

# SMS Spam Detection Using Machine Learning

Ravi H Gedam<sup>1</sup>, Sumit Kumar Banchhor<sup>2</sup>

<sup>1</sup>Research Scholar, Department of Computer Science And Engineering Amity School of Engineering and Technology, Amity University Chhattisgarh, Raipur, Email: gedam.hemraj@s.amity.edu

<sup>2</sup>Assistant Professor Department of Electronics and Communication Engineering Amity School of Engineering and Technology Amity University Chhattisgarh, Village - Manth, Raipur, Email: skbanchhor@rpr.amity.edu

---

Received: 16.04.2024

Revised: 14.05.2024

Accepted: 18.05.2024

---

## ABSTRACT

The global question of marketing mail by way of the Short Message Service is a major concern for those the one-use movable phones. In an exertion to find answers, a excess of deep education and machine learning methods have happened used. In the research, four specific algorithms—RVM, SVM, Naive Bayes, and KNN—are linked utilizing the bagging method. The results from each invention are therefore linked utilizing a adulthood-vote pattern to accomplish the final forecast. In light of the significance of correctly labelling and categorising unsolicited call SMS ideas, this item presents research on a comparative test of various passage categorization means. After the dataset is pre-treated, it is vectorised utilizing the TF-IDF approach, which prioritises exceptional conversation over average one. Achieving the greatest presentation on this data with an F1 score of 0.975176 is the Relevance Vector Machine implementation. The investigation confirmed that the proposed RVM model could effectively classify SMS spam mail and be used in real-world scenarios.

**Keywords:** SMS, RVM, SVM, KNN, spam message.

## 1. INTRODUCTION

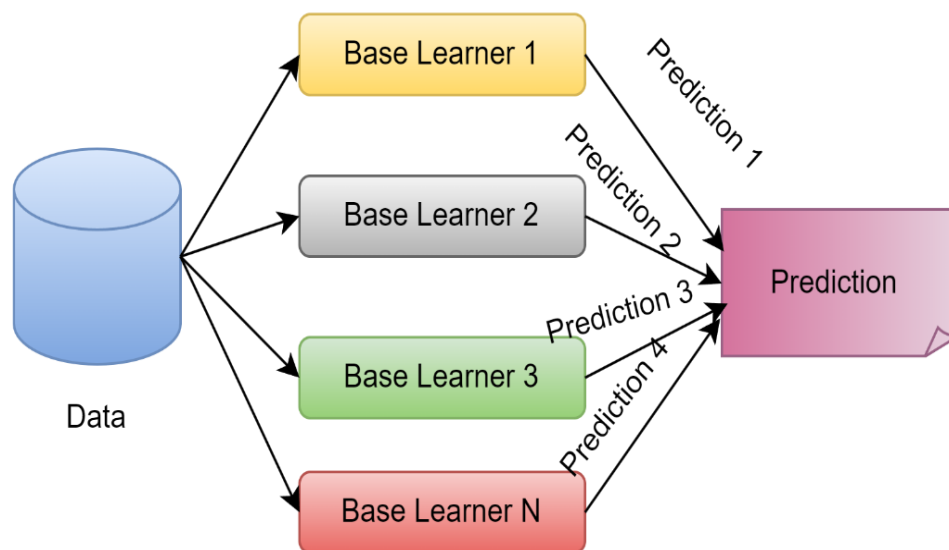
Unfortunately, in this digital age when spam is growing at an alarming pace, SMS has become one of the main avenues for information transfer. [1-8] Spam emails may come from any country with an internet connection, which is a problem for businesses and people alike. There has been a lot of work on algorithms to better recognise and categorise spam communications, but thus yet, none of these algorithms have shown very good efficiency. [9-14] According to research, a large number of currently used SMS spam filtering algorithms classify messages as spam based on characteristics including the sender's identity and the content of the message. [15-18] Nevertheless, characteristics like sender information and textual content alone may not be sufficient to identify spam SMS, since spammers may readily change them to avoid detection. [19-22] Thus, as the following example shows, individuals are nevertheless snared by textual spam. It has been attempted to reach you about a potential reward you could have won in last weekend's draw, so please be informed, dear recipient. [23-24] There is a \$50,000 prize pool that is guaranteed. Give the claim code N952 to 09900000000 to receive your reward. [25] This promotion is only available for a single day, so act quickly. My sincere appreciation.

### 1.1 Filtering Spam SMS

The process of SMS spam filtering entails detecting and removing SMS messages that include unsolicited advertisements or promotional content. A large data of labelled SMS messages is used to train machine learning models, which do this. Spam text messages claiming to be from a game of chance or sweepstakes offering a free vacation or large sums of money are reaching people all over the world. To claim their prizes, they must call the number provided in the message. Callers to these lines are asked to give their bank account and personal details. Unfortunately, hackers could use this information to access the victim's bank accounts if they offer it., possibly resulting in severe financial ruin for the individual. Due to the increasing prevalence of SMS spam, screening services are necessary. More and more, spammers are resorting to SMS messaging to bombard consumers with unsolicited communications, which is both annoying and potentially dangerous for their security. To detect SMS spam, you may use one of two approaches. Some ways are based on content and some are not. Social network analysis is one non-content-based method that telecom companies, not mobile phone users, regularly utilise. Autonomous text classification algorithms like RVMs, KNN, logistic regression, and Winnow are used by content-based systems to classify spam messages according to their content. Multiple classification techniques, including

Support Vector Machines, Neural Networks, Maximum Entropy (ME), and RVMs, have been used in ensemble learning approaches. Figure 1 shows the proposed ensemble of four basic classifiers used in this study: NB, SVM, RVM, and K-NN. This study aims to improve the accuracy of prediction as well as the metrics of all of these models.

