International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 08 Issue: 03 | March - 2024 SJIF Rating: 8.448 ISSN: 2582-3930

SMS SPAM DETECTION WITH MULTINOMIAL NAIVE BAYES

Mrs. J Mounika[1], Ms. Pallerla Sai Navya[2], Ms. Nadikattu Jayadeepika[3],

Ms. Nukala Harsha Vardhani[4], Ms. Kolluri Priscilla[5]

[1] Asst. Professor, Dept. Information Technology, KKR & KSR Institute of Technology and Sciences, Guntur, India

[2-5]Student, Dept. Information Technology, KKR & KSR Institute of Technology and Sciences, Guntur, India

---

Abstract *- SMS (short messaging service) usage has increased dramatically as a result of the growth in mobile users, enabling text messaging between smartphone and landline users. But there has also been a noticeable increase in unsolicited communications, or spam, coinciding with this growth in SMS usage. Through marketing campaigns and attempts to gain private information, such as credit card numbers, these spam messages seek to further business or financial objectives. The duty of removing spam mails has therefore grown in significance. In response, a number of deep learning and machine learning methods have been used to identify SMS spam. Using data from the University of California, Irvine (UCI), this research examines the application of such strategies.*

Key Words: *MultinomailNaiveBayes, SMS Spam Detection, NLTK, Vectorization, Feature Extraction.*

1 .INTRODUCTION

These days, we practically live our lives through our mobile gadgets. Texting is now the primary method of communication for many people, and it has grown incredibly popular. Spam is one of the major problems that come with this popularity. Texts that bombard our phones with unsolicited and occasionally dangerous content, known as spam, aim to obtain personal information and put users' security at risk. Technology such as machine learning, which can automatically detect and filter spam communications, can be used to solve this issue.

Multinomial Naïve Bayes classifier is the efficient method.With the use of this classifier, computers can now analyze and sort text. It distinguishes between spam and ham messages by looking at word patterns and other aspects of the messages.

2. LITERATURE SURVEY

"In the year 2021, XIAOXU LIU, HAOYE LU, AND AMIYA NAYAK on SMS spam detection, prior research has predominantly employed traditional machine learning classifiers such as Logistic Regression, Naïve Bayes, Random Forests, Support Vector Machine, Long Short-Term Memory, and CNN-LSTM. Although these methods have shown some degree of efficacy, the introduction of Transformer models offers a fascinating path toward investigating enhanced spam detection capabilities [1].

"In the year 2020, Tian Xia and Xuemin Chen thoroughly investigated SMS spam detection techniques .and blended more conventional methods such as convolutional neural networks (CNN) and long short-term memory (LSTM) with state-of-the-art methods like support vector machines, naïve Bayes, and vector space models. These approaches usually use the Bag of Words (BoW) paradigm, which treats words as an unordered set and ignores important word order information. Although the BoW model works well, difficult to spot subtle trends in SMS spam since it cannot capture sequential data. As a result, scientists are currently investigating a number of strategies to improve the efficacy of detection[2].

"In the year 2021, Sridevi Gadde,A.Lakshmanarao and S.Satyanarayana, exponential rise in the mobile device usage has led a substantial increase in Short Message Service (SMS) traffic, Accompanied by a surge in spam messages. So Spammers use this platform to advantage for Monetary or commercial benefit, which has increased attention to Spam classification. This study uses a variety of Machine learning Techniques to handle problem and deep learning methods for identifying the SMS spam. authors develop a spam detection model using a dataset from UCI. Their experimental results show that their Long Short-Term Memory (LSTM) model outperforms earlier models, obtaining a 98.5% accuracy rate [3].

"The widespread use of devices like mobile phones has led to the growth of the Short Message Service (SMS) industry, which is estimated to be worth billions of dollars by Abhishek Patel, Priya Jhariya, Sudalagunta Bharath, and Ankita Wadhawan in 2021. with texting services becoming less cost, there's been a rise in unsolicited business offers and SMS spam. In some regions like parts of Asia up to thirty percent of SMS messages were discovered to be spam in 2012. The primary causes of challenges in SMS spam filtering include short messages, limited functionality[4].

"According to Kavya P and Dr. A. Rengarajan, with increase of mobile phone usage and technological advancements, unwanted SMS spam messages makes a threat to user privacy and data security. there is currently no comprehensive literature study on SMS spam detection, as this area is still in its early stages. The study considering SMS spam detection as a two-class document classification problem and using machine learning approaches for filtering. The main aim is to design a Naive Bayes model for spam message recognition using Flask, a Python web service development micro-framework, and create an API for the model [5].

