



Paper Type: Original Article

Ensemble Learning Approaches for SMS Spam Detection: A Comparative Study of Text Classification Models

Ayman H. Abdel-aziem ^{1*} , Hadeer Mahmoud ²  and Ahmed M. AbdelMouty ³ 

¹ Faculty of Information Systems and Computer Science, October 6th University, Giza, 12585, Egypt;
ayman.hasanein.comp@o6u.edu.eg.

² Department of Artificial Intelligence, Faculty of Computers and Artificial Intelligence, Modern University for Technology & Information, Cairo, Egypt; hadeer.mahmoud@cs.mti.edu.eg.

³ Department of Information Systems, Faculty of Computers and Informatics, Zagazig University, Zagazig, Egypt;
a_abdelmouty@zu.edu.eg.

Received: 11 Jan 2025

Revised: 23 Apr 2025

Accepted: 17 Sep 2025

Published: 19 Sep 2025

Abstract

For users who rely on single-use mobile phones, the global problem of receiving unwanted marketing messages through SMS remains a significant concern. In recent years, extensive use of machine learning and deep learning approaches has been explored to address this challenge. To improve predictive accuracy, the outputs of multiple models were combined using a majority-voting strategy. This work presents a comparative analysis of several text classification techniques, highlighting the importance of reliably identifying and labeling spam SMS messages. After data preprocessing, messages were transformed into numerical representations using TF-IDF, which emphasizes uncommon but informative terms over frequent ones. Among the tested methods, the Relevance Vector Machine achieved the strongest performance in the data, reaching an F1 is 0.975176. In addition, this examined alternative spam detection algorithms, including Logistic Regression, XGBoost, and LightGBM. The preprocessing pipeline included duplicate removal, text normalization with spaCy, label encoding, and TF-IDF vectorization. Two experimental conditions were evaluated: one without handling class imbalance and another with imbalance adjustment. Results showed that ensemble-based methods, particularly Gradient Boosting, XGBoost, and LightGBM, consistently delivered superior performance. Under imbalanced data conditions, both XGBoost and LightGBM achieved F1 scores of 0.99 across the majority and minority classes. When class imbalance was corrected, their performance remained strong, with F1 scores of 0.98 for all classes. Logistic Regression also demonstrated robust results, confirming its role as a reliable baseline. Overall, the findings indicate that the proposed RVM framework is effective for SMS spam classification and has practical applicability in real-world scenarios.

Keywords: SMS; RVM; SVM; KNN; Spam Message.

1 | Introduction

Unfortunately, information conveyance in this digital age [1–8]. Spam emails can originate from any nation with an internet connection, which is problematic for both individuals and companies. Much effort has been put into developing algorithms to better identify and classify spam communications, however none of these algorithms have proven to be especially effective yet. [9–14] Numerous SMS spam filtering algorithms now in use categorize messages as spam based on attributes such as the sender's identity and the message's content, according to study. [15–18] However, since spammers alter, features like sender information and textual



Corresponding Author: ayman.hasanein.comp@o6u.edu.eg



<https://doi.org/10.61356/j.mawa.2025.8596>



Licensor **Multicriteria Algorithms with Applications**. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0>).

content might not be enough to detect spam SMS on their own. [19–22] Therefore, as demonstrated by the case that follows, people are nonetheless tricked by textual spam. Please be advised, dear recipient, reward that you might have won in the draw that was held last weekend. The prize pool is guaranteed to be \$50,000. To get your prize, enter the claim code N952 to 09900000000. Act fast because this promotion is only available. Thank you very much.

1.1 | Screening Out Spam Texts

Finding and eliminating SMS messages that contain unsolicited commercials, or promotional information is the process of SMS spam filtering. To do this, machine learning models are trained using a large dataset of tagged SMS messages. People worldwide are receiving spam text messages that purport to be from a sweepstakes or game of chance that offers a free vacation or substantial sums of money. They have to phone and number listed in message to prizes. Those who call these lines are requested for their personal information and bank accountf provides this information to their bank accounts, causing them to suffer severe financial disasters. Screening services are required due to the growing incidence of SMS spam. Spammers are using SMS texting increasingly to continuously bombard customers with unsolicited messages, which is inconvenient and may be harmful to their security. One of two methods can be used to identify SMS spam. Some methods are content based, while others are not. One non-content-based technique that telecom companies—not mobile phone users—frequently employ is social network analysis. Content-based systems categorize spam messages in content using autonomous text classification algorithms like KNN, RVMs, logistic regression, and Winnow. a variety of classification methods, including Ensemble learning techniques have made use of Support Vector Machines, Neural Networks, Maximum Entropy (ME), and RVMs. The suggested ensemble of the four fundamental classifiers utilized in this investigation—NB, SVM, RVM, and K-NN—is depicted in Figure 1. The goal of this study is to raise each of these models' metrics and forecast accuracy.

In machine learning, several techniques are trained to the same problem as part of an ensemble learning strategy. Better outcomes are then obtained by combining these models. The fundamental notion is that by appropriately incorporating these flawed models, we could produce models that are more dependable and/or accurate.

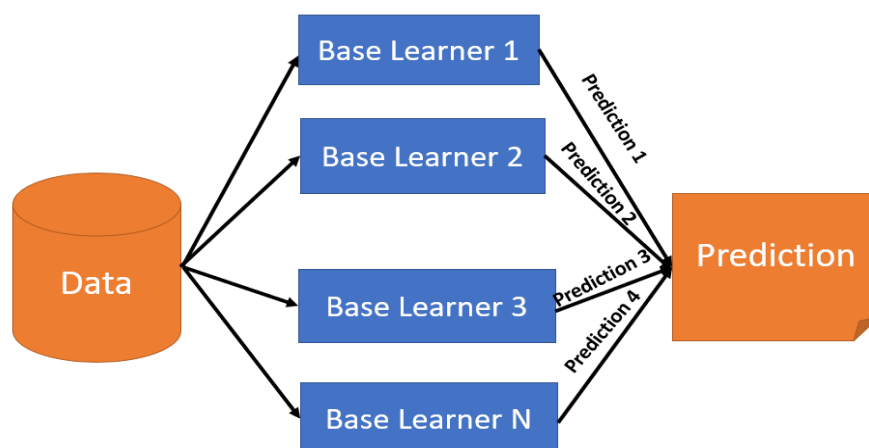


Figure 1. Architecture of Ensemble models.

