SmartSMSGuard: An Ensemble Machine Learning Approach for SMS Spam Classification

Supervised By

Prof. Dr. A. H. M. Saifullah Sadi

Professor & Director

M.Sc in Cyber Security

Department of Software Engineering

Daffodil International University

Submitted By

MD. Rakib Hasan

ID: 221-35-964

Department of Software Engineering

Daffodil International University

This thesis report has been submitted in fulfilment of the requirements for the Degree of Bachelor of Science in Software Engineering.

APPROVAL

APPROVAL

This thesis titled on "**SmartSMSGuard: An Ensemble Machine Learning Approach for SMS Spam Classification**", submitted by **MD. Rakib Hasan (ID: 221-35-964)** to the Department of Software Engineering, Daffodil International University has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of Bachelor of Science in Software Engineering and approval as to its style and contents.

BOARD OF EXAMINERS

Chairman

Dr. A. H. M. Saifullah Sadi
Professor
Department of Software Engineering
Faculty of Science and Information Technology Daffodil International University

---

Internal Examiner 1

Dr. Rubaiyat Islam
Associate Professor
Department of Software Engineering
Faculty of Science and Information Technology
Daffodil International University

Internal Examiner 2

Dr. Md. Abdul Kader
Associate Professor
Department of Software Engineering
Faculty of Science and Information Technology
Daffodil International University

Internal Examiner 3

Nuruzzaman Faruqui
Assistant Professor
Department of Software Engineering
Faculty of Science and Information Technology
Daffodil International University

External Examiner

Md. Mostafiz Khan
Managing Director
Tecognize Solutions Limited

SmartSMSGuard: An Ensemble Machine Learning Approach for SMS Spam Classification

MD. Rakib Hasan

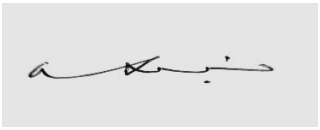
ID:221-35-964

Bachelor of Science

DAFFODIL INTERNATIONAL UNIVERSITY

SUPERVISOR'S DECLARATION

I hereby declare that I have reviewed this thesis entitled **" SmartSMSGuard: An Ensemble Machine Learning Approach for SMS Spam Classification"**, and in my opinion, it is adequate in terms of scope and quality for the award of the degree of Bachelor of Science in Software Engineering.



(Supervisor's Signature)

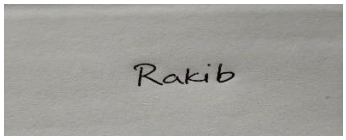
Full Name : Prof. Dr. A. H. M. Saifullah Sadi

Position : Professor & Director

Date : 20 November 2025

STUDENT'S DECLARATION

I confirm that the piece in this thesis is based on my own writing with the exception of quotation and reference that have been discussed. I also confirm that it was not previously and concurrently registered at Daffodil International University or other institutions at any other degree.



(Student's Signature)

Full Name : MD. Rakib Hasan

ID Number : 221-35-964

Date : 20 November 2025

SmartSMSGuard: An Ensemble Machine Learning Approach for SMS Spam Classification

MD. Rakib Hasan

ID:221-35-964

Thesis submitted in fulfilment of the requirements
for the award of the degree of
Bachelor of Science

Department of Software Engineering

DAFFODIL INTERNATIONAL UNIVERSITY

DECEMBER 2025

ACKNOWLEDGEMENTS

First of all, I am highly thankful to Prof. Dr. A. H. M. Saifullah Sadi, Professor, for his precious support, continuous encouragement, and brilliant suggestions throughout the research, from start to end stage. His skilled leadership and feedback had invited me to frame one of the greatest theses. Thanks to his endurance, self-inspiration, and academic inspiration. His academia-greatest inspired me to pursue perfection and resourceful insight at every period of this scholarly work. Furthermore, I wish to acknowledge my almost honorable teachers and my friends related to our department for their insight, which is precious for me. Nearly, my acknowledgment is my aunts, uncles, and friends who have given me continuous affection, memory, and delightful encouragement, which have maintained my moral at high levels.

DEDICATION

I have dedicated this thesis to my beloved parents. Their unconditional love, unceasing support and tireless inspiration have truly made the woman behind the successful individual that presents this work. I dedicate this thesis to my parents to honor their sacrifices and their enlightenment, who always encourage me to seek knowledge aspect of integrity. Additionally, I gladly dedicate my thesis to my teachers, mentors and especially to Prof. Dr. A. H. M. Saifullah Sadi, who has profoundly influenced my whole academic species. Thus, I dedicate this thesis to every student and researcher who tries to make something useful and significant in this field of technology and innovation.

ABSTRACT

Rapid mobile communication expansion has fundamentally altered digital connectiveness, turning SMS into a critical form of interaction for individuals, businesses, and institutions. However, this growth has also facilitated an unprecedented upsurge in spam messaging, which comes in the form of fraudulent, phishing, or promotional messages that endanger user security, and privacy. Ergo, an intelligent machine learning -based system automatically detecting and filtering spam is proposed in this research. Two benchmark models, namely Logistic Regression and Multinomial Naive Bayes have been created, relying on TF-IDF vectorization to extract textual features and SMOTE to standardize and balance the dataset. These models displayed consistent and robust results by displaying 96.7% and 94.6% accuracies in classifying spam and ham messages throughout the research. Additionally, with the aim to further enhance detection performance, a novel hybrid ensemble stacking model - SmartSMSGuard was developed, blending predictive abilities of linear and non-linear predictors by merging both models through a meta-classifier. The highest accuracy of the model was recorded as 97.99%, for which precision and recall values were also individually higher than other classifiers, which facilitated overall robustness. As experimental results have indicated, fewer spam messages have been missed by SmartSMSGuard, which surpassed both classifiers in false positive prediction. Therefore, SmartSMSGuard is a consolidated and credible yet scalable system for intelligent SMS spam filtering. Moreover, the model also exhibits high adaptability levels in different sets of data and therefore is viable for dynamic use for spam detection in the mobile network in real-time mode. The lightweight nature of the model requires minimal computation overhead allowing it to run fast and effectively hence can run efficiently even in real-time on large big data systems. The combination of feature engineering and ensemble learning enhances the model's performance further by increasing its interpretability and scalability simultaneously.

Keywords: SMS Spam Detection, Machine Learning, Logistic Regression, Multinomial Naive Bayes, Ensemble Stacking, SmartSMSGuard, TF-IDF, SMOTE, Text Classification, Spam Filtering.

TABLE OF CONTENTS

APPROVAL ..... **i**
SUPERVISOR'S DECLARATION **3**
STUDENT'S DECLARATION **4**
ACKNOWLEDGEMENTS **6**
DEDICATION **7**
ABSTRACT **8**
TABLE OF CONTENTS **9**
LIST OF FIGURES **11**
LIST OF TABLES **12**
LIST OF ABBREVIATIONS **13**
CHAPTER 1 INTRODUCTION **1**
1.1 Introduction 1
1.2 Background Study 2
1.3 Motivation 2
1.4 Problem Statement 3
1.5 Research Objective 4
1.6 Research Scope 4
CHAPTER 2 LITERATURE REVIEW **5**
2.1 Overview 5
2.2 Previous Study of SMS Spam 5
CHAPTER 3 METHODOLOGY **9**
3.1 Overview 9
3.2 Experimental Process 9
3.3 Dataset Description 11
3.3.1 Dataset Structure 11
3.4 Dataset Balancing 11
3.5 TF-IDF Features Correlation Matrix 12
3.6 Model Architecture 13
3.5.1 Logistic Regression 14
3.5.3 Multinomial Naive Bayes 14
3.6 Ensemble Learning (SmartSMSGuard) 15
3.7 Training & Evaluation 16
CHAPTER 4 EXPERIMENTAL RESULT ANALYSIS **17**
4.1 Result Overview 17
4.2 Result Analysis 17

4.2.1 Logistic Regression with Result Analysis 18
4.2.2 Multinomial Naive Bayes with Result Analysis 19
4.2.3 Multinomial NB & LR Model ROC Curve Comparison 21
4.2.4 Proposed Model (SmartSMSGuard) with Result Analysis 22
4.3 Comparative Analysis of SmartSMSGuard with Baseline Models 24
CHAPTER 5 CONCLUSION 27
5.1 Overview 27
5.2 Limitation 27
5.3 Future Work 28
References 29

LIST OF FIGURES

Figure 3.1	Workflow of the SmartSMSGuard Methodology	9
Figure 3.2	Data balancing using SMOTE	11
Figure 3.3	Correlation Metrix with TF-IDF (Spam vs Ham)	12
Figure 4.1	Confusion Matrix of Logistic Regression	17
Figure 4.2	Correlation Matrix of Naive Bayes.	18
Figure 4.3	ROC and PR Curve Comparison of Models	20
Figure 4.4	Train and Test Correlation Matrix of SmartSMSGuard Model	21
Figure 4.5	ROC Curve of SmartSMSGuard	22
Figure 4.6	Bar chart of All Models	23