"This paper examines recent developments in spam text identification through Machine Learning, Deep Learning, and text-based methods. The article also covers the most challenges, control mechanisms, and datasets which are utilized in social media spam detection research
Sanaa Kaddoura, Ganesh Chandrasekaran, Daniela Elena Popescu, and Jude Hemanth Duraisamy want to detect spam across several social media platforms mailnly, including Twitter, Facebook, YouTube, and email by 2022. The epidemic caused an increase in spam content, such as malicious links, fraudulent accounts, and fake news [6].

"Chensu Zhao, Yang Xin, Xuefeng Li, Yixian Yang, and Yuling Chen present a new methodology for detecting spam in the social networks in 2020, which addresses issue of imbalanced data. To accomplish effective classification, the method employs heterogeneous stacking-based ensemble technique that combines six distinct base classifiers with cost-sensitive learning in a deep neural network. Experiments with Twitter data indicate better performance than conventional methods. Future research aims to improve spam identification by investigating deeper feature representations and experimenting with the other dataset features [7].

"Through an analysis of more than thirty scientific journals, N. Widiastuti did research in 2019 that looked at the development of spam detection algorithms. Notwithstanding the achievements of Convolutional Neural Networks (CNN) in text mining and Natural Language Processing (NLP) fields for tasks like sentiment analysis and document classification, difficulties still exist, especially in computing efficiency and uncharted territory like named entity recognition. According to the study, CNN's computational efficiency should be assessed, and further NLP applications should be investigated, especially with regard to improving spam detection techniques [8].

"Because SMS doesn't require an active internet connection, it continues to be a vital form of communication in today's digital world. However, strong identification systems are required due to SMS vulnerabilities to spammers and hackers. With over 95% accuracy, Authors Suman Kumar Das, Soumyabrata Saha, and Suparn Das Gupta in 2020 studied that, machine learning-based method that uses TF-IDF Vectorizer to identify the fraudulent SMS. So, output highlight how the machine learning algorithms can effectively counter SMS-based attacks, resulting in a mobile computing environment that is more secure [9].

"The technique for SMS spam detection was presented by Sahar Bosaeed, Iyad Katib, and Rashid Mehmood in 2020. For both incoming and outgoing SMS, application is flexible. Operating on cloud, fog, or edge layers, it makes use of preprocessing techniques and the machine learning classifiers like Naive Bayes and Support Vector Machine. An analysis of fifteen datasets produces recommendations based on user preferences. Flexible classification and execution are offered by the Weka-based implementation, where SVM performs better than alternative techniques. Future studies will focus on improving categorization methods and tackling growing problem of SMS spam in communities and smart cities. [10]

"In 2021 study by Kanza Hanif and Hamid Ghous looks into use of graphical representation, deep learning, and the machine learning approaches in Android applications to filter the spam SMS texts. Small, language-specific datasets and inadequate pre-processing and feature selection techniques are among the limitations. Larger datasets, hybrid models combining deep learning and machine learning approaches, and enhanced pre-processing techniques ought to be main foci of future research. This report identifies problems in detecting and reducing SMS spam and makes recommendations for future research and development [11].

"A semi-supervised approach to spam SMS detection was proposed in the year 2014 by Ishtiaq Ahmed, Rahman Ali, Donghai Guan, Young-Koo Lee, Sungyoung Lee, and TaeChoong Chung. The approach which uses frequent itemset mining and ensemble learning with minimal labelled data to effectively expand feature sets from positive and unlabeled SMS dataset, improving security and accuracy especially with limited positive instances. Further research will includes of extending the methodology to other languages and supervised learning applications, as well as optimising minimum support for the diverse datasets [12].

"In year 2020, Wael Hassan Gomaa examines the SMS spam filtering, highlighting SMS marketing's continued Importance in face of the growing Spam concerns. It compares the Deep learning Techniques with classical Machine learning classifiers, Achieving 99.26% accuracy with Random Multi model Deep Learning(RMDL) on dataset of 5574 records. A review of prior studies is conducted, recommending continued advancements in spam filtering. Deep learning Techniques like CNN and RNN are combined with classical classifiers like Naive Bayes and Decision Trees in proposed methods. Future research will use transfer learning and Hierarchical Deep Learning for Text (HDLTex) Algorithms to

increase Identification accuracy [13].