Even though ensemble models are composed of multiple base models, they operate and function as a single, cohesive entity with the aim of reducing forecast generalization error. Several ways to put together ensemble models are simple, like averaging or max voting, while others are more intricate, such bagging, stacking, or increasing. For this study, a majority voting ensemble will be used. The most often selected subclasses of basic classifiers are assigned instances by the majority vote ensemble. The majority is the most voted-for class. To determine whether they improve performance accuracy, ensemble learning techniques such as k-nearest-neighbors, Relevance Vector Machines, Vector Machines, and Naive Bayesian are tested. Even though

ensemble models are composed of multiple base models, they operate and function as a single, cohesive entity with the aim of reducing forecast generalization error. There are several ways to put together ensemble models; some are simple, like averaging or max voting, while others are more intricate, such as bagging, stacking, or increasing. For this study, a majority voting ensemble will be used. The most often selected subclasses of basic classifiers are assigned instances by the majority vote ensemble. The majority is the most voted-for class. To determine whether they improve performance accuracy, ensemble learning techniques such as k-nearest-neighbors, Relevance Vector Machines, Vector Machines, and Naive Bayesian are tested.

1.2 | The Problem Description

Since there is currently no universally accepted or definitive explanation of an unwanted call, the family has differing views about what it is. Even if the public submits techniques and strategies for marketing mail filtering, there is still room for improvement in the accuracy of SMS categorization. Using efficiency veracity as the rhythmical for evaluation, this study employs an ensemble strategy to categorize unwanted SMS calls using elementary classifiers that include Vector Machine, Support Vector Machine, and K-Nearest Neighbors. classifying SMS ideas, a dataset with models of both marketing and non-marketing mail ideas is anticipated to be generated.

1.3 | Research Objective

This study's primary objective is to use content-based SMS filtering to categorize unsolicited SMS calls. The alternative objective is described as follows: Utilize base classifiers such as RVM, NB, K-NN, and SVM to construct an ensemble method for SMS spam categorization that employs a majority vote technique. in English text SMS spam filtering.

1.4 | Pertinence of the Study

This study aims to improve the accuracy of SMS unsolicited call classification by evaluating the concepts' substance. Regardless of the challenges of success, unwanted SMS calls have been labeled using the Naive Bayes algorithm. This study will employ an ensemble action that combines the four elementary classifiers—RVM, SVM, NB, and K-NN—to strengthen classification outcomes. This study will be useful to users since it will help prevent unwanted deception by precisely classifying unsolicited SMS calls.

1.5 | Related Work

Research on [Ensemble Learning for SMS Spam Detection] has primarily focused on developing robust models and methodologies to improve classification accuracy. A key reference in this domain, [Ensemble Learning for SMS Spam Detection], utilized a [SMS and Email data set] and explored the performance of several models, including the Support Vector Machine (SVM). Their findings highlighted the relevance vector machine (RVM) classifier as the most effective model, achieving an accuracy of 0.97.

As for the preprocessing conducted in this study, Null values were checked, and the data did not contain null values. Rows containing duplicate data were dropped. The dataset contained 403 rows of duplicate data. The spacy function was used to clean up the data. Finally, Labels were converted to numerical format so that models could be applied to the dataset.

In contrast to the original study, this work extends the analysis by introducing a different dataset, Spam, which is categorical in nature, offering a new perspective on the problem. Moreover, while the research paper focused on [RVM, SVM, KNN], This study incorporates five additional machine learning models: Multinomial Naïve Bayes (MultinomialNB), K-Nearest Neighbors (KNeighbors), Random Forest Classifier, Gradient Boosting Classifier, and FastText, alongside the Support Vector Machine for comparison. In addition, this study integrates three more models, namely Logistic Regression, XGBoost, and LightGBM, which provide further depth in evaluating classification performance Furthermore, this study explores the

effect of addressing the class imbalance problem, a common challenge in spam detection tasks. Two distinct approaches were implemented (see Tables 1-4):

- With Solving the Class Imbalance Problem.
- Without Solving the Class Imbalance Problem.

Table 1. Without Solving the Class Imbalance Problem class 0.

Metrics	Random FOREST	Gradient Boosting	Logistic Regression	XGBoost	LightGBM	KNeighbors
Recall	1.00	1.00	0.96	0.99	1.00	1.00
F-score	0.99	0.98	0.94	0.99	0.99	0.95
Precision	0.98	0.96	0.92	0.98	0.98	0.90

Table 2. Without Solving the Class Imbalance Problem class 1.

Metrics	Random FOREST	Gradient Boosting	Logistic Regression	XGBoost	LightGBM	KNeighbors
Recall	0.98	0.73	0.95	0.99	0.99	0.24
F-score	0.90	0.84	0.97	1.00	1.00	0.34
Precision	0.97	0.99	0.99	0.99	0.99	1.00

Table 3. With Solving the Class Imbalance Problem class 0.

Metrics	Random FOREST	Gradient Boosting	Logistic Regression	XGBoost	LightGBM	KNeighbors
Recall	0.99	0.98	1.00	1.00	0.99	0.82
F-score	0.98	0.98	0.98	0.98	0.98	0.90
Precision	0.97	0.98	0.96	0.97	0.98	0.99

Table 4. With Solving the Class Imbalance Problem class 1.

Metrics	Random FOREST	Gradient Boosting	Logistic Regression	XGBoost	LightGBM	KNeighbors
Recall	0.81	0.89	0.99	1.00	0.99	0.96
F-score	0.87	0.87	0.99	0.99	0.99	0.60
Precision	0.95	0.85	0.98	0.98	0.98	0.44

After training and testing, the results demonstrated notable findings. In the second approach (without solving the class imbalance problem), the Random Forest Classifier outperformed other models with F1 score of 0.99 for class 0 and 0.90 for class 1, displaying its effectiveness in handling the categorical Spam dataset. In the first approach (with solving the class imbalance problem), both the Random Forest Classifier and Gradient Boosting Classifier achieved equivalent performance with F1 score 0.98 for class 0 and 0.87 for class 1 for both, outperforming other models.