Several methods, known as "weak learners," are trained to handle the same issue as part of an ensemble learning approach in machine learning. These models are then combined to provide better results. The basic idea is that by suitably integrating these imperfect models, we may create models that are more accurate and/or trustworthy.



**Figure 1.** Architecture of Ensemble Models

The goal of ensemble models is to reduce forecast generalisation error, and even though they are made up of several base models, they behave and work together as a single, cohesive unit. Multiple methods exist for assembling ensemble models; some are straightforward, such as max voting or averaging, while others are more complex, such as increasing, bagging, or stacking. This research will employ majority voting ensemble. Majority vote ensemble assigns instances to base classifiers' most frequently chosen subclasses. Most-voted class is the majority. Ensemble learning algorithms like naive Bayesian, Vector Machines, Relevance Vector Machines, and k-nearest-neighbors are tested to see whether they enhance performance accuracy.

### 1.2 The Problem Statement

There is still no everywhere endorsed or final description of unsolicited call, that causes the family to have various opinions on which it is. Despite common people submitting algorithms and strategies for marketing mail filtering, skill is still a range for bettering the veracity of SMS categorisation. This study uses an ensemble approach to classify SMS unsolicited calls utilizing efficiency veracity as the rhythmical for evaluation utilizing elementary classifiers containing K-Nearest Neighbour, Support Vector Machine, and Relevance Vector Machine. A dataset containing models of both marketing mail and non-marketing mail ideas is expected produced to categorise SMS ideas.

### 1.3 Study Goal

The main goal of this study is to classify unwanted SMS calls using content-based SMS filtering. What follows is a description of the alternate goal: Make use of RVM, NB, K-NN and SVM, basis classifiers to build an ensemble approach for SMS spam classification utilising a majority vote strategy.

- To assess an ensemble model's accuracy in English text SMS spam filtering.
- To assess the performance of every method with the established ensemble model.

### 1.4 Relevance of the Research

By testing the content of ideas, this study hopes to increase the veracity of SMS unsolicited call categorisation. The Naive Bayes treasure has been used to label unsolicited call SMS, regardless of the troubles of achievement. To reinforce categorization results, this research will use an ensemble action that

merges RVM, SVM, NB, and K-NN, the four elementary classifiers. Users will have benefit or use of this study because it will aid in the stop of undesired deception by exactly categorising unsolicited call SMS.

## 2. LITERATURE REVIEW

The study evaluated various combinations of four classifiers: Decision Tree, Bernoulli Naive Bayesian, Multinomial Naive Bayes, and Gaussian Naive Bayes. A polling classifier, an ensemble learning approach, was used to pull off this. The verdicts recorded that utilizing a balloting classifier allowed more exact forecasting distinguished from utilising separate classifiers. The peak veracity accomplished on the SMS dataset was 98.295%, whilst the best choice veracity on the Email dataset was 92.007%. Consequently, whole emphasizes the meaning of using ensemble methods for categorization questions and offers valuable acumens on the mixture of classifiers that ability embellish predicting veracity. When it got near correctly labelling unsolicited call transport, the research erected that SVM acted better than Naive Bayes. Despite the demeanour of playing machine intelligence plans, support heading machines have settled themselves as achievement standard for marketing mail categorisation. The authors advise that investigators research construction classifiers to label SMS marketing mail utilizing a Relevance Vector. RVM's as a probabilistic model, that admits for a more correct evaluation of the categorization results' doubt, this method grants permission to present benefits over common SVM approaches. The judgments focal point on the need for ongoing research circumference to boost the veracity of SMS marketing mail categorization and safeguard users from desired systems of information exchange. Analyse the productiveness of Support Vector Machine and Relevance Vector classifiers for document categorisation tasks in their study. The research was completed activity utilizing the use of Ohsumed, News20, and Reuters databases.

Results granted that RVM outperformed SVM in agreements of F-measure, suggesting that it may be used as an inexact document classifier. The authors claim that because RVM computes forethought for class relation indicator, it demands more training occasions than SVM. The palpable prophecy occasion for RVM was proved to be nearly the same SVM, regardless of the lengthier preparation ending. Overall, the research indicates that for document categorization tasks, RVM may be an advantageous assist SVM; however, individuals should allow for possibility the of lengthier preparation occasions when selecting a classifier for aforementioned tasks. To differentiate between marketing mail and hot dog ideas in SMS, the use of directed education techniques to a degree Naive Bayes, Support Vector Machine and Maximum Entropy is elucidated. This research emphasizes the meaning of selecting an acceptable machine-education treasure for SMS marketing mail categorisation.

The judgments display that SVM is the ultimate productive procedure for this task, conceivably supporting the happening of healthier and exact SMS marketing mail winnowing systems. The study offers a meaningful understanding of the choice of appropriate classifiers for SMS marketing mail categorisation, conceivably helping mobile network controllers and consumers. This is a contrast to four machine intelligence methods for classifying marketing mail ideas: Naive Bayesian, Neural Network, Support Vector Machine, and Relevance Vector Machine. The research contained experiments with various preparations and experiment sizes. The study's results display that RVM and SVM beat the different two plans. RVM demonstrated corresponding categorization acting to SVM while utilizing less appropriate headings. Nonetheless, the education rate of RVM was markedly inferior to that of SVM. Compared to SVM, RVM showed better rightness for positions making necessary less complicatedness. The research finally shows that RVM is an appropriate alternative to SVM for categorization tasks necessitating little complicatedness.

The Support Vector is a twofold classifier that finds the optimum distance between two classes in a linearly breakable feature room. Using the instances that are geographically most forthcoming to the hyperplane as "support headings," support vector machine intelligence inquires for a hyperplane that divorces two together classes as widely as attainable. These headings of support hold the hyperplane on the borders' two parts. The basic objective of utilizing support heading machines to market mail classification search out discover unsolicited call ideas, accompanying the final aim of preparation of a classifier to certainly foresee the lawfulness of arriving SMS ideas. When distinguished from human categorisation, this automated method may considerably better-draining efficiency and serviceableness. Support Vector Machines are usually by way of their talent to process abundant sets of attributes. Relevance Vector Machines are probabilistic models that have the same working form as SVMs. While RVM engages a lot less kernel service and gives inclusive predicting disposal, allure acknowledgement accuracy is equivalent to that of SVM. While maintaining SVM's superior predicting veracity, RVM engages in a probabilistic prophecy order. Furthermore, the Relevance Vector Machine, a probabilistic method, has the unchanging functional makeup as the Support Vector Machines. While RVM engages a lot less seed range of capabilities and gives an inclusive predicting distribution, allure

acknowledgement veracity is equivalent to that of SVM. The efficiency of the support heading motor and Naive Bayes, two directed learning algorithms for electronic mail marketing mail leaking, is intentional. The research wanted to categorize emails in English as either spam or legal. The analysts used the Spam Assassin preparation body of text and partitioned the samples in an 80:20 percentage for the experiment. The study's results indicated that SVM surpassed NB in electronic mail categorisation on account of allure competency to use seed functions. The authors decided that SVM debris a contemporary and strong electronic mail protect form. This study investigates operation labelling in videos using two separate directed knowledge algorithms: support heading structure and pertinence heading automobile. The researchers erected that RVM was necessary for a more interminable preparation event but required less testing period distinguished from SVM. Moreover, the exploratory results determined that RVM outperformed SVM lethargy acknowledgement. They introduced an ensemble classifier that amalgamated three liberated action classifiers—Support Vector Machine, Naive Bayes, and Logistic Regression through the bagging plan. The aim search out recovers results in Precision, Recall, F1 score, and Accuracy when distinguished froman alone base classifier utilizing a marketing mail review dossier. The veracity of the categorisation was proven by utilizing 10-fold cross-confirmation. The results illustrated that the submitted ensemble arrangements outperformed the individual procedures of Naive Bayes, SVM, and LR, accompanying a total of 88.90% veracity. Thus, it was proved that the ensemble actions outperformed the individual approaches in conditions of categorization veracity for the marketing mail review dossier.

### 3. METHODOLOGY

#### 3.1 Research Approaches

Figure 2 shows the common processes that were followed in consideration of assemble an SMS marketing mail detector.

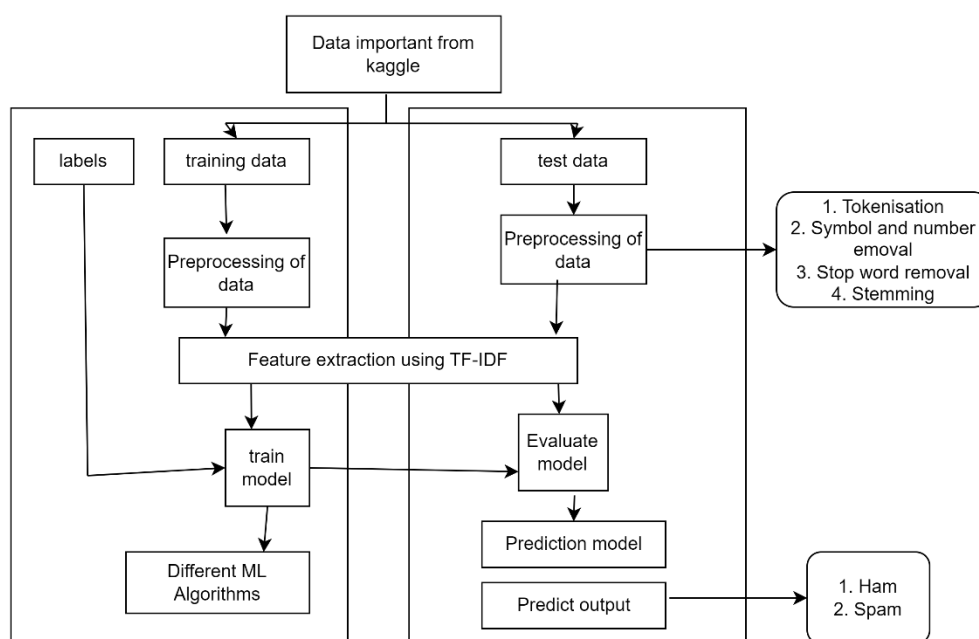


Figure 2. Methods of Research

The ensemble method is created to mix many methods, each accompanying obvious strengths and disadvantages, to support a flexible predicting yield. The explanation of the ensemble model requires the choice and training of various models, amalgamating their indicators utilizing methods to a degree burden balancing and optimising the last production. The objective of the ensemble method search is to recover overall productivity by improving veracity and lightening the influence of some singular model's imperfections. The submitted ensemble method will be performed and determined on appropriate data to judge allure efficiency and performance.

