classes.

The project involves collecting a dataset of labeled SMS messages, performing text preprocessing (such as tokenization, stop word removal, and vectorization using TF-IDF), training an SVM classifier, and evaluating its performance using metrics such as accuracy, precision, recall, and F1-score.

This system can be integrated into messaging platforms to automatically detect and filter out spam messages, thereby improving user experience and security

2. Methodology

This project uses a machine learning approach to classify SMS messages as either "spam" or "ham" using the Support Vector Machine (SVM) algorithm. A pre-labeled dataset containing SMS messages is used as input for training and testing the model.

First, we clean and prepare the text data by converting all messages to lowercase, removing punctuation and special characters, and filtering out common stop words. This step ensures the data is consistent and easier to analyze.Tokenization is performed to break the messages into individual terms, enabling effective analysis.

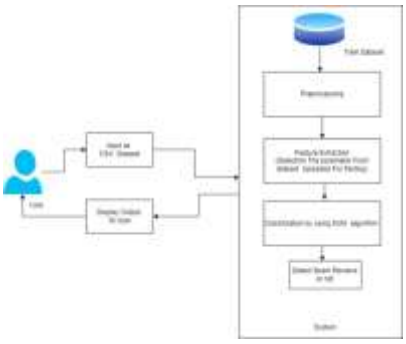
After preprocessing, the messages are transformed into numerical vectors using TF-IDF (Term Frequency-Inverse Document Frequency). This method assigns importance to terms based on how frequently they appear in a message relative to their frequency across all messages.

After cleaning the data, the next step is creating separate training and testing sets so we can accurately evaluate our model's effectiveness. The SVM classifier is trained on the training data to learn the decision boundary that best separates spam from ham messages. Because SVM performs exceptionally well with high-dimensional data, it's an ideal choice for text classification tasks."

The trained model is evaluated using metrics such as accuracy, precision, recall, and F1-score to measure its

performance. These results indicate how reliably the model can identify spam messages in real-world scenarios.