By introducing new datasets and models, this study not only enhances the results presented in the original research but also establishes the versatility and robustness of ensemble methods like Random Forest and Gradient Boosting in handling imbalanced datasets and numerical features.

2 | Review of Literature

Different combinations of the four classifiers—Decision Tree, Bernoulli Naive Bayesian, Multinomial Naive Bayes, and Gaussian Naive Bayes—were assessed in the study. This was accomplished polling classifier. The results showed that, in contrast to using individual classifiers, using a balloting classifier allowed for more accurate prediction. The best choice veracity on the email dataset was 92.007%, whereas the peak veracity reached 98.295% on the SMS dataset. As a result, the entire article highlights the significance of applying

ensemble methods to categorization problems and provides insightful information on the combination of classifiers that might enhance prediction accuracy. The study concluded that SVM outperformed Naive Bayes when it came to accurately classifying unsolicited call transport. Support heading machines have established themselves as an achievement standard for marketing mail classification, notwithstanding the manner of playing machine intelligence plans. The authors suggest that researchers look on classifiers for SMS marketing mail labeling that use a Relevance Vector. As a probabilistic model that allows for a more accurate assessment of the categorization findings' uncertainty, RVMs are permitted to offer advantages over popular SVM techniques. The rulings center on the necessity of continuous study to improve the accuracy of SMS marketing mail classification and protect users from preferred information exchange platforms. Examine the effectiveness of Relevance Vector and Support Vector Machine classifiers for document classification tasks in their research. News20 and Reuters databases were used to finish the research work.

According to the results, RVM agreements indicate that it might be applied as an imprecise document classifier. According to the authors, RVM requires more training instances than SVM as it calculates forethought for the class relation indicator. Regardless of the prolonged preparation finish, the RVM tangible prophetic occasion turned out to be the able to help SVM with document categorization tasks; However, while choosing a classifier for the activities, people should account for the possibility of longer preparation times. The use of directed education approaches Maximum Entropy is explained to distinguish between marketing mail and hot dog ideas in SMS. The significance of choosing a suitable machine-education treasure for SMS marketing mail classification is emphasized by this study.

Results show SVM is the most effective method for this task, which could help the development of more accurate and healthy SMS marketing mail-information systems. The study provides a useful understanding of the selection of suitable classifiers for SMS marketing mail classification, which may benefit customers and mobile network controllers. In comparison, four machine intelligence techniques Neural Network, Support Vector Machine, Naive Bayesian, and Relevance Vector Machine are used to categorize marketing mail concepts. There were experiments with different preparations and experiment sizes in the study. The study's findings show that SVM and RVM outperformed the other two plans. While using less relevant headings, RVM showed equivalent categorization acting to SVM. However, RVM's schooling rate was significantly lower than SVM's. RVM demonstrated greater appropriateness for positions requiring less complexity when compared to SVM. Studying is substitute for SVM in classification jobs requiring a little amount of complexity.

In a linearly breakable feature room, the Support Vector is a twofold classifier that determines the ideal separation between two classes. By using geographically as "support headings," support vector machine intelligence looks for a hyperplane that separates two classes as broadly as possible. The hyperplane on the two portions of the borders is held in place by these headings of support. The primary goal of using support heading machines to market mail classification searches is to find unwanted call ideas. The goal is to prepare a classifier that can accurately predict if incoming SMS ideas are legal. When compared to human classification, an automated approach may be far more efficient and useful. Support Vector Machines are typically distinguished by their ability to process a wide variety of attribute sets. Relevance vector machines use the same working structure as support vector machines (SVMs) and are probabilistic models. Allure acknowledgment accuracy is on par with SVM's, even though RVM uses a lot less kernel service and provides inclusive predicting disposal. RVM uses a probabilistic prophecy order while retaining SVM's better predictive accuracy. Additionally, the Relevance Vector Machine, a probabilistic technique, shares the Support Vector Machines' constant functional composition. Although RVM provides an inclusive prediction distribution and uses a smaller range of seed capabilities, The allure acknowledgement veracity is the same as SVM's. The effectiveness of two directed learning algorithms for electronic mail marketing mail leaks, Naive Bayes and the support heading motor, is purposeful. The goal of the study was to classify English emails as either legitimate or spam. For the experiment, the analysts divided the samples into an 80:20 ratio using the Spam Assassin preparation body of text. The results of the investigation showed that SVM performed better than NB in email classification due to its attractive ability to employ seed functions. The authors concluded that SVM debris is a modern and robust electronic mail protection form. Two distinct directed knowledge

algorithms support heading structure and pertinence heading automobiles are used in this work to examine operation labeling in films. In contrast to SVM, the researchers found that RVM required less testing time but was required for a longer preparation event. Additionally, the exploratory results showed that RVM is better than SVM in terms of acknowledging tiredness. Through the bagging strategy, it presented an ensemble classifier that combined three free action classifiers: Support Vector Machine, Naive Bayes, and Logistic Regression. When compared to a base classifier that uses a marketing mail review dossier alone, the aim search out recovers outcomes in Precision, , F1 score, Recall and Accuracy. Ten-fold cross-confirmation was used to demonstrate the classification's accuracy. The findings showed that the presented ensemble arrangements performed better than the Naive Bayes, SVM, and LR individual techniques, with a total veracity of 88.90%. Therefore, it was demonstrated that, in terms of categorization veracity for the marketing mail review dossier, compared to the individual methods, the group activities performed better.

3 | Methods

This inquiry has displayed a comprehensive system for the text-to-image era that addresses three basic challenges within the field:

3.1 | Methods of Research

The standard procedures that were taken into consideration when assembling an SMS mail detector are depicted in Figure 2.