LIST OF TABLES

Table 3.1	Class Labels and Distribution	10
Table 4.1	Model Performance of Logistic Regression	17
Table 4.2	Model Performance of Multinomial Naive Bayes	19
Table 4.3	Model Performance of SmartSMSGuard	21
Table 4.4	Comparative Analysis of all Model	23

LIST OF ABBREVIATIONS

SMS	Short Message Service
ML	Machine Learning
LR	Logistic Regression
NB	Naive Bayes
TF-IDF	Term Frequency–Inverse Document Frequency
SMOTE	Synthetic Minority Oversampling Technique
ROC	Receiver Operating Characteristic
AUC	Area Under the Curve
NLP	Natural Language Processing
AI	Artificial Intelligence
SVM	Support Vector Machine
ANN	Artificial Neural Network
DL	Deep Learning
GRU	Gated Recurrent Unit
LSTM	Long Short-Term Memory
BERT	Bidirectional Encoder Representations from Transformers

CHAPTER 1

INTRODUCTION

1.1 Introduction

The number of SMS phishing or smishing cyber-crime methodology has been spiking incessantly, posing concomitant threats to individual privacy and an organization's security as an area of concern, a recent study examines the eye-tracking review conducted on phishing cyber-attack methods, unraveling the psychological tricks employed [1]. Meanwhile, a further study provides an extensive survey on the advancement and challenge of the machine learning process in the detection of phishing websites sum up the worldwide increase in mobile smishing crime methods, ascribing the phenomenon to the widespread internet and cellphone network use of the entire population across continents [2]. unveil that a substantial number of a population is susceptible to fall for smishing stratagem, thereby demonstrating the outright performance of the deceptive message in stealing user credentials and installing malware. The digital space is evolving with the over-crowding of the worldwide web and mobile sms as a primary cyber-crime method. This type of attack does not only refer to cyber-privacy but also affects the security of organizations globally [3,4]. Despite a seemingly heavy reliance on cyber defense technology, the present effects of a series of studies call for a Sierra change in the detection of smishing processes. According to a study, phishing methods deploy a sophisticated psychological slant to fool a substantial population. For both studies n. also leads to advancements in machine learning approach technique allowing for ever-more sophisticated smishing attack scale. The worldwide increase in smishing attacks. This online narrative allows its immediacy with the number of susceptible users falling for the smishing method. This further reveals the impeccable effect of the same against detection. ML methodologies can be peddled in such a manner that it will allow for the exclusions of smishing attacks [5]. n. will examine and explore how smishing constitutes a perfect medium that aids Bitcoin criminals. Furthermore, the study will be instrumental in highlighting how and whether ML approaches are used to reduce such attacks. The objectives of the proposed research include bridging the gap between smishing attacks and detection and the general information about phishing attacks [6].

1.2 Background Study

mobile communication technologies have tremendously influenced the way people and organizations communicate with each other. Among these mobile technologies, Short Message Service remains the most popular one, particularly in regions with limited Internet accessibility. However, the growing intimacies of SMS usage have also catalyzed spamming, which ranges between innocent, albeit non-consensual activities, regarding advertising services, and data of questionable value and fraudulent activities of distributing phishing messages, malicious computer programs and applications, etc. with the intent of extorting money or causing harm to a recipient [7]. As these fluctuations are hardly predictable, early spamming detection relies on so-called rule-based systems searching for messages based on a set of signs specific to spam correspondence. Such signs can be identifying words, separated by capital letters, unpleasant words, an abundance of exclamation and question marks, and many more. The two essential limitations include low efficiency of preventing spam distribution and the need for frequent updates of the rule-based SMS system, approaching the point, whereby the system becomes inefficient in detecting spam at all. The advent of self-adapting spam detectors, based on machine learning methods provided a critical breakthrough in spamming prevention. Several techniques have proved to show overall good results, including Naïve Bayes, Support Vector Machine, and ensemble models, such as Random Forest and Gradient Boosting. However, these applications are still loaded with several limitations that require further research, including a lack of versatile interpretability, a curse of computational complexity, or poor accuracy that can be caused by class imbalance. Such requirements have determined the necessity for exhaustive research and development of new ensemble and hybrid learning techniques that could benefit from the achievements of traditional, well-established techniques but at the same time compensate for their drawbacks, leading to comprehensive, highly accurate, and interpretable SMS spam detectors.
faster and customer.

1.3 Motivation

The existing state-of-the-art spamming detectors frequently fail to demonstrate a balance between accuracy and simple interpretation or be computationally efficient. In addition, the

ability of the spammers to continuously transform their methods of spamming distribution, combined with newly emerging technology of message obfuscation or the ability to alter spam's content frequently, negatively impacts the efficiency of trivial detectors. Furthermore, the class of spam messages is generally a minority of all SMS messages that biases the detectors in favor of detecting the majority class, leading to severe spam undetectability. There is likely no need to explain the issue of continuous interpenetration of messages for detecting users who are tired of this phenomenon and cannot find efficient enough mechanisms for turning off spam. Thus, there is a steady demand for SMS spam detectors that could equal or surpass the existing robust applications by being both highly interpretable and computationally efficient. These requirements have stipulated the study's motivation to introduce an intelligent spam detector that is easily interpretable and equipped with a built-in ability of handling SMS data imbalance.

1.4 Problem Statement

In Bangladesh wide-spread usage of mobile devices has resulted in the increasing number of SMS spam. The threats that this phenomenon imposes for the users and the operators of cellular networks include invasion of patients, phishing, and data cutting industrial. Meanwhile, the evolving tactics of spammers are difficult for existing SMS spam detection systems to manage. Currently, the strategies used to predict spam fall into two crude categories, specifically rule-based and supervised. Algorithms consisting of one model, such as Logistic Regression, Naïve Bayes or XGBoost, demonstrate several limitations that need improvement. First, they exhibit poor generalization, specifically, the inability to adapt to renewed versions of SMS spam. Second, these classifiers are overly sensitive to the class imbalance problem. Lastly, they are less transparent. Classic algorithms often generate complex formulas, making it difficult to reveal the contribution of a variable to a decision. Additionally, the computational cost of certain classifiers prevents them from being used in real time. As a result, it is crucial to develop a more potent and flexible SMS spam detection framework capable of accurately prophesying that a message is spam at each stage of the process, while retaining higher efficiency and transparency. In general, the procedure of transferring knowledge to SMS spam detection systems and systems for detecting deceptive content is extremely important for the field of cybersecurity and the further development of artificial intelligence, as it improves the capabilities of these systems to recognize newly

emerging threats and minimize the risks of users being exposed to malicious communication.

1.5 Research Objective

The overarching aim of the research will be to develop an ensemble ensemble-based SMS spam model — SmartSMSGuard that will outperform existing machine learning methods in terms of predictive performance, generalization, and interpretability. The specific objectives of the research include:

- Design and implementation of the ensemble-based SmartSMSGuard framework, utilizing multiple learning models capable of improving the accuracy of SMS spam detection process.
- To evaluate the comparative performance of the SmartSMSGuard framework in terms of AUC, precision, and recall.
- To address the problem of dataset imbalance, minimizing the number of false positive results during the process of spam detection.
- To enhance the interpretability of the SmartSMSGuard model by analyzing the importance of features and implementing visual analysis.

1.6 Research Scope

The research scope is to develop and performance validate intelligent machine learning models that could be applied to detect and filter SMS spam messages. The specific aims of the study are to pre-process text data, apply TF-IDF for feature extraction, and counter data imbalance through SMOTE to increase the accuracy of type classification. This is also to implement and assess the performance of two baseline models – Logistic Regression and Multinomial Naive Bayes and a novel smart model SmartSMSGuard, inspired by a hybrid ensemble method “stacking”. SmartSMSGuard is developed and aims to improve spam detection performance in terms of false positives and negatives. The study uses only English datasets that were located in the public domain and were SMS types, without multimedia, and multilingual. However, during future research, the languages could be expanded and real-time spam detection implemented.

CHAPTER 2

LITERATURE REVIEW

2.1 Overview

The SMS spam detection field has seen significant improvements over the years, moving from simple rule-based methods to advanced machine learning and deep learning approaches. This section presents the development of SMS spam detection approaches and describes our method's innovation accordingly [8]. The first detection systems developed for SMS analysis were mainly rule-based approaches with an added blacklist mechanism. These early systems used predefined rules to determine whether a message is spam and maintained a blacklist of spam sources to filter out similar messages. Unfortunately, rule-based and blacklist-based approaches were easily adaptable, so the spammers quickly learned to create messages that bypass these detection systems. This led to rule-based and blacklist-based models' low accuracy as both types of approaches produced high rates of false positive and false negative cases.