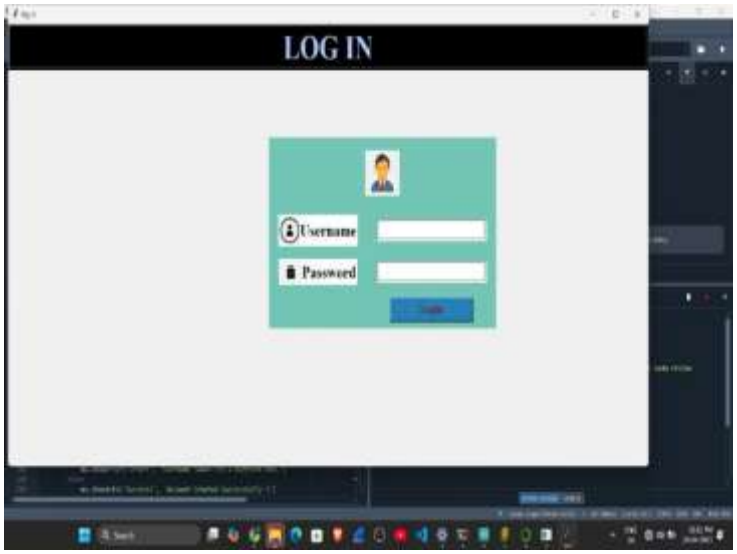
3.Architecture

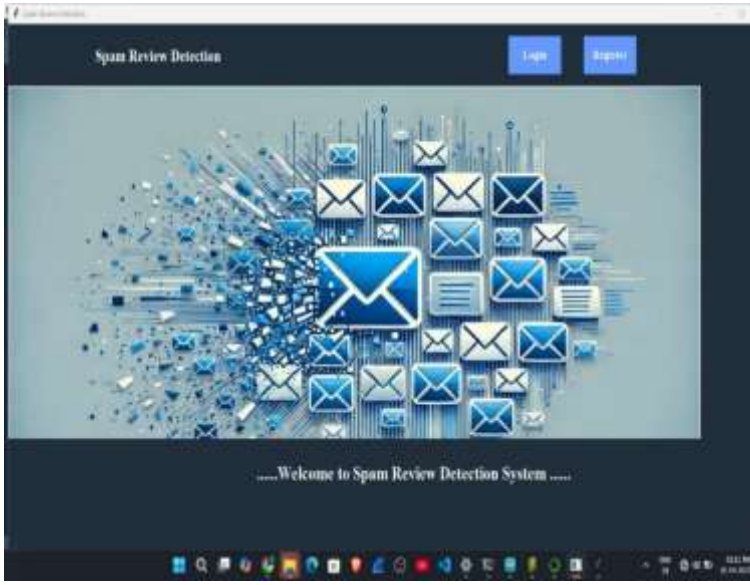


4.Literature Survey

1.Paper Name: Investigating Evasive Techniques in SMS Spam Filtering: A Comparative Analysis of Machine Learning Models
Authors: Muhammad Salman, Muhammad Ikram, Mohamed Ali Kaafar
Abstract: SMS spam remains a significant challenge, necessitating robust detection systems to counteract spammers' evasive strategies. This study addresses key challenges in SMS spam detection, including data scarcity, lack of benchmark datasets, and vulnerability to evasion techniques. The authors introduce a new, large SMS dataset comprising over 68K messages (61% legitimate, 39% spam), the largest publicly available to date. They evaluate the performance of various machine learning models, ranging from shallow techniques to advanced deep neural networks, and analyze their robustness against evasion strategies such as paraphrasing, character swapping, and Punycode attacks. Findings reveal that deep learning models outperform traditional methods, achieving higher accuracy and resilience against adversarial manipulations. However, all models exhibit vulnerabilities to certain evasion techniques, highlighting the need for further research to enhance SMS spam detection systems. The dataset and code are released to support future research in this domain.
2.Paper Name: Machine Learning-Based Opinion Spam Detection: A Systematic Literature Review Author: Atika Qazi[1], Najmul Hasan[2], Rui Mao[3]_Member IEEE, Mohamed Elhag Mohamed Abo4, Samrat Kumar Deys, Glenn Hardaker6
Abstract: This study reviews existing methodologies for detecting spam reviews, individual spammers, and group spam using machine learning (ML) and deep learning (DL) techniques. It categorizes and assesses these techniques, finding that accuracy is the most common metric used. The research highlights the effectiveness of SMS spam filtering strategies and proposes a new framework for applying ML and DL to spam review detection. The findings offer insights for academics and practitioners on overcoming challenges in identifying spam reviews and improving detection methods.

5.Result





6. CONCLUSION

This paper presents a deep learning model for SMS spam detection, tested on a UCI dataset with three word embedding methods and different classifiers. It outperforms previous models and will be tested on more datasets in the future.

ACKNOWLEDGEMENT

We would like to express our sincere gratitude to our project guide for their invaluable support and guidance.
Prof.P.T.Khese and Head of the Department Prof. Y.R.Khalate for their valuable guidance and for providing all the necessary facilities, which were
Their guidance was invaluable in helping us complete this project. We're also deeply grateful to all the faculty and staff members who supported us along the way.
Department of Computer of SVPM's College of Engineering, Malegaon (Bk) for their valuable time

REFERENCES

1. . Bhat, J.S.P. SMS Spam Detection using Support Vector Machine. *Int. J. Comput. Appl.* **2017**, *168*, 10–15. doi:10.5120/ijca2017913501.
2. Almeida, M.; Hidalgo, J.M.G.; Yamakami, A. Contributions to SMS Spam Filtering: Dataset and Comparative Study. *Expert Syst. Appl.* **2012**, *39*, 9899–9908. doi:10.1016/j.eswa.2012.03.038.
3. Verma, S.; Singh, P.K. Spam Message Detection Using Machine Learning Approaches: A Review. *Int. J. Comput. Appl.* **2016**, *141*, 1–6.
4. Bhatia, R.D.; Gupta, S. SMS Spam Filtering Techniques: A Survey. *Int. J. Adv. Res. Comput. Sci. Softw. Eng.* **2015**, *5*, 501–507.
5. Joachims, T. Text Categorization with Support Vector Machines: Learning with Many Relevant Features. *ECML*, 1998, pp. 137–142.