iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** I **Month of publication:** January 2026

DOI: https://doi.org/10.22214/ijraset.2026.76964

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue I Jan 2026- Available at www.ijraset.com

An Intelligent SMS Spam Detection System Using Ensemble Machine Learning Techniques

Kushi A
Department of Artificial Intelligence and Data Science, East West Institute of Technology, Bengaluru, India

Abstract: ***The rapid growth of mobile communication has resulted in a significant increase in unsolicited and fraudulent spam messages. These messages not only inconvenience users but also pose serious security and privacy risks. Manual filtering of spam messages is inefficient due to the large volume of data generated daily. This paper proposes an intelligent SMS spam detection system using ensemble machine learning techniques. Text preprocessing is applied to clean and normalize SMS content, followed by feature extraction using the Term Frequency–Inverse Document Frequency (TF-IDF) method. Multiple machine learning classifiers, including Naive Bayes, Logistic Regression, and Support Vector Machine, are trained and combined using a voting-based ensemble approach. Experimental results on the SMS Spam Collection dataset demonstrate that the ensemble model outperforms individual classifiers by achieving higher accuracy and reduced false positives. The proposed system provides an effective and reliable solution for automated spam detection.***
Keywords: Spam Detection, Ensemble Learning, Machine Learning, NLP, TF-IDF, Text Classification.

I. INTRODUCTION

Short Message Service (SMS) continues to be one of the most widely used communication methods due to its simplicity and low cost. However, the popularity of SMS has also led to a rise in spam messages, including promotional advertisements, phishing attempts, and fraudulent content. These spam messages can result in financial loss and compromise user privacy.

Traditional spam filtering techniques rely on rule-based systems and keyword matching, which lack adaptability to evolving spam patterns. Machine learning-based approaches offer a more robust solution by learning patterns from historical data. This paper focuses on developing an intelligent SMS spam detection system using ensemble machine learning techniques to improve classification performance and reliability.

II. RELATED WORK

Spam detection has been extensively studied using various machine learning techniques. Early approaches focused on rule-based filtering, which required manual updates and performed poorly against new spam types. Probabilistic classifiers such as Naive Bayes were later introduced and showed improved performance due to their efficiency in handling text data.

Logistic Regression and Support Vector Machine classifiers have also been widely applied to spam detection tasks due to their strong generalization capabilities. Recent studies emphasize ensemble learning approaches, which combine multiple classifiers to reduce bias and variance. Although deep learning models have shown promising results, they require large datasets and high computational resources. This study adopts an ensemble machine learning approach that balances performance and computational efficiency, making it suitable for practical SMS filtering systems.

III. DATASET DESCRIPTION

The SMS Spam Collection dataset obtained from Kaggle is used in this study. The dataset consists of SMS messages labeled as either *spam* or *ham* (non-spam). Each record contains the message text and its corresponding label. The dataset is widely used as a benchmark for spam detection research due to its reliability and well-structured format.

Prior to model training, unnecessary columns were removed and the dataset was examined to ensure consistency and data quality.

IV. METHODOLOGY

A. Text Preprocessing

Text preprocessing is performed to reduce noise and improve classification accuracy. All SMS messages are converted to lowercase, and punctuation, special characters, and extra spaces are removed. Common English stopwords are eliminated to retain only meaningful words relevant to classification.

B. Feature Extraction

The cleaned text data is transformed into numerical features using the Term Frequency–Inverse Document Frequency (TF-IDF) technique. TF-IDF assigns higher importance to informative words while reducing the impact of frequently occurring terms, enabling effective text representation for machine learning models.

C. Model Training

The dataset is divided into training and testing sets using an 80:20 split. Three machine learning classifiers—Naive Bayes, Logistic Regression, and Support Vector Machine—are trained individually. These models represent different learning strategies and provide diverse predictions.

D. Ensemble Learning

To enhance performance, a voting-based ensemble classifier is constructed by combining the predictions of the individual models. Hard voting is used, where the final class label is determined based on majority voting among the classifiers.

E. Performance Evaluation

The performance of the models is evaluated using accuracy, precision, recall, F1-score, and confusion matrix analysis. These metrics provide a comprehensive evaluation of the spam detection system, with particular emphasis on minimizing false positives.