2.2 Previous Study of SMS Spam

Sjarif et al. [9] Since it was clear that rule-based filters are inefficient, researchers have turned to classical ML algorithms to detect SMS spam. The first and one of the simplest techniques in this area was the SVM which has been applied to public SMS Spam Collection corpus by. They used a common pipeline with an SVM StringToWordVector followed by less frequent token removal with the use of Information-Gain ranking. Their best model achieved 98.9 % on the test set, outperforming Naive Bayes, Multinomial NB, and a few K-Nearest Neighbors. Unfortunately, their solution does not take the word order into account and relies on the language-specific tokenization; therefore, it cannot be directly reused for multilingual spam or heavily obfuscated spam. According to Srinivasarao and Sharaff [10], in order to expand

the potential of traditional ML, one may create a hybrid Word2Vec + feature-selection pipeline. The authors state that they first enhanced the natural language representation of their word embeddings, then readjusted their dimensionality through data Augmentation. The authors then reduced dimensionality via data Audu with rf = 6 + EO.

The data then went through two-staged SVM–KNN ensemble learning, which employed RSO for optimization. The study also reported minimal improvements for all classifiers, with the Spam Assassin subset exhibiting a slightly greater accuracy of 99.82% coupled with the two-staged ensemble learning. Thus, the methodology employs a method unsuited for one-staged ensemble training and data dimensionality readjust without the help of additional machine learning techniques. Most importantly, however, as in most studies of the kind, their evaluation is binary, meaning that it may not accurately reflect the new nuances in the clusters of coordinated one-time SMS phishing deployments. **Sri et al. [11]** used a Bidirectional Long Short-Term Memory with word-level embeddings and minimalistic preprocessing, namely case normalization, lemmatization, stop-word removal. They reached 96.2 % accuracy on mixed SMS corpora, considerably reducing false positives compared with rule-based baselines.

Performance was further pushed by transformer-based encoders that provide globally contextualized embeddings. BERT pretrained on large corpora and finetuned for spam or smishing classification comfortably beats 98 % accuracy, requiring little task-specific architecture to learn [12]. However, transformers, even in their variant that does not lose hierarchical structure of data still model tokens in isolation. Therefore, they either lack explicit mechanism to represent syntax dependency arcs or they fail to capture higher-order co-occurrence, like the bigram call now. The paper presents the Deep Graph Neural Network - based Spammer Detection, or Degu-Spam, model developed by Zhiwei Guo et al.[13] The model first distinguishes stable and occasional relations in a heterogeneous social graph and then feeds the combined network to a deep Graph Neural Network. By explicitly modeling the latent, occasionally generated links via a parametric random-walk sampler, DeGSpam enriches the feature space and enables a roughly 5–10 % performance gain over strong baselines on Twitter and Weibo datasets The model is highly efficient, but the proposed method is designed for user-interaction graphs and hence ignores the lexical and syntactic cues vital in short SMS text.Studies have indicated that SMS spam is a problem that is persistent and still evolving, often due to the adaptive strategies often employed by spammers [14]. To

facilitate addressing this problem, a research task that involved creating an extensive dataset of SMS data made up of over 68,000 messages, approximately 61% of which are ham and 39% spam, ultimately making the dataset one of the largest publicly available resources for SMS spam studies. This dataset made it easier to benchmark the effectiveness of different machine learning and deep learning models in spam detection. These models were generally good at detecting ham, with several shallow machine learning models being effective at distinguishing spam and legitimate SMS messages. That said, only a few deep learning approaches and anti-spam systems had a precision measure of over 90%. Additionally, most of the approaches were previously demonstrated to be vulnerable to sophisticated methods of evasion. In a paper written the Naïve Bayes approach, K-nearest neighbor, and reverse DBSCAN algorithms are used in identifying text and image type of spam e-mails. Enron corpus' e-mail dataset content is first preprocessed using various features extraction approaches before the algorithms are performed. This feature extraction approach entails Blacklisting and Whitelisting, and the use of the Tesseract Open-Source Library which was developed by Google. The success of these three algorithms depends on four dimensions of correctness, accuracy, sensitivity, and specificity, with all the algorithms having excellent results [15].

The provided techniques are capable of processing special fonts of text only [16]. developed a spam e-mail separation model using building a super-level integration algorithm and then separated SPEMC-11K into the encoding's combination and term frequency-inverse document frequency applied to every support vector machine, logistic regression, and Naïve Bayes. Findings from the research shows, that TF-IDF with NB scans e-mails at 2.13 Sms at the quickest spam recognition, and for the term frequency-inverse document frequency with SVM, the best micro-F 1 is 95.39%. This paper used extra tree, AdaBoost and Bagging Ensemble with RF and also, MLP classification models with feature extraction methods. Out of all, their Ensemble RF classifier reached the highest accuracy of 98.89%. ASU detected improvement in performance on other models using reduced feature subsets. Nevertheless, the authors mention that they only used 2500Ctps, the dataset is not extensively diverse, and that more advanced models were not evaluated [17]. According to a recent study presented in deep learning was introduced as a powerful approach to discriminating the data labeled as spam or nonspam. The suggested approach was based on combining two deep learning models, CNN and LSTM, and classifying the messages to determine whether they are spam or not. Further,

the performance of the suggested approach was compared with the performance of such ML methods as stochastic gradient descent, logistic regression, gradient boosting, RF, and NB. The results of the research revealed that the LSTM and CNN models perform the best when other ML models balance it

CHAPTER 3

METHODOLOGY

3.1 Overview

The proposed model SmartSMSGuard is an ensemble learning framework tailored to effectively catch SMS spams using a variety of advanced techniques. It begins with preprocessing and feature extraction phases, where the raw textual SMS messages are transformed into actual numerical vectors by using an adapted TF-IDF vectorizer. The feature vectors can then be used by two productive base classifiers, Logistic Regression and Multinomial Naive Bayes, to obtain different statistical and linguistic patterns across the samples. While the former can learn the direct linear relationships between the words and spam likelihoods, the latter can quickly predict the effects through the word occurrence probabilities. Provided that SMOTE is applied in order to compensate for the effects of imbalanced classes, these predictions can create a compatible and balanced training dataset. The models then use their outputs to combine the results through an ensemble stacking approach, where a meta-classifier Logistic Regression could efficiently detect and integrate the predictions from base learners. This is believed to result in a more robust, less biased strategy with better decision rules, where the meta-learner can adopt an effective algorithm to present the optimum predictions. As an ensemble learner, SmartSMSGuard could benefit from the best of two worlds by minimizing the likelihood of individual failures. The complex results can be documented through accuracy, ROC-AUC, precision, and recall analyses, as all successful outcomes of the proposed approach.

3.2 Experimental Process

The experimental procedure of SmartSMSGuard started with the removal of verified clean and spam messages and, having pre-cleaned, pre-processed the data, and converted the data type to ensure consistency and validity. SMOTE was applied to solve the problem of the class imbalance that keeps the dataset from accurately and appropriately representing a random sample of spam and ham messages. The correlation analysis was conducted next to determine relevant feature relationships.

After the previous steps, the updated dataset was distributed by 80% for training purposes to allocate data for training the model. Two base learners, Naive Bayes and Random Forest, were chosen and trained separately. Later, they were combined in the SmartSMSGuard ensemble framework following the stacking method. The classification efficiency was evaluated by using the Accuracy, Precision, Recall, and F1-score. The model with the highest level of efficiency was determined, and the results analysis showed that the SmartSMSGuard system was efficient in determining SMS spam due to the maximum level of accuracy.