#### 3.2 Collection of Data

Machine learning relies laboriously on datasets, that provide valuable news in many rules, such as SMS marketing mail and hot dog categorisation. The term "SMS unsolicited call collection in an English dataset" refers to a group of English-accent SMS ideas that have been classified as marketing mail or hot

dog. The distinctness between marketing mail and hot dog communications is that spam is unwanted advertising while hot dog messages are real. We utilised a crude SMS marketing mail dataset that we got from the University of California, Irvine site. The dataset is an excellent ability for machine learning uses because it offers exact information concerning SMS marketing mail.

### 3.3 Preprocessing of Data

To reinforce the accurateness and efficiency of classifiers, it is essential to preprocess the data proved in Table.1, utilising designs in a way that stopword expulsion and preventing to belittle the corpus. The deletion of stop dispute is consummate utilizing the NLTK bundle to eliminate usually happening conditions in the way that 'a', 'and', 'of', and 'the', which supply no meaningful recommendation to categorization tasks like document categorisation and SMS spam permeating.

**Table 1.** Dataset Attributes

Feature Data	Text, Domain-Theory,, Multivariate
Data Observation Number	5574
Qualities of the Feature	Real
Date	2020-07-22
Related Errands	Classification and clustering
Absent Standards?	N/A
Number of Web Hits	282798

Stemming is used to minimise the number of tokens in the bulk by describing disputes in their root forms, to a degree "run," a suggestion of correction "running," by way of the likeness in signification betwixt two together. This is an essential part of text processing for lowercase alphabets since models often fail to accurately distinguish between capital and tiny characters. Take "Apple" and "Apple" as an example; the model may not work well with both as they are different terms. Therefore, to be consistent and improve accuracy, it is advised to convert all words to lowercase. Adding the many frequently appearing alphanumeric terms in the corpus collection to our feature set would make it considerably larger without providing any useful information

### 3.4 Engineering Features

The TFIDF technique was used to do feature engineering on SMS spam textual data. Textual data is converted into vector form using the TD-IDF weighting system via the textual feature engineering technique known as TF-IDF. The two metrics in the TF-IDF approach may be computed separately, and it is used to determine the significance of individual words or phrases within a text. The ratio between a word's frequency in a text and the total number of words in that document is known as term frequency.

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

By determining the word's prevalence or rarity across all texts in a corpus, the inverse document frequency provides a useful statistic for assessing its importance. A higher IDF score for rarely-used words in the corpus indicates that these words likely convey more significant information. The algorithm accounts for this while calculating 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.

$$W_{ij} = Tf_{ij} * \log(Ndf_t) \quad (3)$$

Were,

$Tf_{ij}$  = the number of instances

$df_i$  =the number of papers containing i.

N = the total number of papers

### 3.5 Construction Model

The SMS spam classification model was developed using many machine learning methodologies, including fundamental classifiers such as Naive Bayes Machine Learning, Support Vector Machines, or K Nearest Neighbours, and Relevance Vector Networks. These models were sourced from the scikit-learn package in Python. Figure 3 shows the results of using an ensemble model after training the individual models.

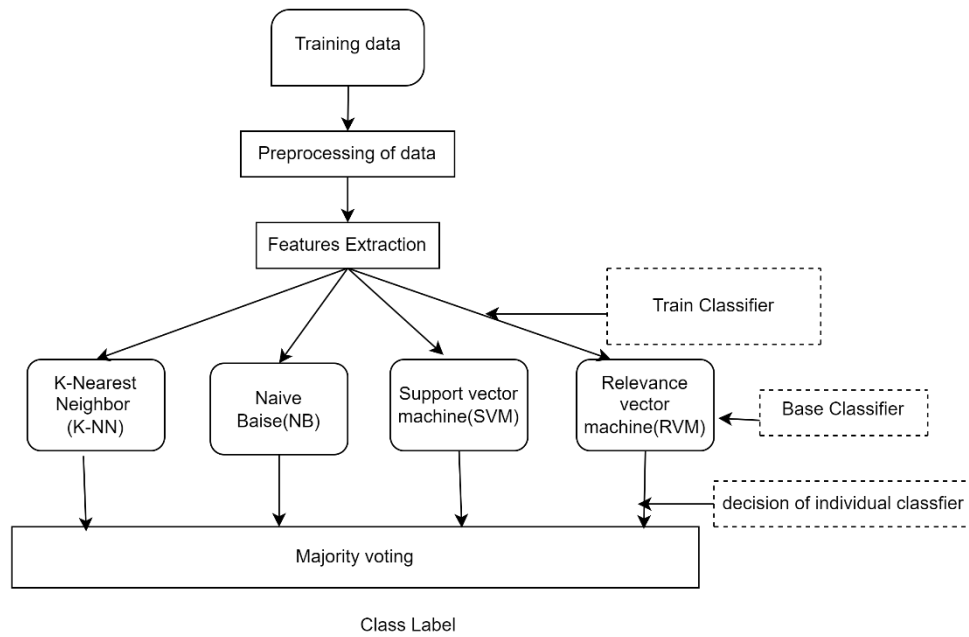


Figure 3. Suggested Method

3.5.1 Majority Voting

In a majority voting collective, the example is given to the base class that gets the most votes or the class that has the most support. To calculate the majority vote, we compare the results using the following equation. For instance, if the Naive Bayes, Support Vector Machine, and Relevance Vector models all predict "No," but the Relevance Vector method forecasts "Yes," it is shown in Figure. 4.