"Deep Convolutional Forest (DCF), a dynamic ensemble model for mobile spam detection that combines the convolutional layers with base classifiers, is first presented in a work by Mai A. Shaaban, Yasser F. Hassan, and Shawkat K. Guirguis in 2022. DCF outperforms deep neural networks and the Conventional classifiers with an accuracy of 98.38% by the Dynamically Adjusting Complexity. It is very important when times like COVID-19 epidemic ,because it reduces Security concerns and spread the false information. Scope of future research could include image-based Classification and multilingual Spam Detection. Extensive usage of this paper is permitted under the terms of Creative Commons Attribution 4.0 International License[14].

"In 2020, Dima Suleiman1, Ghazi Al-Naymat and Mariam Itriq paper tackles SMS spam detection using machine learning Algorithms like DL, RF, and NB, discussing unique challenges are compared to the email spam. It suggests the framework that includes feature extraction, choosing an algorithm, and assessing it with a range of criteria. Key characteristics for spam identification, such as message length and digit presence, are highlighted by experiments on a UCI dataset. Both DL and RF performance are optimized by tuning parameters, with RF emerging as the most efficient classifier. All things considered, the study offers a thorough method for effective SMS spam identification that makes the use of Machine learning and H2O platform [15].

3. PROPOSED SYSTEM

Addressing any missing or corrupted data as well as balancing the dataset in the event of a class imbalance problem are included in the data preprocessing step. Furthermore, addressing noisy data or outliers that may have an impact on model performance may receive further attention.

To verify robustness and lower the chance of overfitting, methods such as k-fold cross-validation may be used during model evaluation. To do this, divide the data into k subgroups. Then, train the model on k-1 subsets, then test it on the remaining subset. Every subset serves as the test set once during the k iterations of this procedure.

By capturing more subtle patterns in the text input, feature engineering approaches like word embeddings and n-grams may be investigated to improve the efficacy of the model.

3.1 WORKFLOW

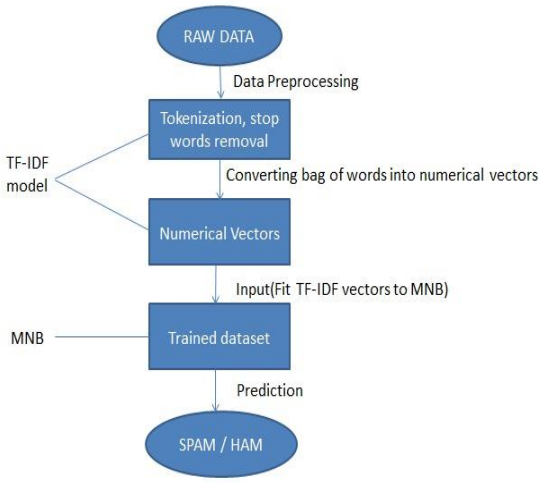

Fig 1 Represents the Workflow of project

3.2 IMPLEMENTATAION METHODS

1. Data importing and pre-processing process. Separate unique SMS messages from the folders in our devices (ham or spam) to check the data

2. Feature Extraction: Take basic features like (text content, images , special symbols and other data) from the SMS data. Use the techniques like bag-of-words for representation or TF-IDF to change the data from the text into numerical feature data.

3. Building the Model: By using the toolkit named as scikit-learn, create a model called multinomial Naive Bayes .And then Analyze the model of this archictecture And also how this model algorithm's values are defined.

4. Model training: By preprocessing text data, Evaluate the Multinomial Naive Bayes model in step four. Using the class labels (spam or non-spam), fit the model to get the probability distribution of different features..

5. Model Evaluation: Moving forward, Take the trained models metrics like F1-score, accuracy, precision, and recall. And then later to evaluate these metric performance, divide the set of data into trained data and testing sets.

6. Speculation: Take received SMS messages whether it is spam or not We use the testing techniques to predict them. show the user with the prediction's findings, whether the given message is ham or not .