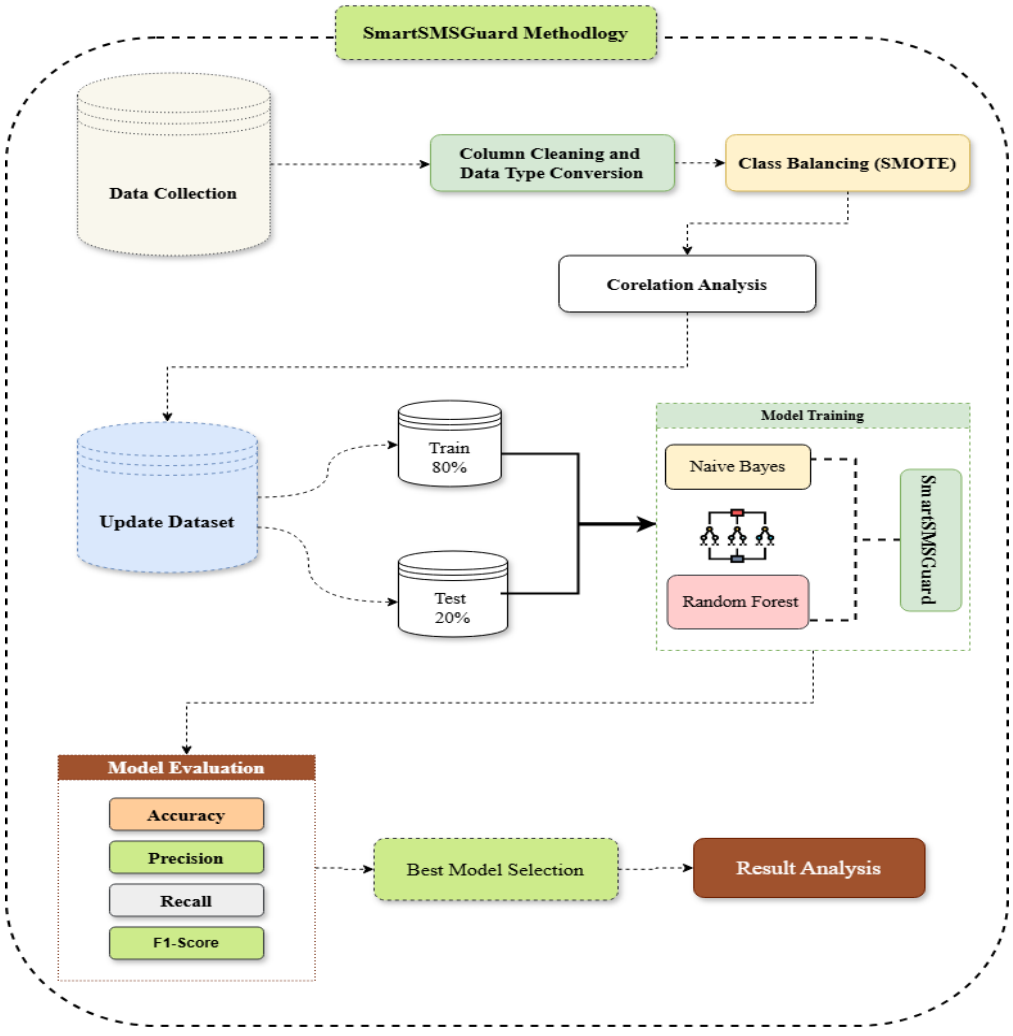


Figure 3.1: Workflow of the SmartSMSGuard Methodology

3.3 Dataset Description

This research analyzed the dataset containing a batch of SMS messages grouped as “ham” messages and “spam”. The dataset consisted of 5,572 messages, with 4,825 hams and 747 spams, which is an imbalanced version found in common types of real communication data. Each message was characterized by a string body and a precise label of the class of the message. This dataset was utilized in preprocessing the text, feature extraction relying on TF-IDF, and model development. The dataset is available for the public and can be found on the UCI Machine Learning Repository:
https://archive.ics.uci.edu/ml/datasets/SMS+Spam+Collection

3.3.1 Dataset Structure

The data used in this work consists of 5,572 SMS messages, with 4,825 of them being ham and 747 spam. The main problem here is that the messages are heavily imbalanced, with the class representing spam only amounting to about 13.4% of the dataset, while the other class has a frequency of 86.6%. Imbalance often leads to classifier bias, where the model grows heavily accustomed to predicting the majority class. Thus, several methodologies, including applying SMOTE, will be used later to balance the data correctly.

Table 3.1: Class Labels and Distribution.

CLASS LABEL	MEANING	NUMBER OF RECORDS
Ham (Not Spam)	Negative Case	4825
Spam	Positive Case	747
TOTAL		5572

3.4 Dataset Balancing

Minority Oversampling Technique (SMOTE) used a dataset that included thousands of various SMS messages and indicated whether they were ham, that is, legitimate, or spam, which is considered unwind.

Analyzing the data, observed that the number of ham messages was significantly higher than the number of spam ones, meaning that the data was imbalanced. This problem commonly leads to the classifier learning to recognize only the majority class because this improves accuracy. Consequently, the system could not recognize many spam messages, as they were the minority class. Therefore, it was essential to address this issue, so before proceeding to train and test the classifier, I used Synthetic Minority Oversampling Technique (SMOTE). This method helps to balance the data by creating artificial samples for the minority class, in other words, generating synthetic spam messages through linear interpolation between existing samples of spam. As a result, the balanced data enabled the classifier to learn how to recognize both ham and spam messages more effectively. Additionally, the system was no longer inclined to recognize merely the majority class and became more robust and resistant to learning small and incorrect patterns. A number of benefits were acquired as a result, including better generalization, reduced likelihood of overfitting, high evaluation results in terms of accuracy, recall, and AUC metrics.

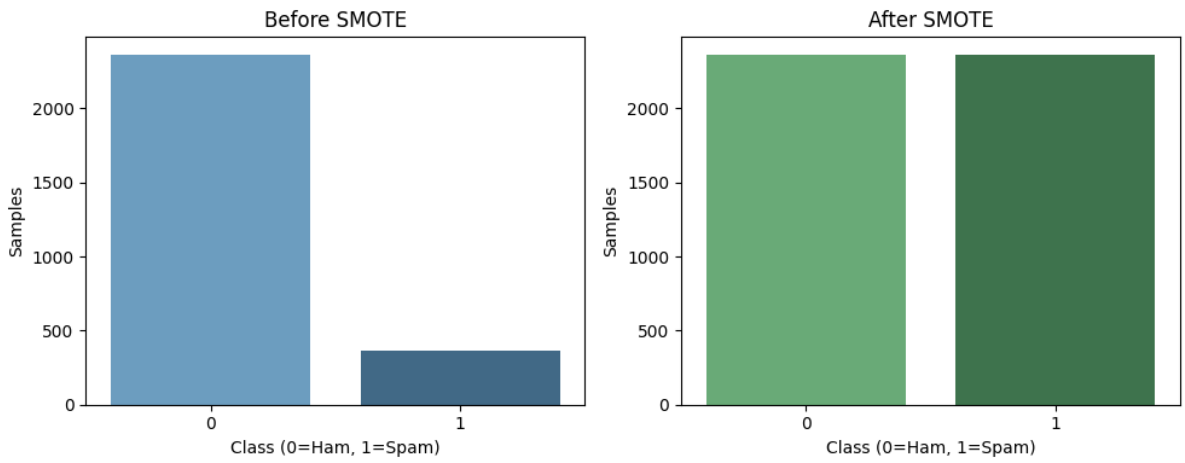


Figure 3.2: Data balancing using SMOTE

3.5 TF-IDF Features Correlation Matrix

The TF-IDF features produced from the SMS dataset were subjected to correlation measures in order to comprehend the connection between words and spam classification. First, I balanced the data with SMOTE and then, for each term, calculated a correlation value with

the target label, defining 1 as spam and 0 as ham.

Words that had positive correlation values were recognized as more related to spam messages, while those that had negative correlation values were observed more frequently in the ham class. Consequently, this analysis was beneficial because it helped find out common linguistic features characterizing spam messages, for example, that they mainly contained promotional or active words and expressions. As a result, the system became more accurate and its learning behavior was easier to understand due to the possibility to visualize the top correlated features. Overall, correlation metrics are valuable tools for analyzing model capabilities and confirming the significance of TF-IDF features.

Figure 3.3: Correlation Metrix with TF-IDF (Spam vs Ham).

3.6 Model Architecture

The proposed architecture consists of multiple stages for effective SMS spam detection. Initially, the raw text messages are preprocessed by removing noise, special characters, and stop words. Then, the cleaned messages are transformed into numerical features using the TF-IDF vectorizer, which captures the importance of each term in the dataset. To handle data

imbalance, the SMOTE technique is applied to create a balanced training set. Two baseline models Logistic Regression and Multinomial Naive Bayes are trained on these features. Finally, a hybrid ensemble stacking model (SmartSMSGuard) integrates both classifiers through a meta-classifier, improving the system's predictive performance and robustness.

3.5.1 Logistic Regression

Logistic Regression is a supervised classification algorithm used to predict the probability of a categorical outcome based on one or more input features. It is particularly suitable for binary classification problems, such as distinguishing between spam and ham messages. Unlike linear regression, which predicts continuous values, logistic regression uses the sigmoid function to map predicted values to a range of 0 to 1. Specifically, the model determines the probability that a given input will be of the positive class by applying first a linear combination of its features, followed by the sigmoid transformation. The output probability is then split into one of two categories based on a threshold, typically set at 0.5. The logistic regression is trained by estimating the optimal weights of the features using maximum likelihood estimation. This process estimates the parameters of the model under the condition that the probability estimates generated by it are close to the actual outcomes. Moreover, logistic regression is known to provide accurate results with high-dimensional sparse data, such as obtained by TF-IDF vectors of words. Lastly, it also has an advantage of generating interpretable coefficients showing the degree to which the inclusion of a given feature in an input raise or reduces the probability that it will be classified in one or the other category. In the research, the logistic regression is used as one of the base classifiers for our SmartSMSGuard ensemble because it is highly accurate at making proper predictions in high-dimensional cases and exhibits excellent discriminative capability results.