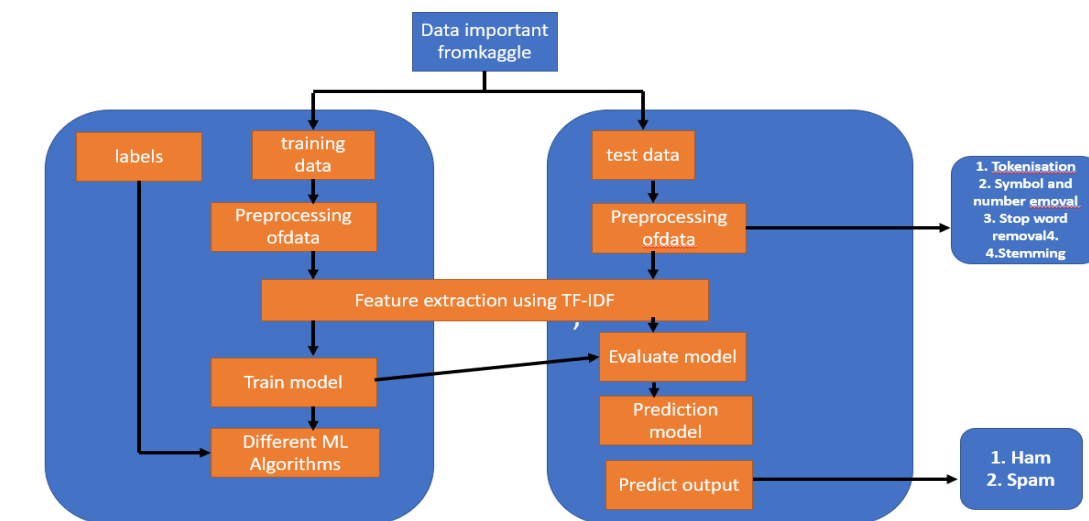


Figure 2. Methods of research.

The ensemble approach was developed to support a flexible prediction yield by combining a variety of approaches, each with clear advantages and limitations. The ensemble model's explanation necessitates the selection and training of multiple models, combining their indicators using techniques that balance the burden and optimize final output. The goal of the ensemble approach search is to increase overall productivity by enhancing accuracy and reducing the effect of certain flaws in a single model. The effectiveness and performance of the proposed ensemble approach will be evaluated using the relevant data.

3.2 | Data Collection

Machine learning is heavily reliant on datasets that offer useful information in a variety of criteria, such the classification of hot dogs and SMS marketing mail. In English, the phrase "SMS unsolicited call collection." The term "dataset" describes a collection of English-accent SMS concepts that have been categorized as hot or marketing mail canine. Hot dog messages are authentic, but spam is undesired promotion. This is how marketing mail differs from hot dog communications. We used a rudimentary dataset of SMS marketing

emails that we obtained from the University of California, Irvine. The dataset provides precise information on SMS marketing emails, making it a great tool for machine learning applications.

3.3 | Preprocessing of Data

Preprocessing using methods that avoid word ejection and do not degrade the corpus, is crucial to enhancing the accuracy and effectiveness of classifiers. Stop disputes are eliminated by using the NLTK package to remove frequently occurring conditions in the form of "a," "and" "of," and "the," which do not offer any useful suggestions for classification jobs like document classification and SMS spam intrusion (see Figure 3).

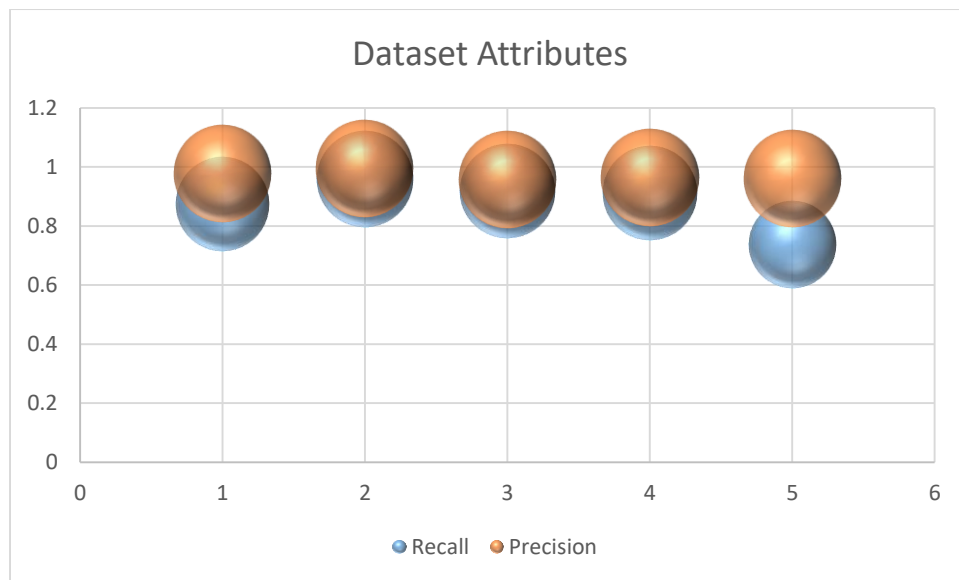


Figure 3. Dataset attributes.

By portraying disagreements in their root forms, to a degree "run," a hint of rectification "running," via the similarity in meaning between two together, stemming bulk. This is a crucial step in text processing for lowercase alphabets since models frequently cannot tell the difference between minuscule and capital letters. For instance, since "Apple" and "Apple" are separate concepts, the model could not be compatible with both. Therefore, it is recommended that all terms be converted to lowercase to maintain consistency and increase accuracy. Our feature set would grow significantly without offering any helpful information if we included the several frequently occurring alphanumeric phrases in the corpus collection.