4. RESULT ANALYSIS

The number of spam and non-spam messages that were successfully or wrongly identified is determined by examining a confusion matrix, which is the result of training the model. Metrics such as accuracy, precision, recall, and F1-score are computed to assess overall performance and the trade-off between accurately detecting spam and reducing false alerts. With ROC curves, we analyze the trade-off between precision and recall while visualizing the trade-offs between true positive rate and false positive rate. To further uncover trends and opportunities for enhancement, we carefully examine misclassified messages. We compare our model's performance with other approaches for SMS spam identification and use cross-validation to guarantee the validity of our conclusions. To guarantee that the model's conclusions are consistent with how people view spam communications, we lastly take into account how interpretable its decisions are. Moreover, we supplied 95%

Copy and paste the message

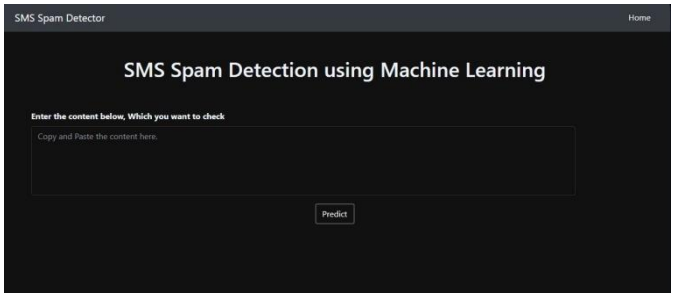

Fig 2 copy and paste the message

click on the predict button

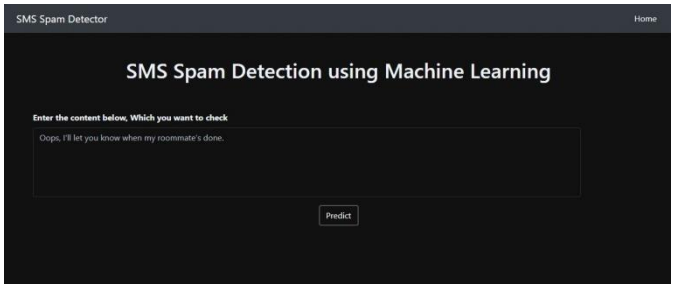

Fig 3 click on predict button

Final Prediction:-

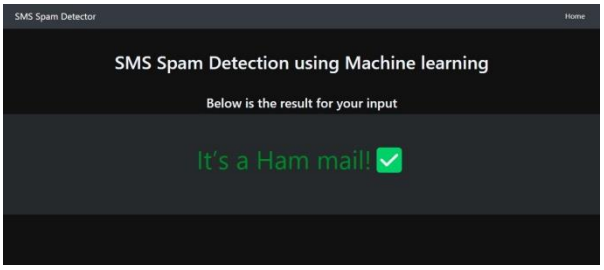

Fig 4 Result of Prediction of SMS(HAM Message)

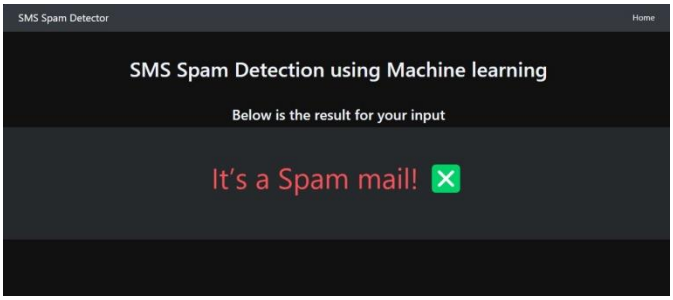

Fig 5 Result of Prediction of SMS(SPAM Message)

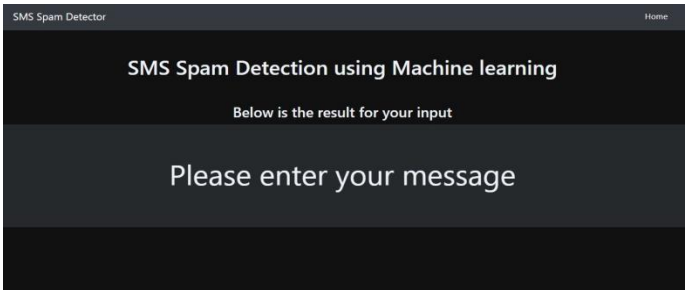

Fig 6 Output screen if no message is placed in the box and try to predict the message nature

5. CONCLUSION

A reliable method for distinguishing between spam and non-spam messages is shown by the use of Multinomial Naive Bayes in the SMS spam detection system. The system is able to categorize SMS messages with impressive accuracy by means of thorough data preparation, model training, and evaluation. This helps to reduce the amount of unsolicited spam communication. The system is made more useful and dependable in real-world situations by regular updates and ongoing monitoring that guarantee it stays responsive to changing spamming tactics and messaging patterns. All things considered, project emphasizes how important it is to

use machine learning approaches to fight spam and shows how much more spam detection technology can advance.