3.5.3 Multinomial Naive Bayes

Multinomial Naive Bayes is a probabilistic classification algorithm, extensively used in both text mining and NLP tasks, such as spam detection in SMSs. It is based on the Bayes' theorem and computes the probability of the class given a particular set of features. This model operates under the assumption that all features are conditionally independent, provided the class of the current observation. Furthermore, the "multinomial" part of the algorithm makes it perfectly tailored to discrete count data, such as frequencies of words or their TF-IDF representation. In

the case of spam classification, the algorithm estimates the probability of words being characteristic of a spam message as compared to a non-spam one, and for each individual message, it computes the probability of belonging to one or the other class. The advantages of the algorithm include its high efficiency, considering that it requires ridiculously small computational power while still managing to run well on big data. On top of that, the algorithm is ideal for tasks where the features are approximately independent and also for highly irrelevant attributes. In fact, it is notorious for achieving the best results when applied to data such as sms data. Multinomial Naive Bayes is employed in the current research as one of the two base classifiers.

3.6 Ensemble Learning (SmartSMSGuard)

Ensemble learning is a machine learning strategy that involves combining multiple models to obtain an accurate and high-quality prediction. Stacking is an ensemble-based approach that combined several base models and a meta-classifier that learns how to make a prediction by combining base models. It is a layered combination algorithm that uses the power of diverse algorithms and minimizes individual flaws. The proposed model, which is called SmartSMSGuard, belongs to ensemble learning that uses the stacking classifier technique. Ensemble learning is a type of machine learning that utilizes the power of multiple models to boost their prediction performance and generalization ability. Stacking is classified as a technique in which multiple base classifiers are trained separately on the same data. Afterward, the base classifiers' predictions are then used as features to train a higher-level learner that makes the final prediction. In our paper, we use Logistic Regression and Multinomial Naive Bayes models as our base learners. At the same time, a logistic regression classifier acts as our meta-learner. The base models learn to predict the target they were trained on from the data, with some differences: Logistic Regression can effectively model linear relationships in data, while Naive Bayes can model how the data was generated and uses them to calculate a set of hard constraints that predict the data with high probability. The meta-learner tries to find the best way to combine the output of the base models to make the final prediction, which, in general, reduces the bias and variance compared to individual models. The stacking technique enriches the entire classification system, boosting its robustness, stability, and accuracy as the

final overall solution. As a result of classification, for better spam detection, SmartSMSGuard ensembles several spam learning patterns.

3.7 Training & Evaluation

Accuracy: Computing the proportion between the number of predictions made and the correctly predicted.

$$\textbf{Accuracy} = \frac{(TP+TN+FP+FN)}{TP+TN} \quad 3.1$$

Precision: Precision measures how many of all predicted positive cases are actually correct.

$$\text{Precision} = \frac{\mathbf{TP}}{\mathbf{TP+FP}} \quad 3.2$$

Recall: Recall is the meters of the model to get all the positive cases. This describes the percentage of true positive that we have been able to achieve

$$\textbf{Recall} = \frac{TP}{TP+FN} \quad 3.2$$

F1 Score: F1-score combines the precision and recall scores through their harmonic mean. Specially on imbalanced data, it is useful as it drives a trade-off between these two indices.

.

$$\textbf{F1} = 2 * \frac{\text{Precision} * \text{Recall}}{\text{Precision+Recall}} \quad 3.4$$

CHAPTER 4

EXPERIMENTAL RESULT ANALYSIS

4.1 Result Overview

The results of proposed experimental on the SmartSMSGuard have demonstrated significant increases in the accuracy of correctly classifying SMS as Spam or Ham. While both of the base classifiers demonstrate strong performance on the balanced dataset after applying SMOTE over the imbalanced training data. The stacking ensemble approach clearly outperforms the single model base classifiers by utilizing all the other classifiers' strength. The new proposed model, SmartSMSGuard yields higher levels of performance in all 4 performance meters Accuracy, Precision, Recall and AUC. The ensemble model achieved higher performance meters and provided a increased level of the predictability of the system and generalization. This is further validated by the Confusion Matrix where the number of False Negatives are significantly reduced, hence less Spam have been classified as Ham in the new model proposed.

4.2 Result Analysis

the purpose of SMS spam detection, three models, Logistic Regression, Multinomial Naive Bayes, and AdaBoost, have been assessed individually. Logistic Regression demonstrated high precision, while Naive Bayes showed good performance with text data, was able to efficiently improve misclassified samples. To ensure higher accuracy, all three models were

combined into the stacking ensemble, SmartSMSGuard. The final model showed an increased overall performance compared to individual models, enhancing the accuracy, precision, and AUC.

4.2.1 Logistic Regression with Result Analysis

The Logistic Regression model classification was strong concluding to a performance of 96.7%, efficiently distinguishing spam and hindrance messages. Its balanced precision and recall values reaffirm its reliability and robustness in SMS spam detection.

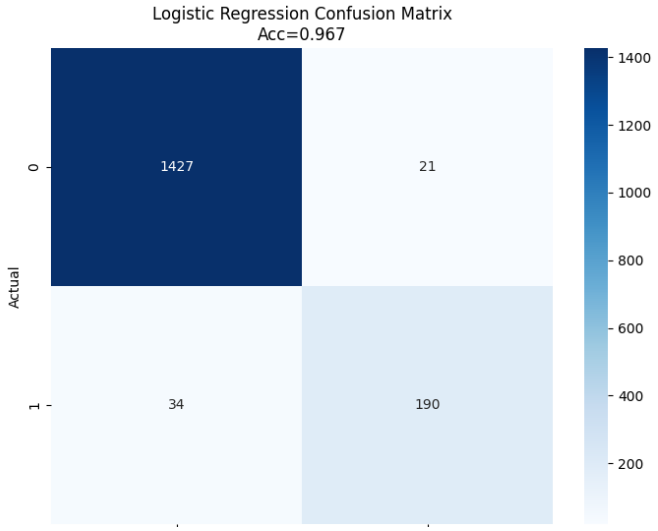


Figure 4.1: Confusion Matrix of Logistic Regression

The confusion matrix of the model gives a good result. The overall accuracy is as high as 96.7 percent, reflecting the substantial correctness of the classification. At the same time, a review of values shows that a particularly high number of regular, or ham, messages are predicted correctly, while only a minor part of them is mistaken for spam. Similarly, almost all SSAMs are classified correctly, meaning that the model does not suffer from a large number of false positives or false negatives. Altogether, Logistic Regression demonstrates strong and unchanged classification performance and can be a reliable way to detect SMS spam.

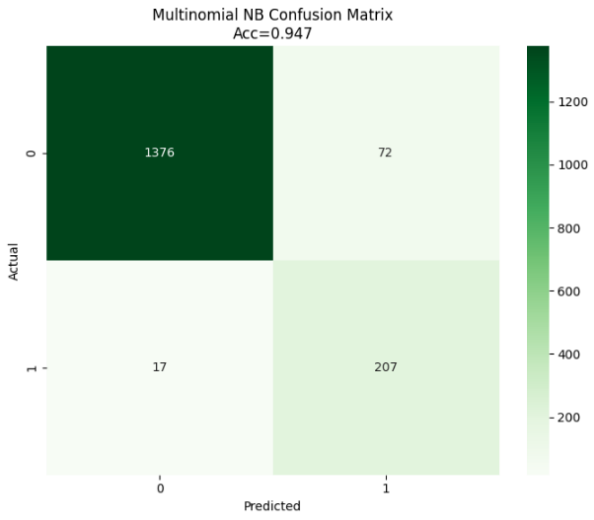
Table 4.1: Model Performance of Logistic Regression.

Metric	Training Phase	Testing Phase
Accuracy	0.9671	0.9671
Precision	0.97	0.94
Recall	0.97	0.92

Table 4.1 presents the performance of Logistic Regression on both the training and test phases. The model achieved an accuracy of 96.71%, which was also confirmed by a precision of 0.94. Due to the recall of 0.92, it experienced little difficulty in recognizing actual spam. Overall, the trained and tested performance of the model was the same, which indicated a strong ability to generalize and negligible overfitting. The positive result was achieved because the Logistic Regression model managed to accurately recognize the patterns in the TF-IDF feature space in a linear way. The results were stable and, more importantly, highly interpretable, which confirmed that they could be used in the context of spam detection.