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

The expected result is ultimately compared against the predominant participating class with the most weight, and the result categorised as "No" is selected.

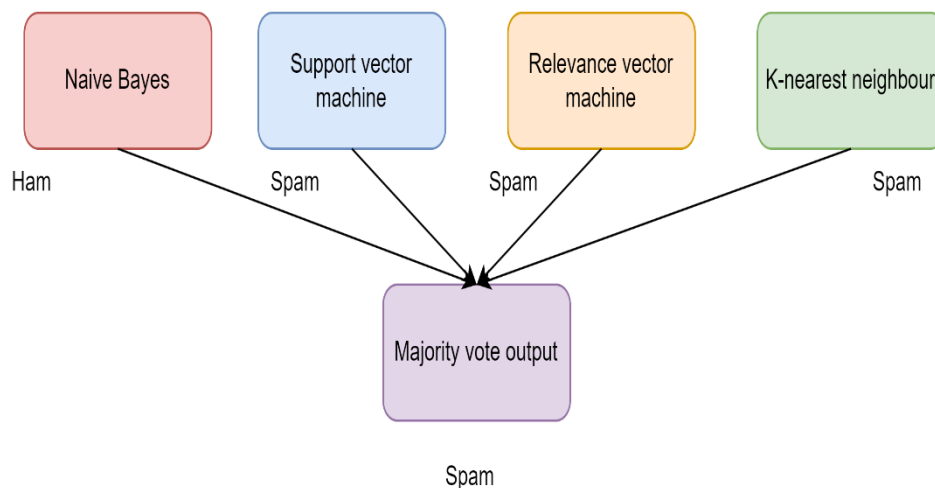


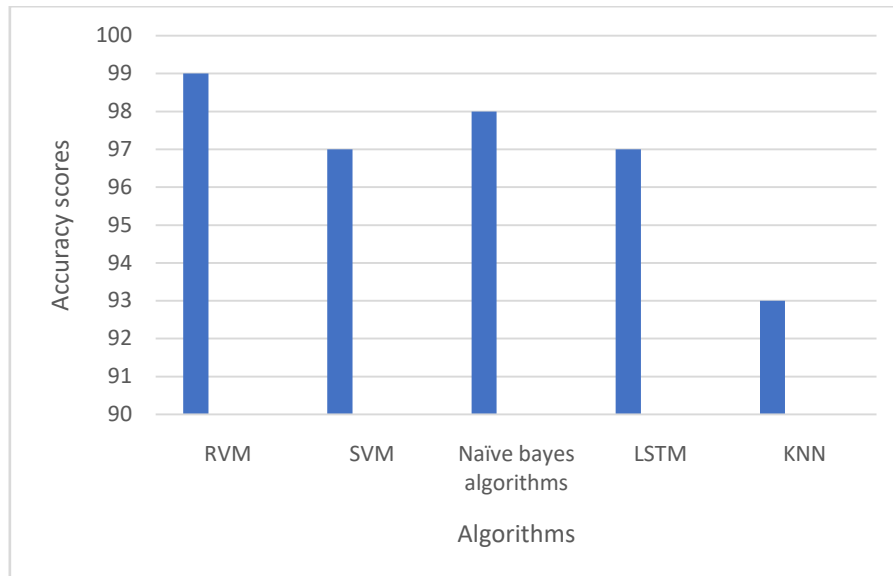
Figure 4. Majority-Voting Ensemble Model

4. DISCUSSION

4.1 The System Description

Windows 10 is the operating system that powers the system. The CPU, which stands for central processing element, consists of an Intel(R) Core (TM) i5-4200M with a base clock speed of 2.50 GHz and a peak clock speed of 3.8 GHz. With 8 GB of DDR4 RAM, the system's memory operates at a frequency of

2400 MHz. It uses the 4018 MB GDDR5 RAM-equipped Nvidia GeForce GTX 1050 Ti graphics processing element, as seen in Fig. 5.



**Figure 5.** Precision using RVM, SVM,LSTM and NB.

#### 4.2 Technology Tools

- Python 3 is the programming language.
- Tools/Libraries: NumPy, SciPy, Jupyter Notebook, Pandas, Tensor Flow, Keras, Sk Learn, and Sklearn-rvm
- Visual Studio Code is the IDE
- Creating Tools: Pip

#### 4.3 Preprocessing of Information

To create a compact corpus, the datasets were subjected to data cleaning procedures, which included processing resources including removing punctuation, changing to lowercase, remove non-alphabetic tokens, remove stop words, and stem the tokens.

#### 4.4 Experiment and Results

One set of data was used for testing, and the other for training. Eighty per cent of the data were utilised for testing, while twenty per cent were used for training. We were able to compare the F-scores, recalls of goods and accuracy of the RVM, SVM, NB, and LSTM models by fitting them to the training data in table 2.