6. REFERENCES

[1]XIAOXU LIU, HAOYE LU, AND AMIYA NAYAK, "A Spam Transformer Model for SMS Spam Detection", VOLUME 9, 2021, IEEE access, https://doi.org/10.1109/ACCESS.2021.3081479.

[2]Tian Xia and Xuemin Chen, A Discrete Hidden Markov Model for SMS Spam Detection, Appl. Sci. 2020, 10, 5011; doi:10.3390/app10145011.

[3]Sridevi Gadde, A .Lakshmanarao and S.Satyanarayana, SMS Spam Detection using Machine Learning and Deep Learning Techniques, 2021 7th International Conference on Advanced Computing & Communication Systems (ICACCS), DOI: 10.1109/ICACCS51430.2021.9441783.

[4] Abhishek Patel , Priya Jhariya , SudalaguntaBharath and Ankita Wadhawan, SMS Spam Detection using Machine Learning Approach, © 2021 IJCRT |Volume 9, Issue 4 April 2021 | ISSN: 2320-2882.

[5] Kavya P , Dr. A. Rengarajan, A Comparative Study for SMS Spam Detection, International Journal of Trend in Scientific Research and Development (IJTSRD) Volume 5 Issue 1, November-December 2020 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470, Unique Paper ID – IJTSRD38094.

[6] Sanaa Kaddoura, Ganesh Chandrasekaran, Daniela Elena Popescu and Jude Hemanth Duraisamy ,A systematic literature review on spam content detection and classification,2022, PeerJ Comput. Sci. 8:e830 DOI 10.7717/peerj-cs.830.

[7] Chensu Zhao ,Yang Xin ,Xuefeng Li , Yixian Yang and Yuling Chen, A Heterogeneous Ensemble Learning Framework for Spam Detection in Social Networks with Imbalanced Data,MDPI, Appl. Sci. 2020, 10, 936; doi:10.3390/app10030936.

[8] N. Widiastuti, Convolution Neural Network for Text Mining and Natural Language Processing, 2019, IOP Conference Series: Materials Science and Engineering, doi:10.1088/1757-899X/662/5/052010.

[9] Suparna Das Gupta, Soumyabrata Saha and Suman Kumar Das, SMS Spam Detection Using Machine Learning,Journal of Physics: Conference Series,Volume 1797, International Online Conference on Engineering Response to COVID-19 (IOCER-COVID-19) 2020 8-9 October 2020, JIS College of Engineering, Kalyani, West Bengal, India, DOI 10.1088/1742-6596/1797/1/012017.

[10] Sahar Bosaeed, Iyad Katib, Rashid Mehmood, A Fog-Augmented Machine Learning based SMS Spam Detection and Classification System, 2020 Fifth International Conference on Fog and Mobile Edge Computing (FMEC), 978-1-7281-7216-3/20/$31.00 ©2020 IEEE.

[11] Kanza Hanif , Hamid Ghous, DETECTION OF SMS SPAM AND FILTERING BY USING DATA MINING METHODS: LITERATURE REVIEW, e-ISSN: 2582-5208 International Research Journal of Modernization in Engineering Technology and Science Volume:03/Issue:01/January-2021 Impact Factor- 5.354 www.irjmets.com.

[12] Ishtiaq Ahmed , Rahman Ali, Donghai Guan, Young-Koo Lee, Sungyoung Lee, TaeChoong Chung,Semi-supervised learning using frequent itemset and ensemble learning for SMS classification, Expert Systems with Applications (2014), http://dx.doi.org/10.1016/j.eswa.2014.08.054.

[13] Wael Hassan Gomaa, The Impact of Deep Learning Techniques on SMS Spam Filtering , (IJACSA) International Journal of Advanced Computer Science and Applications,Vol. 11, No. 1, 2020.

[14] Mai A. Shaaban, Yasser F. Hassan and Shawkat K. Guirguis, Deep convolutional forest: a dynamic deep ensemble approach for spam detection in text,Springer, Complex & Intelligent Systems (2022) 8:4897–4909,https://doi.org/10.1007/s40747-022-00741-6.

[15] Dima Suleiman1, Ghazi Al-Naymat and Mariam Itriq, Deep SMS Spam Detection using H2O Platform, ISSN 2278-3091,Volume 9, No.5, September - October 2020International Journal of Advanced Trends in Computer Science and Engineering, https://doi.org/10.30534/ijatcse/2020/326952020.