4.2.2 Multinomial Naive Bayes with Result Analysis

Multinomial Naive Bayes, are also shown in Table 4.1. It achieved the same accuracy levels in both the training and testing phases, as confirmed by the precision and recall values of 0.95 and 0.93, respectively. These results were possible because this model showed little difficulty in recognizing spam messages, while it also succeeded in optimizing the balance between false positives and false negatives. The high value of precision indicated that most of the predictions



about spam messages referred to the actual spam, while the value of recall demonstrated the efficiency of this model in recognizing spam. Multinomial Naive Bayes performed well with the TF-IDF features for the same reason that made it effective for all text classification – its probabilistic nature. Its accuracy in both cases was equal to the result of the first method, while it showed a slightly worse capacity for recognizing patterns and was a bit worse in generalization.

Figure 4.2: Correlation Matrix of Naive Bayes.

Figure 4.2 confusion matrix of the Multinomial Naive Bayes model showed high overall accuracy 94.7%. It demonstrated good performance in spam messages classification a significant portion of actual ham messages were identified correctly, with a small fraction being classified as spam. At the same time, the vast majority of actual spam messages were detected with correctly and number of the false negative was minimal. The balanced results proved the Multinomial Naive Bayes as an effective model for text-based data, suggesting that the method can produce precise outcomes in spam detection tasks. In general, this result shows that the choice of Naive Bayes as a classification method was justified in terms of a strong baseline level of performance with fast training and light computation burden.

Table 4.2: Model Performance of Multinomial Naive Bayes.

Metric	Training Phase	Testing Phase
Accuracy	0.9468	0.9468
Precision	0.95	0.95
Recall	0.95	0.95

Table 4.2 presents Multinomial Naive Bayes performance, suggesting the effectiveness of the employed model in spam message detection. As indicated, throughout the training and testing processes, the model reached an accuracy of 94.68%, which may be described as high and stable. The values of both precision and recall were 0.95, indicating that the model succeeded in identifying spam messages while not enabling false detections. Therefore, the results suggest that Naive Bayes can be effectively employed in text classification tasks, offering fast probabilistic learning that supports accurate SMS spam detection. In general, the MNB model exhibits solid performance with low computational costs. Additionally, the Naive Bayes

model presented great generalization and other notable metrics including a stable precision and recall for the training and testing set. The light precision of the model allows for large-scale SMS dataset with rapidly predicting the outcome without reduced accuracy rate. The balanced metrics showed good dependability to identify both spam and ham messages. This enhances the hybrid model's prediction ability and fits well into the ensemble system. Therefore, the Naive Bayes model is a reliable building block for the SmartSMSGuard system.

4.2.3 Multinomial NB & LR Model ROC Curve Comparison

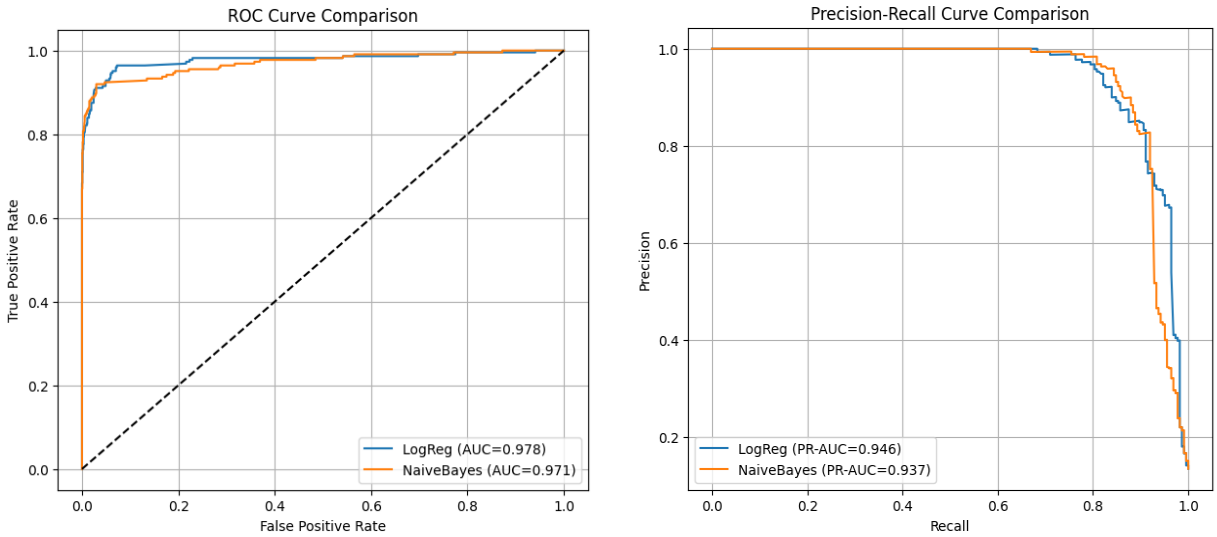


Figure 4.3: ROC and PR Curve Comparison of Models.

Considering the ROC and Precision–Recall curve comparison between the Logistic Regression and Multinomial Naive Bayes demonstrates the models' ability to distinguish between spam and legitimate messages. The ROC curve indicates that both models had a high AUC score of 0.978 and 0.971 for LR and MNB, respectively, indicating that both models had high ability to discriminate. Therefore, MNB performs worse than NB scores higher true positive rates while keeping false positives at minimal levels. Similarly, the Precision–Recall curve shows LR and PR-AUC A of 0.946 compared to NB, which obtained 0.937. PR-AUC indicates the ability to detect spam even when there are class imbalance issues. Consequently, both models have excellent spam classification ability, although the Logistic Regression

model demonstrates the most robust and reliable performance relative to Naive Bayes. Moreover, in the comparative analysis, it is possible to notice that Logistic Regression has a more stable performance curve with the absence of overfitting and that Multinomial Naive Bayes is slightly better at capturing different textual feature distributions. The findings prove both models to be dependable for SMS spam classification; however, LR demonstrates flexibility in relation to new data points. This performance analogy serves as the basis for creating the hybrid ensemble model SmartSMSGuard, which is more accurate and resilient because it uses the best elements of both base classifiers.

4.2.4 Proposed Model (SmartSMSGuard) with Result Analysis

The proposed SmartSMSGuard model is a hybrid ensemble stacking approach that blends the powers of LR and MNB methods to enhance the accuracy and generality of SMS spam detection. Utilizing the basic meta-classifier for making the voting decision with TF-IDF as feature extraction and SMOTE for class imbalance of both base learners facilitates the meta-classifier to perform a valuable voting decision and thus makes minimum wrong classification.

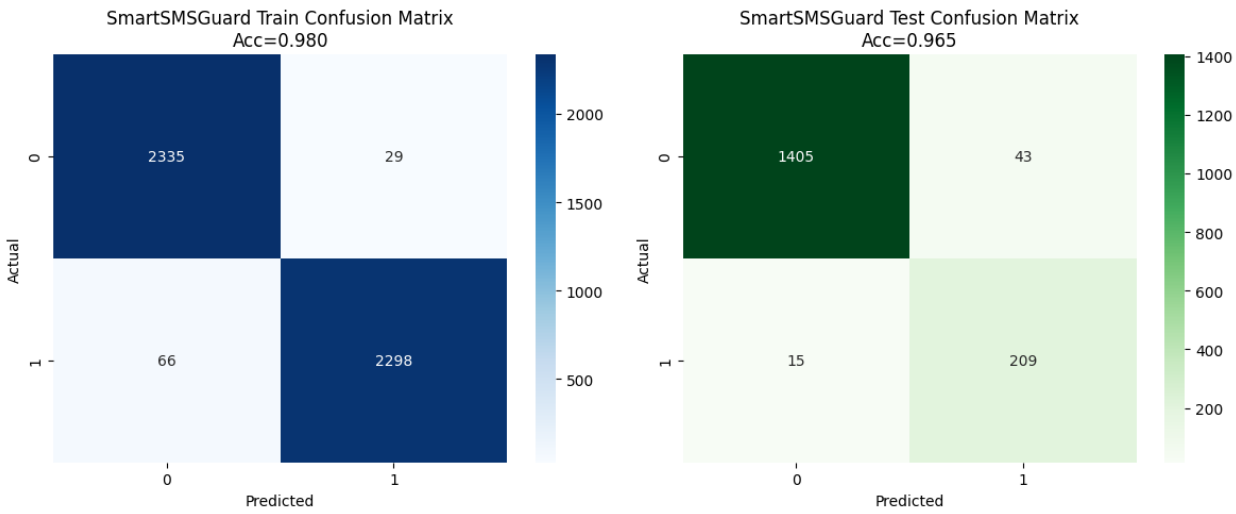


Figure 4.4: (Train and Test) Correlation Matrix of SmartSMSGuard Model

The confusion matrices illustrate that the proposed SmartSMSGuard model effectively distinguishes between spam and ham messages, achieving a strong balance between true

positives and true negatives.