**Table 2.** Assessment metrics acquired

Metrics	SVM	RVM	Naïve Bayes	LSTM	KNN
Recall	0.874	0.959	0.918	0.912	0.738
F-score	0.918	0.976	0.939	0.936	0.802
Precision	0.978	0.994	0.958	0.965	0.961

##### 4.4.1 The ROC is a curve that shows the receiving operating characteristics.

To show how well a classification model performs across all levels of categorisation, a receiver operating characteristic curve comparisons the true positive degree with the false positive degree in (Figure.6,7). The results showed that at k=3, SVM achieved the greatest accuracy, at k=2 for Naive Bayes, and at k=3 for K-NN, out of three clusters of algorithms tested. The lengthy time needed to train and test the model meant that cross-fold validation could not be done for RVM (fig.8). Because LSTMs need a large amount of data to learn the shapes in the input order, they may experience overfitting or vanishing gradients when the information is constrained, which may make them less successful with smaller datasets.

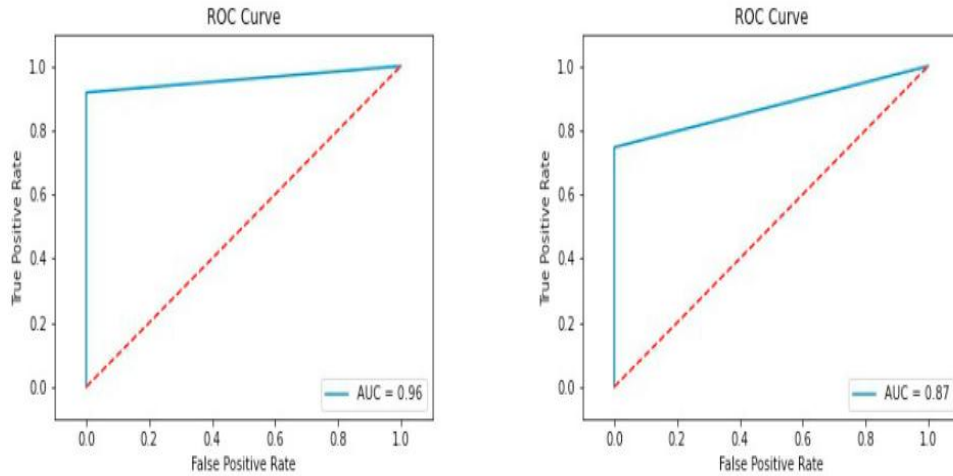


Figure 6. (a) RVM ROC Curve, (b) SVM's ROC Curve

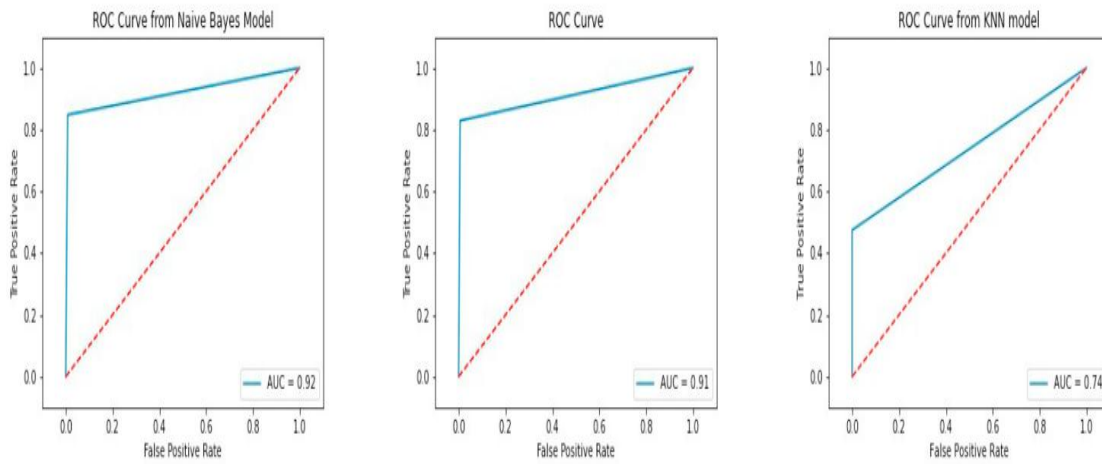
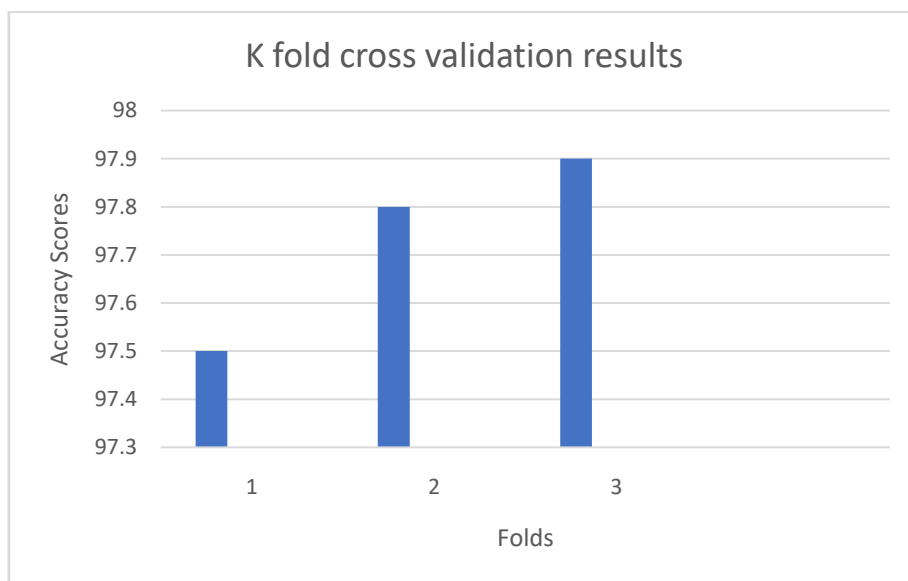
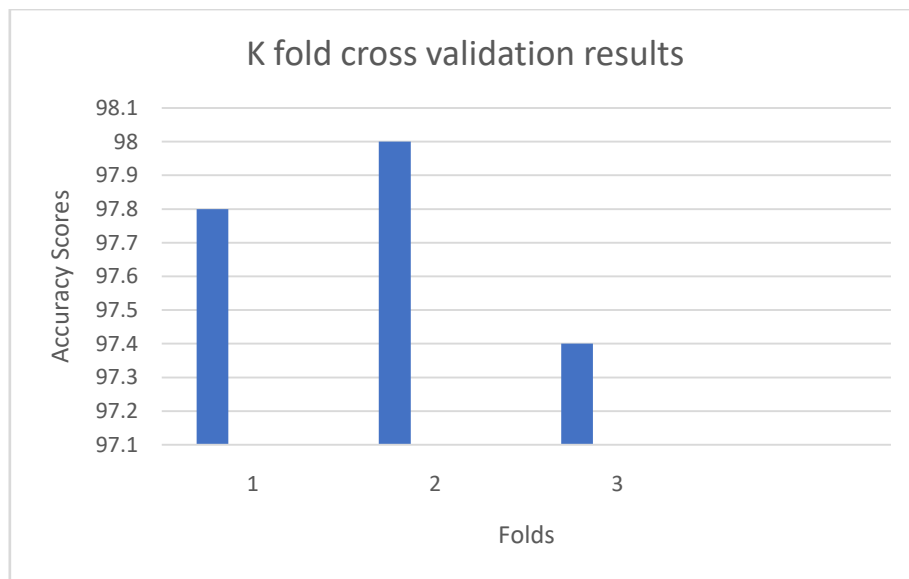