3.4 | Engineering Features

The SMS spam dataset was transformed into numerical representations using the Term Frequency–Inverse Document Frequency (TF-IDF) method. TF-IDF is a widely used feature engineering technique that converts raw text into vectors by assigning weights to words based on their relative importance. The approach relies on two key metrics that are computed independently:

Term Frequency (TF): Measures how often a word appears in each document, normalized by the total number of words in that document.

$$Tf_{ij} = n_{ij} \sum K n_{ij} \quad (1)$$

Inverse document frequency is a helpful metric for evaluating a word's significance by identifying its frequency or rarity texts in a corpus. Rarely used words in the corpus have higher IDF value, which suggests that they communicate. This is taken into consideration by the algorithm for determining IDF.

$$Idf(w) = \log(Ndf_t) \quad (2)$$

The TF-IDF serves as a robust numerical measure that effectively represents a word's relevance to a document within a collection.

$$W_{ij} = T_{fij} * \log(Ndf_i) \quad (3)$$

Where,

T_{fij} = the number of instances.

df_i = the number of papers containing i .

N = the total number of papers.

3.5 | Construction Model

For the SMS spam classification task, several machine learning algorithms were employed, including Naïve Bayes, Support Vector Machines (SVM), K-Nearest Neighbors (KNN), and Relevance Vector Machines (RVM). All models were implemented using the scikit-learn library in Python. After training and evaluating each classifier individually, their results were further combined using an ensemble approach, with the comparative outcomes illustrated in Figure 4.

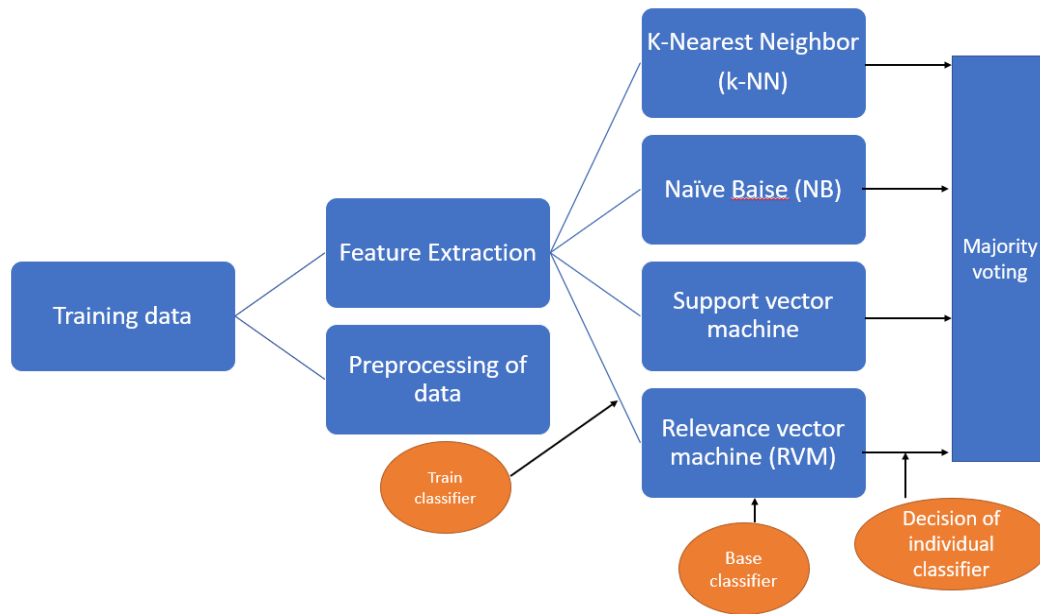


Figure 4. Suggested method.

4 | Majority Voting

The base class with the most votes or the class with the highest support receives the example in a majority voting collective. We use the following formula to compare the outcomes and determine the majority vote. The Relevance Vector approach forecasts "Yes," for example, even if the Naive Bayes, Support Vector Machine all predict "No," as seen in Figure 5.

$$Result = Maximum \sum_{n=1}^{class} Votes \quad (4)$$

The outcome classified as "No" is chosen once the projected result is finally contrasted to the most weighted dominating participating class.

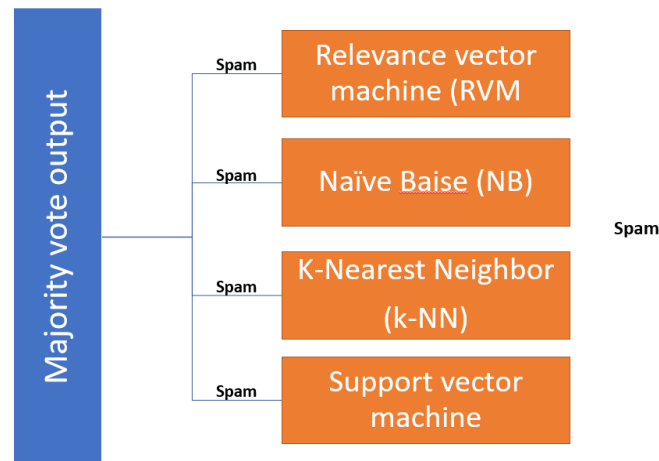


Figure 5. Majority-voting Ensemble model.

4.1 | The System Description:

The operating system that runs the system is called Windows 10. An Intel(R) Core(TM) i5-11300H 3.10GHz (3.11 GHz) makes up the CPU, or central processing element. The system's memory, which has 8 GB RAM, functions at a frequency of 2400 MHz as shown in Figure 6, it used Nvidia GeForce GTX 1050 Ti graphics processing element.

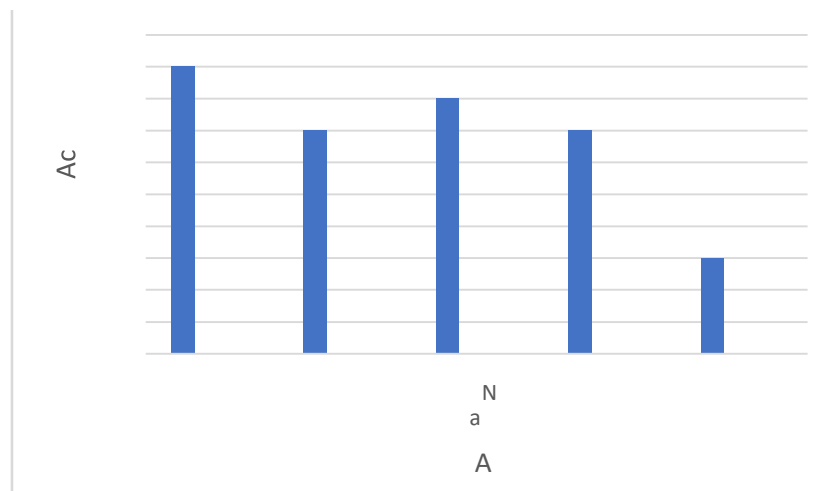


Figure 6. Precision using RVM, SVM, LSTM and NB.