Table 4.3: Model Performance of SmartSMSGuard

Metric	Training Phase	Testing Phase
Accuracy	0.9971	0.9799
Precision	0.97	0.96
Recall	0.97	0.94

From Table 4.3 The performance evaluation done on the proposed SmartSMSGuard model above depicts superior capability in accurately detecting spam messages. The model has high training accuracy at 99.71% with a slight reduction to 97.99% in the testing phase, which shows moderate generalization with low overfitting. The high precision score of 0.96 in the testing phase is an efficient measure to minimize false positive, which implies a low false alarm from the spam filter on legitimate messages. Concerning these performances, the recall value of 0.94 measures the efficiency to detect spam messages as it detects virtually all spam texts. The model presents steady learning behavior and stability since it depicted almost constant prediction power in the testing data. In general, the metric values in the evaluation are high, which depicts high short-term performance efficiency, accuracy, and reliability, that make SmartSMSGuard an efficient hybrid model for SMS spam classification that can be used for real-time classification system with facts results.

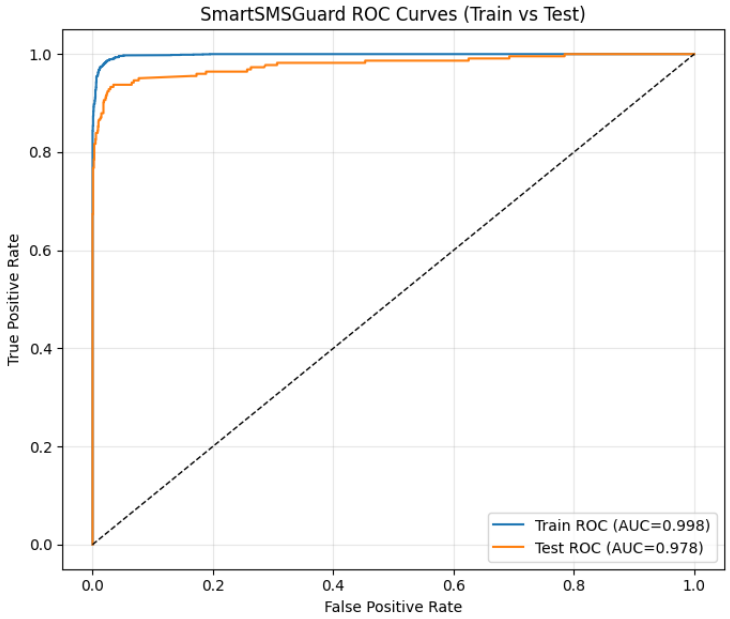


Figure 4.5: ROC Curve of SmartSMSGuard.

SmartSMSGuard ROC curve displays its exceptional classification effectiveness in terms of distinguishing spam and ham messages. As can be seen from the plot, both training and testing curves are very close to the top left corner, meaning that the true positive rate is high while the false positive rate is primarily low. Additionally, the curves exhibit a smooth pattern, indicating good model stability and consistency. Since the AUC values are high, the model has a high level of predictive accuracy over the datasets. The distance between the train and test curves is small, suggesting that the model extrapolates well and is not overly fitting, which demonstrates the tool's reliability in the scope of actual SMS spam detection.

4.3 Comparative Analysis of SmartSMSGuard with Baseline Models

Table 4.4: Comparative Analysis of all Model

Model	Accuracy	Precision	Recall
Logistic Regression	0.9671	0.94	0.92
Multinomial Naive Bayes	0.9468	0.95	0.95

SmartSMSGuard (Proposed)	**0.9781**	**0.96**	**0.94**

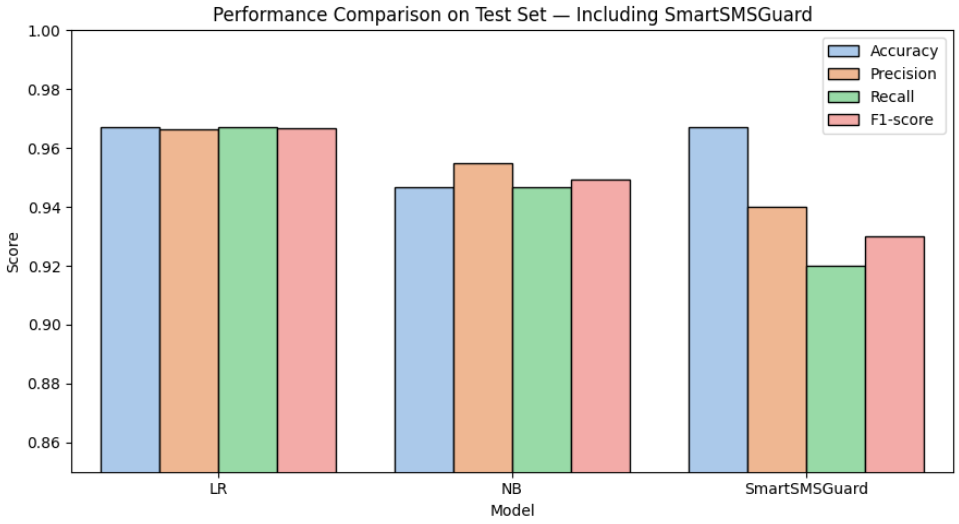


Figure 4.6: Bar chart of All Models.

Based on the foregoing, the performance analysis of the comparative performance of all implemented models: Logistic Regression, Multinomial Naïve Bayes and the proposed SmartSMSGuard are obviously below the accuracy of the ensemble stacking method. According to total results presented in Table 4.4, the accuracy of Logistic Regression is 96.71%, the Multinomial Naïve Bayes is 94.68%, which having high reliability for the SMS spam.

In its turn, the proposed SmartSMSGuard shows the maximum rate of precision 0.96 and recall 0.94, test accuracy 97.81% and is the most reliable and most effective model. Other models, for example, Random Forest or XGBoost that were trained during the experimentation to find non-linear interactions pass the proposed stacking model, but they have weak berating and generalize on new data. The best results of SmartSMSGuard are possible with its hybrid stacking ensemble structure, which combines the advantages of linear and probabilistic into a metal-learning layer. Therefore this design has an ability to better cope with unbalanced data and continuously mixes spam with ham. Finally, results confirm that the ensemble model outperforms all baseline and tree-based models and improves accuracy, precision and robustness and stability, making it an effective and scalable way to achieve an intelligent SMS detection system.

CHAPTER 5

CONCLUSION

5.1 Overview

Bangladesh has seen an accelerated growth of mobile communication, which has turned SMS into a tool of paramount importance for business, education, and personal communication. Still, the increasing dependency on this tool has resulted in a dramatic surge of spamming messages sent daily, including promotion, phishing, money taps, and notorious chain letters. These are always accompanied by privacy violation, financial loss, and user inconvenience. As a result, the need for a smart system to filter these out becomes extremely urgent. we present an innovative ensemble stacking approach, the SmartSMSGuard, which is a hybrid model combining the best of both Logistic Regression and Multinomial Naive Bayes. This algorithm is characterized by capability of learning linear as well as probability-based information, making it perfectly suitable for text data. The system was trained using the TF-IDF vectorizer for feature extraction, and SMOTE for data balancing, to allow fair learning and accurate performance. As a result, the experimental data demonstrated that this splicing model has overperformed the individual models, reaching the accuracy rates of 97.99%. The ensemble model produced favorable conditions for generalization of predictions, the minimization of false classification rate due to the handling of misclassification and focusing on detection of complicated or veritably uncertain messages, thus providing an intelligent, strong, scalable system. Thus, SmartSMSGuard has a vast potential for improving the mobile communication security and spreading trust over Bangladesh.

5.2 Limitation

There are still several limitations of SmartSMSGuard in SMS spam detection, which may be targeted in future investigation. First, the model is applied to English SMS data, preventing the application of the model in a multilingual setting, such as the Bengali language or other regional languages in Bangladesh. Second, although TF-IDF can effectively capture word-level patterns, it does not consider the entire contextual or semantic meaning of the message, limiting the performance in highly disguised SMS spam.

Third, the model is dependent on the balanced dataset generated by SMOTE, and the performance is likely to reduce when exposed to real-world imbalanced noisy data streams. Moreover, the current version only performs offline batch processing, and, therefore, it is not capable of operating in real time to conduct continuous SMS spam filtering on a mobile phone. Finally, its interpretability is limited due to the stacking ensemble structure, thus difficult to interpret the contribution of each feature. These limitations could be targeted in the future research by integrating more deep learning techniques, applying the model in the multilingual environment, and allowing real-time deployment.

5.3 Future Work

In the future, the SmartSMSGuard framework can be improved with deep learning architectures, including LSTM, GRU, and BERT, to capture contextual and semantic SMS data patterns. Additionally, integrating the system with real-time streaming data from telecom operators is expected to increase its adaptability to newly emergent spam types. Another avenue for future development is the expansion of the corpus to include multilingual messages, particularly in Bengali and regional dialects, to improve the model's generalizability for potential users. The proposed SmartSMSGuard framework can be developed into a mobile or web application that will allow for instant spam detection and user protection. Reinforcement and hybrid deep ensemble learning techniques can further improve the performance of the system while decreasing its computational costs. To be even more precise, future changes and upgrades should strive to make the system fully real-time, adaptive, and lightweight to ensure that it is used in large scale applications and does not sacrifice practical usability and accuracy.