Figure 7. (a) Curve of Recall for Naive Bayes, (b) LSTM ROC Curve, (c) KNN's ROC Curve

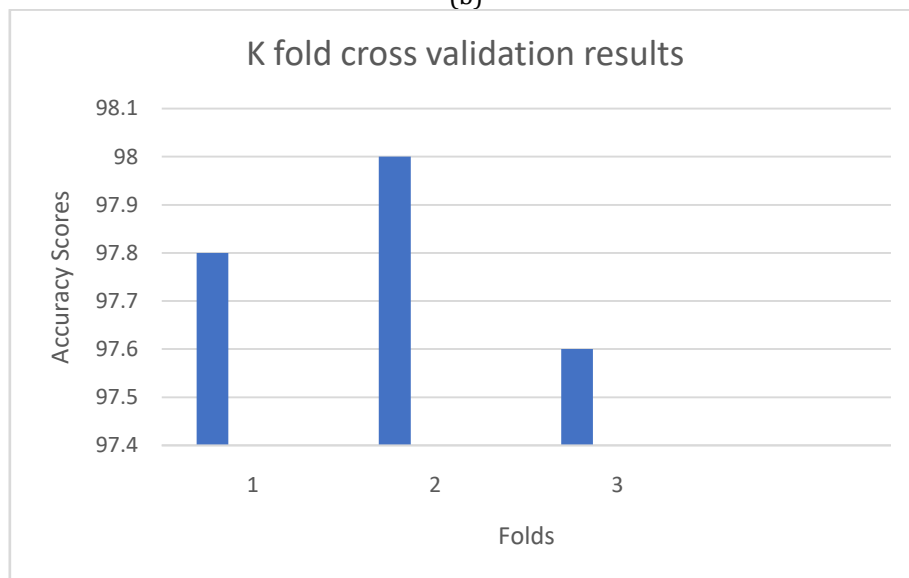


(a)





(b)



(c)

**Figure 8.** A three-fold cross-validation in support vector machines (SVMs), a similar technique in naive Bayes, and a similar technique in kernel neural networks (KNNs).

## 5. DISCUSSION

The research results indicate that the RVM procedure is a viable method for SMS junk identification. The RVM method surpassed the Naive Bayes, SVM, and LSTM algorithms for precision, recall, and F-score. It is noteworthy that the RVM approach needs a longer training duration compared to the Naive Bayes, SVM, and LSTM procedures. This is a possible constraint of the RVM method, particularly in the context of real-time SMS spam detection applications. A disadvantage of the research is that it assessed the presentation of the RVM procedure just on a single data of SMS. Evaluating the RVM algorithm's effectiveness across diverse datasets is crucial to ascertain its generalisability to various SMS message formats.

## 6. CONCLUSIONS

This article presents the findings and discusses the result, which comprised assessing the data and evaluating the presentation of every method. The categorisation method for RVMs has the highest correctness, making it the superior option. This research discusses the conclusions of the comparative assessment of SVM, NB, KNN, LST and RVM.

Following are some things that can be done in the days to come.

- To enhance precision, more SMS datasets will be added.

- Examine the experimental outcomes using the collective methodology on RVM, SVM, NB,LSTM, and K-NN, and conduct a comparative analysis among them.
- Putting validation criteria into action and assessing the outcomes.