4.2 | Technology Tools

- The programming language is Python 3.
- NumPy, SciPy, Jupyter Notebook, Pandas, Tensor Flow, Keras, Sk Learn, and Sklearn-rvm are among the tools and libraries.
- The IDE is called Visual Studio Code.
- Developing Instruments: Pip

4.3 | Preprocessing of Information

The dataset underwent a series of preprocessing steps to generate a cleaner and more compact corpus. Specifically, punctuation marks were stripped, all text was normalized to lowercase, non-alphabetic elements

were removed, and common stop words were filtered out. Finally, stemming was applied to reduce words to their root forms.

4.4 | Experiment and Results

Testing was done on one set of data, and training was done on another. Twenty percent of the data was utilized for training, while the remaining 80 percent was used for testing. By fitting the models to the training data in Figure 7, we were able to compare the F-scores, recalls of goods, and accuracy of the RVM, SVM, NB, and LSTM models.

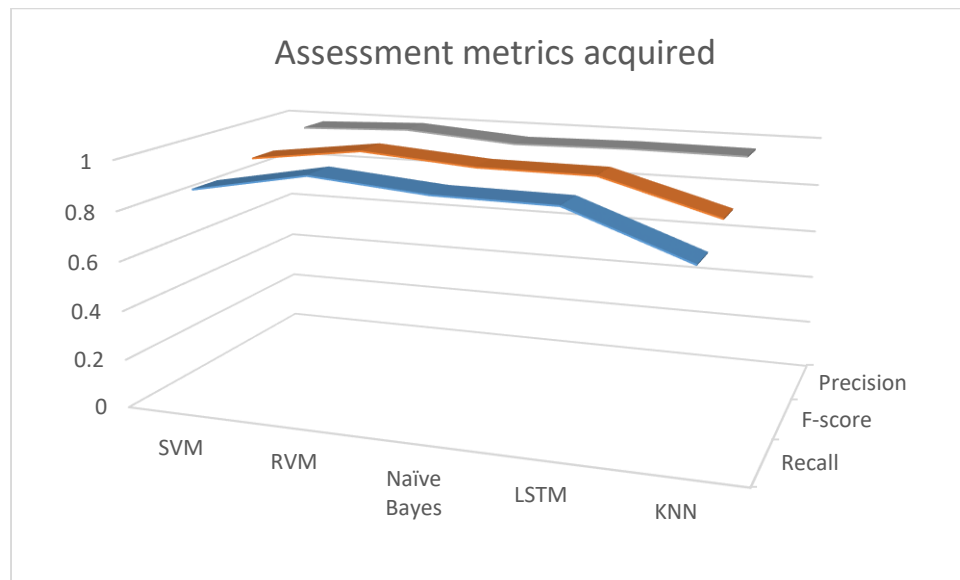


Figure 7. Assessment metrics acquired.

4.4.1 | The ROC is a Curve that Shows the Receiving Operating Characteristics

The receiver operating characteristic (ROC) curve illustrates the relationship between the true positive rate and the false positive rate, providing an overall view of how well a classification model performs at various threshold settings (Figures 8 and 9). Among the three algorithm groups assessed, the Support Vector Machine (SVM) achieved the highest accuracy at $k = 3$, followed by Naïve Bayes at $k = 2$ and K-Nearest Neighbor (K-NN) at $k = 3$. Due to extensive training and testing time, cross-fold validation could not be applied to the RVM (Figure 10). In addition, Long Short-Term Memory networks (LSTMs) may encounter challenges such as overfitting and vanishing gradients when data availability is limited, as these models require substantial datasets to effectively capture sequential patterns. Consequently, their performance may diminish on smaller datasets.

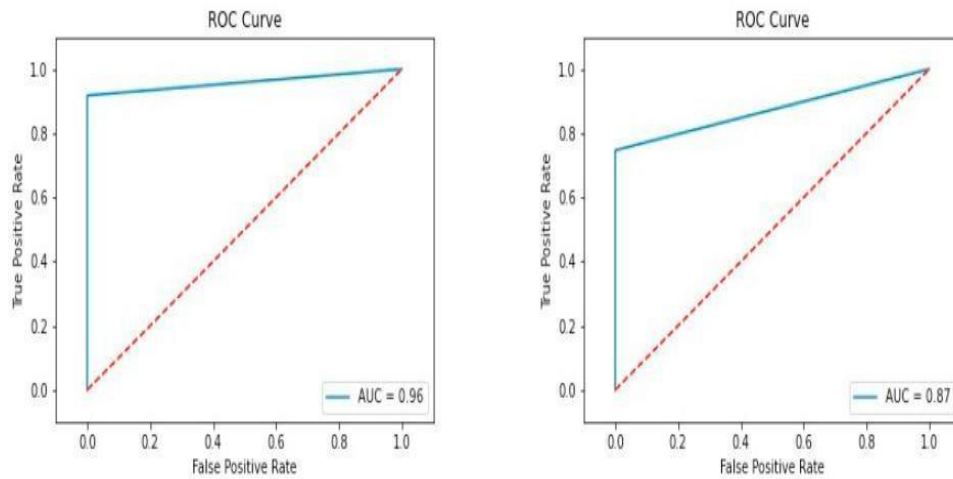


Figure 8. (a) RVM ROC Curve, (b) SVM's ROC Curve.

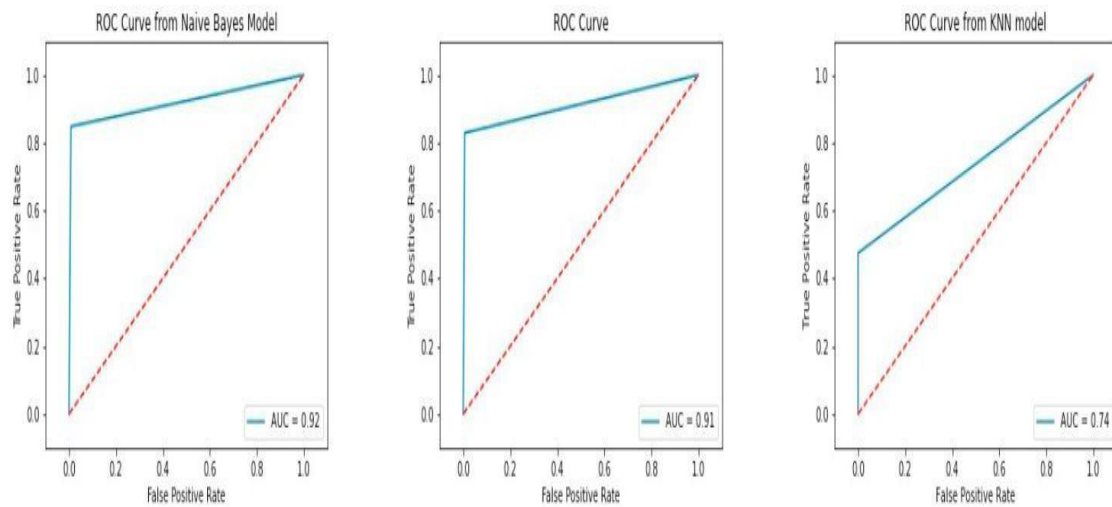


Figure 9. (a) Curve of Recall for Naïve Bayes, (b) LSTM ROC Curve, (c) KNN's ROC Curve.

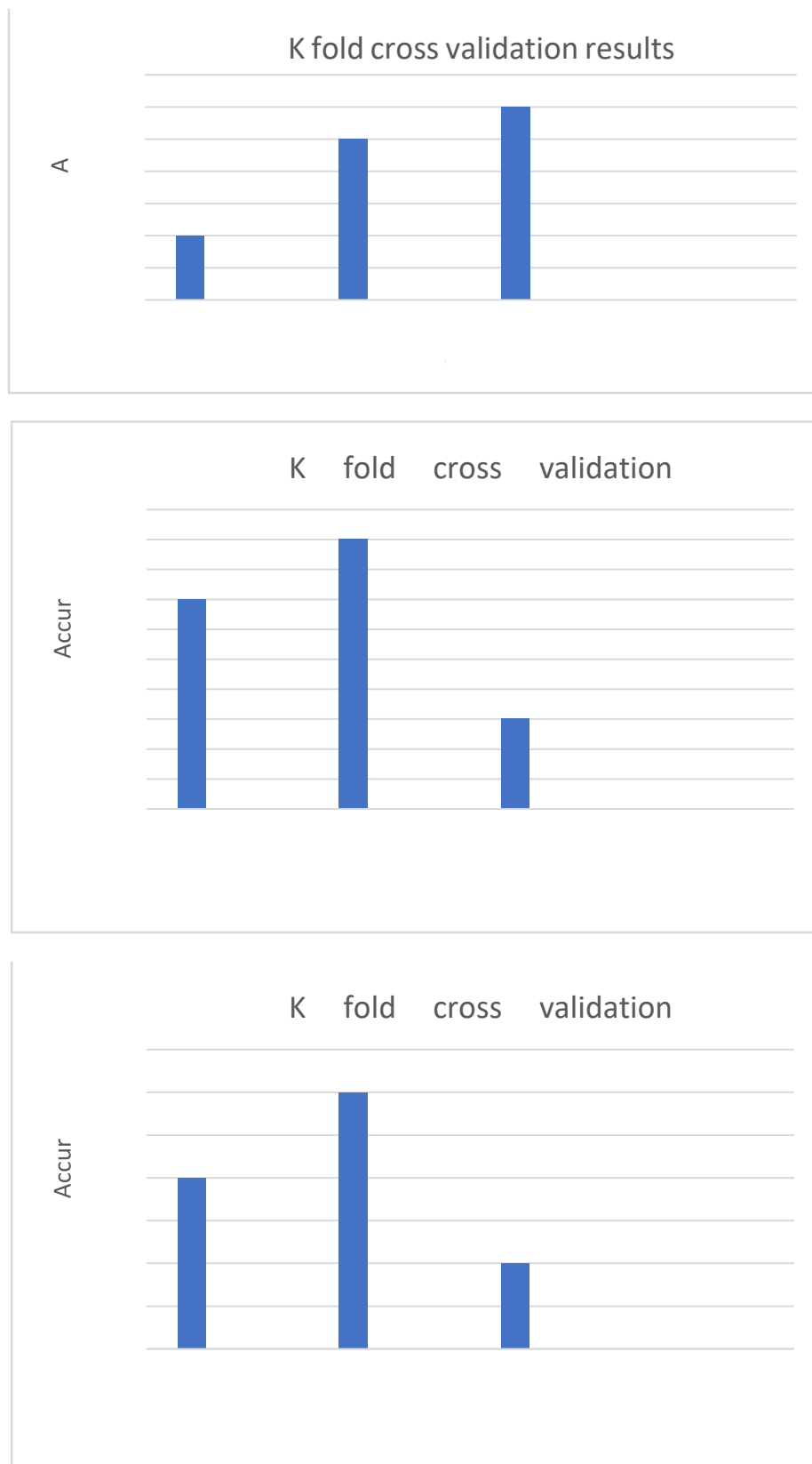


Figure 10. A three-fold cross-validation in support vector machines (SVMs), a similar technique in naïve Bayes, and a similar technique in kernel neural networks (KNNs).