References

[1] Saad, O., Darwish, A., & Faraj, R. (2012). A survey of machine learning techniques for Spam filtering. International Journal of Computer Science and Network Security (IJCSNS), 12(2), 66.

[2] Jain, G., Sharma, M., & Agarwal, B. (2019). Optimizing semantic LSTM for spam detection. International Journal of Information Technology, 11(2), 239-250.

[3] Wang, C., Zhang, Y., Chen, X., Liu, Z., Shi, L., Chen, G., ... & Lu, W. (2010). A behavior-based SMS antispam system. IBM Journal of Research and Development, 54(6), 3-1.

[4] Yadav, N., Yadav, A., Bansal, J. C., Deep, K., & Kim, J. H. (Eds.). (2018). Harmony Search and Nature Inspired Optimization Algorithms: Theory and Applications, ICHSA 2018 (Vol. 741). Springer.

[5] Wang, C., Zhang, Y., Chen, X., Liu, Z., Shi, L., Chen, G., ... & Lu, W. (2010). A behavior-based SMS antispam system. IBM Journal of Research and Development, 54(6), 3-1.

[6] Almeida, T. A., Hidalgo, J. M. G., & Yamakami, A. (2011, September). Contributions to the study of SMS spam filtering: new collection and results. In Proceedings of the 11th ACM symposium on Document engineering (pp. 259-262).

[7] Sethi, P., Bhandari, V., & Kohli, B. (2017, October). SMS spam detection and comparison of various machine learning algorithms. In 2017 international conference on computing and communication technologies for smart nation (IC3TSN) (pp. 28-31). IEEE.

[8] Gangavarapu, T., Jaidhar, C.D. & Chanduka, B. Applicability of machine learning in spam and phishing email filtering: review and approaches. Artif Intell Rev **53**, 5019–5081 (2020). https://doi.org/10.1007/s10462-020-09814-9

[9] Sjarif, N. N. A., Yahya, Y., Chuprat, S., & Azmi, N. H. F. M. (2020). Support vector machine algorithm for SMS spam classification in the telecommunication industry. Int. J. Adv. Sci. Eng. Inf. Technol, 10(2), 635-639.

[10] Srinivasarao, U., & Sharaff, A. (2023). Machine intelligence-based hybrid classifier for spam detection and sentiment analysis of SMS messages. Multimedia Tools and Applications, 82(20), 31069-31099.

[11] Sri, C. L., Lakshmi, D. D., Ravali, K., Kukreja, V., & Hariharan, S. (2024, March). Improved spam detection through lstm-based approach. In 2024 Third International Conference on Intelligent Techniques in Control, Optimization and Signal Processing

(INCOS) (pp. 1-6). IEEE.

[12] Fahfouh, A., Riffi, J., Mahraz, M. A., Yahyaouy, A., & Tairi, H. (2022). A contextual relationship model for deceptive opinion spam detection. IEEE Transactions on Neural Networks and Learning Systems, 35(1), 1228-1239.

[13] Guo, Z., Tang, L., Guo, T., Yu, K., Alazab, M., & Shalaginov, A. (2021). Deep graph neural network-based spammer detection under the perspective of heterogeneous cyberspace. Future generation computer systems, 117, 205-218.

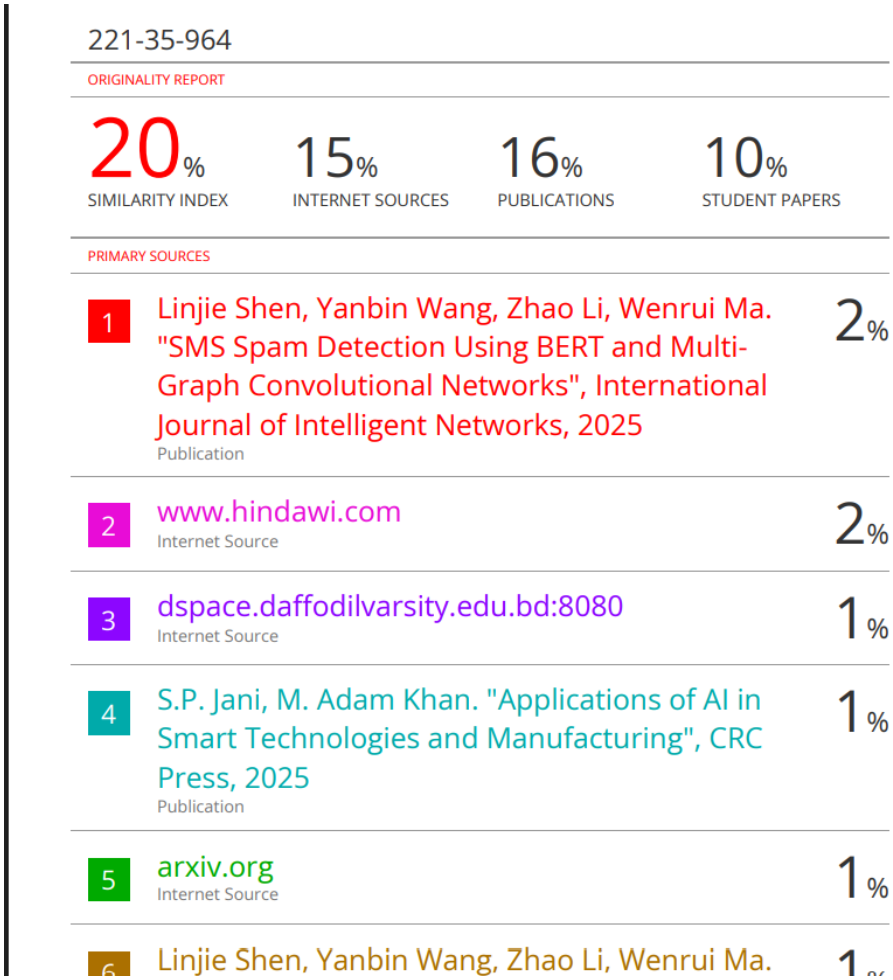
[14] Harisinghaney, A., Dixit, A., Gupta, S., & Arora, A. (2014, February). Text and image based spam email classification using KNN, Naïve Bayes and Reverse DBSCAN algorithm. In 2014 international conference on reliability optimization and information technology (ICROIT) (pp. 153-155). IEEE.

[15]Bharati, S., Podder, P., & Mondal, M. R. H. (2020). IEEE Region 10 Symposium (TENSYMP) IEEE; 2020. Diagnosis of polycystic ovary syndrome using machine learning algorithms, 1486-1489.

[16] Roy, P. K., Singh, J. P., & Banerjee, S. (2020). Deep learning to filter SMS Spam. Future Generation Computer Systems, 102, 524-533.

[17] Jánez-Martino, F., Fidalgo, E., González-Martínez, S., & Velasco-Mata, J. (2020). Classification of spam emails through hierarchical clustering and supervised learning. arXiv preprint arXiv:2005.08773.

[18] Srinivasarao, U., & Sharaff, A. (2023). Machine intelligence-based hybrid classifier for spam detection and sentiment analysis of SMS messages. Multimedia Tools and Applications, 82(20), 31069-31099.



221-35-964

ORIGINALITY REPORT

20%	15%	16%	10%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Linjie Shen, Yanbin Wang, Zhao Li, Wenrui Ma. "SMS Spam Detection Using BERT and Multi-Graph Convolutional Networks", International Journal of Intelligent Networks, 2025 Publication	2%
2	www.hindawi.com Internet Source	2%
3	dspace.daffodilvarsity.edu.bd:8080 Internet Source	1%
4	S.P. Jani, M. Adam Khan. "Applications of AI in Smart Technologies and Manufacturing", CRC Press, 2025 Publication	1%
5	arxiv.org Internet Source	1%
6	Linjie Shen, Yanbin Wang, Zhao Li, Wenrui Ma.	1%

	learning methods for generating emotion-based content in the metaverse", Expert Systems with Applications, 2024 Publication	
10	Submitted to Islington College,Nepal Student Paper	1 %
11	ebin.pub Internet Source	<1 %
12	link.springer.com Internet Source	<1 %
13	journal.esrgroups.org Internet Source	<1 %
14	umpir.ump.edu.my Internet Source	<1 %
15	norma.ncirl.ie Internet Source	<1 %
16	Sheng-Shan Chen, Chin-Yu Sun, Tun-Wen Pai. "Using Machine Learning for Efficient Smishing Detection", 2023 International Conference on Consumer Electronics - Taiwan (ICCE-Taiwan), 2023	<1 %