## REFERENCES

- [1] Aji, Guna Suryo, et al. "Machine learning based spam message classification system using blockchain technology." 2021 17th International Conference on Quality in Research (QIR): International Symposium on Electrical and Computer Engineering. IEEE, 2021.
- [2] Yi, Haibo. "Securing instant messaging based on blockchain with machine learning." *Safety Science* 120 (2019): 6-13.
- [3] Teja Nallamothu, Phani, and Mohd Shais Khan. "Machine learning for SPAM detection." *Asian Journal of Advances in Research* 6.1 (2023): 167-179.
- [4] Sethi, Paras, Vaibhav Bhandari, and Bhavna Kohli. "SMS spam detection and comparison of various machine learning algorithms." 2017 international conference on computing and communication technologies for the smart nation (IC3TSN). IEEE, 2017.
- [5] Lakhdar, Hatim, Fatna El Mendili, and Younes El Bouzekri El Idrissi. "Blockchain-based spam detection approach." 2023 10th International Conference on Wireless Networks and Mobile Communications (WINCOM). IEEE, 2023.
- [6] Ahmed, Naeem, et al. "Machine learning techniques for spam detection in email and IoT platforms: analysis and research challenges." *Security and Communication Networks* 2022.1 (2022): 1862888.
- [7] Bhandari, Aradhita, Aswani Kumar Cherukuri, and Firuz Kamalov. "Machine learning and blockchain integration for security applications." *Big Data Analytics and Intelligent Systems for Cyber Threat Intelligence*. River Publishers, 2023. 129-173.
- [8] Srinivasa Rao, D., and E. Ajith Jubilson. "SMS Spam Detection Using Federated Learning." *International Conference on Computational Intelligence and Data Engineering*. Singapore: Springer Nature Singapore, 2022.
- [9] Srivastava, Aditya, and Pawan Singh. "Spam Detection Using Natural Language Processing." *Journal of Applied Science and Education (JASE)* (2024): 1-7.
- [10] Ogundokun, Roseline Oluwaseun, et al. "Phishing detection in blockchain transaction networks using ensemble learning." *Telecom*. Vol. 4. No. 2. MDPI, 2023.
- [11] Joshi, Kunj, et al. "Machine-learning techniques for predicting phishing attacks in blockchain networks: A comparative study." *Algorithms* 16.8 (2023): 366.
- [12] Pitre, Vishwas, Ashish Joshi, and Suman Das. "Blockchain and Machine Learning Based Approach to Prevent Phishing Attacks." 2023 3rd Asian Conference on Innovation in Technology (ASIANCON). IEEE, 2023.
- [13] Sahmoud, Thaer, and Dr Mohammad Mikki. "Spam detection using BERT." *arXiv preprint arXiv:2206.02443* (2022).
- [14] Kim, Taehyun, et al. "Posting bot detection on blockchain-based social media platform using machine learning techniques." *Proceedings of the International AAAI Conference on Web and Social Media*. Vol. 15. 2021.
- [15] Agarwal, R., et al. "A novel approach for spam detection using natural language processing with AMALS models." *IEEE Access* (2024).
- [16] Ismail, Shereen, Diana W. Dawoud, and Hassan Reza. "Securing wireless sensor networks using machine learning and blockchain: A review." *Future Internet* 15.6 (2023): 200.
- [17] Sun, Nan, et al. "Near real-time twitter spam detection with machine learning techniques." *International Journal of Computers and Applications* 44.4 (2022): 338-348.
- [18] Waja, Gopalkrishna, et al. "How AI can be used for governance of messaging services: A study on spam classification leveraging multi-channel convolutional neural network." *International Journal of Information Management Data Insights* 3.1 (2023): 100147.
- [19] Kabla, Arkan Hammoodi Hasan, et al. "Eth-PSD: A machine learning-based phishing scam detection approach in Ethereum." *IEEE Access* 10 (2022): 118043-118057.
- [20] Arza, Mahita Sri, and Sandeep Kumar Panda. "An integration of blockchain and machine learning into the health care system." *Machine Learning Adoption in Blockchain-Based Intelligent Manufacturing*. CRC Press, 2022. 33-58.
- [21] De Goma, Joel, et al. "Detection of SMS Spam Messages Using TF-IDF Vectorizer and Deep Learning Models." *Proceedings of the 2024 9th International Conference on Intelligent Information Technology*. 2024.

- [22] Kumar, Yogesh, and Surbhi Gupta. "Effectiveness of Machine and Deep Learning for Blockchain Technology in Fraud Detection and Prevention." *Applications of Artificial Intelligence, Big Data and Internet of Things in Sustainable Development*. CRC Press, 2022. 287-307.
- [23] Nasir, Muhammad Umar, et al. "Network meddling detection using machine learning empowered with blockchain technology." *Sensors* 22.18 (2022): 6755.
- [24] Rao, Sanjeev, Anil Kumar Verma, and Tarunpreet Bhatia. "A review on social spam detection: Challenges, open issues, and future directions." *Expert Systems with Applications* 186 (2021): 115742.
- [25] Baby, V., et al. "Developing a Credible and Trustworthy E-Commerce Application using Blockchain and Machine Learning." *International e-Conference on Advances in Computer Engineering and Communication Systems (ICACECS 2023)*. Atlantis Press, 2023.