V. RESULTS AND DISCUSSION

Experimental results indicate that all individual classifiers achieve satisfactory performance in spam detection. Among them, the Support Vector Machine performs better than Naive Bayes and Logistic Regression. However, the ensemble model achieves the best overall performance by combining the strengths of all classifiers. Fig. 1 shows the accuracy comparison of different machine learning models.

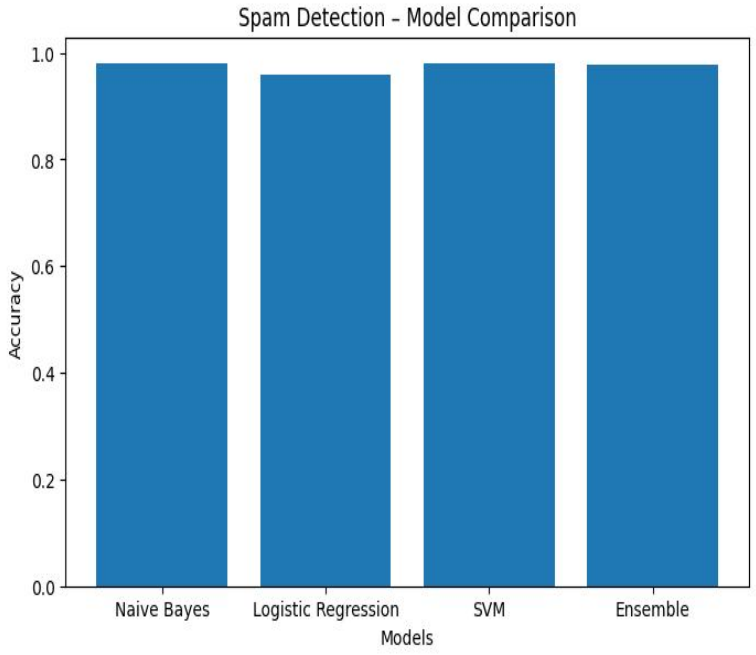


Fig. 1. Accuracy comparison of spam detection models.

The confusion matrix analysis shows that the ensemble approach significantly reduces false positives, which is crucial for preventing legitimate messages from being incorrectly classified as spam. The results confirm that ensemble learning improves the robustness and reliability of SMS spam detection systems.

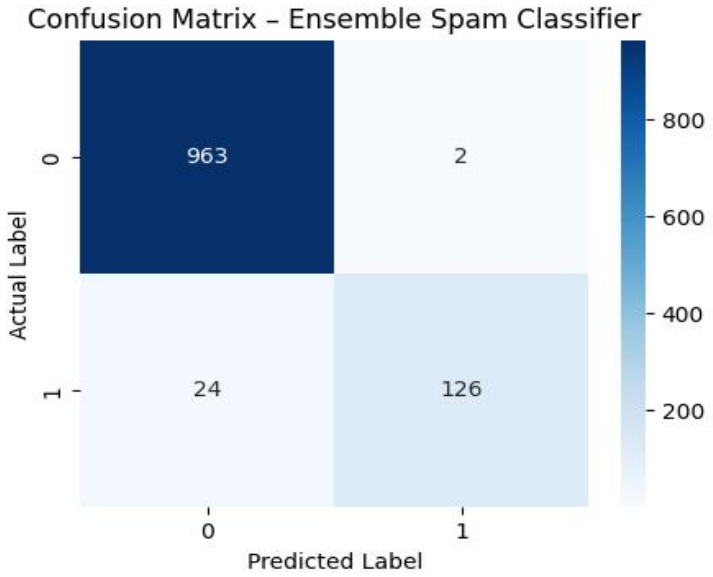


Fig. 2. Confusion matrix of the ensemble spam detection model.