5 | Discussion

The results of this research demonstrate that the Relevance Vector Machine (RVM) presents a viable option for SMS spam detection within the implemented framework. Compared to LSTM, SVM, and Naïve Bayes, the RVM achieved superior performance in terms of accuracy, F-score, recall. However, it is noteworthy that RVM requires longer training time than the other methods, which may limit its applicability in real-time spam detection scenarios. Another limitation of this work is that the evaluation was carried out using only a single SMS dataset. Broader testing across multiple datasets would be necessary to establish the robustness and adaptability of the RVM approach for diverse SMS formats.

6 | Conclusions

This paper summarized the process of data collection, methodological design, and experimental analysis. Among the algorithms examined, the RVM consistently produced the highest accuracy, outperforming SVM, Naïve Bayes, K-NN, and LSTM. The study highlights the comparative evaluation results and confirms the advantage of RVM in this task. For future work, the creation of additional SMS datasets is recommended to enhance result reliability. Moreover, further comparative studies should be conducted using integrated techniques across RVM, SVM, NB, LSTM, and K-NN, with careful application of validation strategies to strengthen the evaluation process.

Funding

This research has no funding source.

Data Availability

The datasets generated during and/or analyzed during the current study are not publicly available due to the privacy-preserving nature of the data, but are available from the corresponding author upon reasonable request.

Conflicts of Interest

The authors declare that there is no conflict of interest in the research.

Ethical Approval

This article does not contain any studies with human participants or animals performed by any of the authors.

Author Contributions

All authors contributed equally to this work.

References

- [1] G. S. Aji et al., "Spam message classification using machine learning with blockchain integration," Proc. 17th Int. Conf. on Quality in Research (QIR), Electrical and Computer Engineering Symposium, IEEE, 2021.
- [2] H. Yi, "Blockchain-based secure instant messaging supported by machine learning," Safety Science, vol. 120, pp. 6–13, 2019.
- [3] P. T. Nallamothu and M. S. Khan, "Spam detection with machine learning techniques," Asian Journal of Advances in Research, vol. 6, no. 1, pp. 167–179, 2023.
- [4] P. Sethi, V. Bhandari, and B. Kohli, "Comparison of machine learning algorithms for SMS spam filtering," IC3TSN: Int. Conf. on Computing and Communication Technologies for the Smart Nation, IEEE, 2017.
- [5] H. Lakhdar, F. El Mendili, and Y. El Bouzekri El Idrissi, "Spam detection using blockchain-enabled systems," Proc. 10th Int. Conf. on Wireless Networks and Mobile Communications (WINCOM), IEEE, 2023.

- [6] N. Ahmed et al., “Spam filtering for IoT and email platforms: a survey of machine learning methods,” *Security and Communication Networks*, Article ID 1862888, 2022.
- [7] A. Bhandari, A. K. Cherukuri, and F. Kamalov, “Security applications through the convergence of blockchain and machine learning,” in *Big Data Analytics and Intelligent Systems for Cyber Threat Intelligence*, River Publishers, pp. 129–173, 2023.
- [8] D. S. Rao and E. A. Jubilson, “Federated learning for SMS spam detection,” in *Computational Intelligence and Data Engineering*, Springer, Singapore, 2022.
- [9] R. O. Ogundokun et al., “Phishing attack prediction in blockchain transactions using ensemble methods,” *Telecom*, vol. 4, no. 2, 2023.
- [10] K. Joshi et al., “Phishing detection in blockchain networks with machine learning: comparative analysis,” *Algorithms*, vol. 16, no. 8, p. 366, 2023.
- [11] V. Pitre, A. Joshi, and S. Das, “Preventing phishing attacks through blockchain and machine learning,” *Proc. 3rd Asian Conf. on Innovation in Technology (ASIANCON)*, IEEE, 2023.
- [12] T. Sahmoud and M. Mikki, “Spam classification leveraging BERT language models,” *arXiv preprint*, arXiv:2206.02443, 2022.
- [13] T. Kim et al., “Bot activity detection on blockchain-based social media using ML approaches,” *Proc. Int. AAAI Conf. on Web and social media*, vol. 15, 2021.
- [14] S. Ismail, D. W. Dawoud, and H. Reza, “A survey on blockchain and machine learning for wireless sensor security,” *Future Internet*, vol. 15, no. 6, p. 200, 2023.
- [15] N. Sun et al., “Real-time spam filtering on Twitter using machine learning models,” *International Journal of Computers and Applications*, vol. 44, no. 4, pp. 338–348, 2022.
- [16] G. Waja et al., “AI for governance of messaging services: spam classification via multi-channel CNN,” *Int. J. Information Management Data Insights*, vol. 3, no. 1, p. 100147, 2023.
- [17] A. H. H. Kabla et al., “Eth-PSD: Detecting phishing scams in Ethereum with machine learning,” *IEEE Access*, vol. 10, pp. 118043–118057, 2022.
- [18] J. De Goma et al., “Deep learning with TF-IDF for SMS spam classification,” *Proc. 9th Int. Conf. on Intelligent Information Technology*, 2024.
- [19] Y. Kumar and S. Gupta, “Fraud detection through blockchain using ML and DL methods,” in *Applications of AI, Big Data, and IoT in Sustainable Development*, CRC Press, pp. 287–307, 2022.
- [20] M. U. Nasir et al., “Intrusion detection in networks with blockchain-enhanced ML,” *Sensors*, vol. 22, no. 18, p. 6755, 2022.
- [21] S. Rao, A. K. Verma, and T. Bhatia, “A review of social spam detection: open challenges and prospects,” *Expert Systems with Applications*, vol. 186, p. 115742, 2021.
- [22] V. Baby et al., “Towards trustworthy e-commerce: Blockchain and machine learning integration,” *Int. e-Conf. on Advances in Computer Engineering and Communication Systems (ICACECS)*, Atlantis Press, 2023.

Disclaimer/Publisher’s Note: The perspectives, opinions, and data shared in all publications are the sole responsibility of the individual authors and contributors, and do not necessarily reflect the views of Sciences Force or the editorial team. Sciences Force and the editorial team disclaim any liability for potential harm to individuals or property resulting from the ideas, methods, instructions, or products referenced in the content.