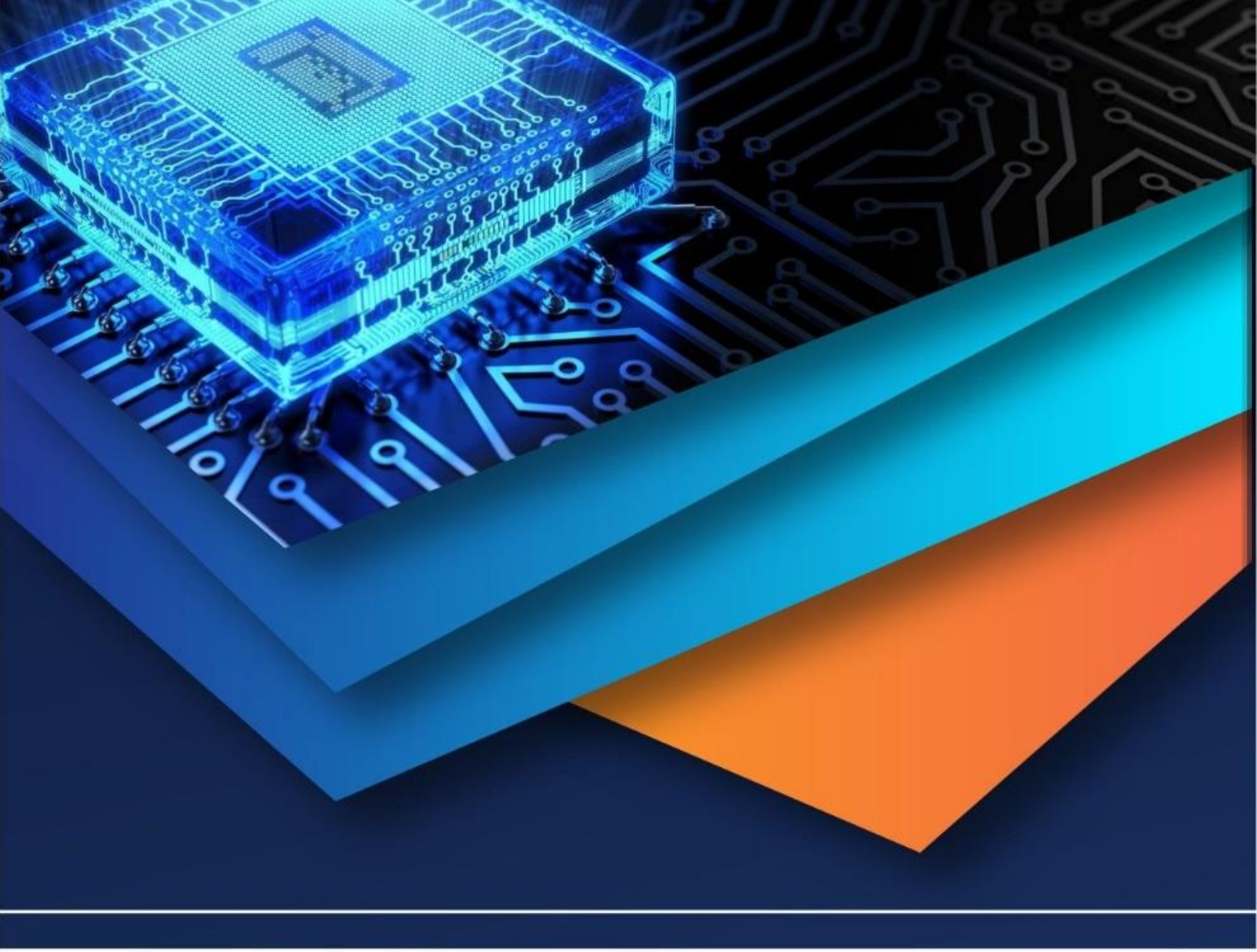
VI. CONCLUSION AND FUTURE WORK

This paper presented an intelligent SMS spam detection system using ensemble machine learning techniques. By combining multiple classifiers through a voting-based ensemble approach, the proposed system achieved improved performance compared to individual models. The results demonstrate the effectiveness of ensemble learning in reducing false positives and enhancing spam detection accuracy.

Future work may explore the use of deep learning and transformer-based models for handling more complex spam patterns. Additionally, incorporating contextual and metadata features could further improve detection performance in real-time applications.

REFERENCES

[1] T. Almeida et al., "Contributions to the Study of SMS Spam Filtering," *ACM Symposium*, 2011.
[2] H. Drucker et al., "Support Vector Machines for Spam Categorization," *IEEE Transactions on Neural Networks*, 1999.
[3] J. Ramos, "Using TF-IDF to Determine Word Relevance in Document Queries," 2003.
[4] C. Cortes and V. Vapnik, "Support Vector Networks," *Machine Learning*, 1995.
[5] L. Breiman, "Random Forests," *Machine Learning*, 2001.
[6] Kaggle, "SMS Spam Collection Dataset," Kaggle Repository.
[7] T. Mitchell, *Machine Learning*, McGraw-Hill, 1997.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY