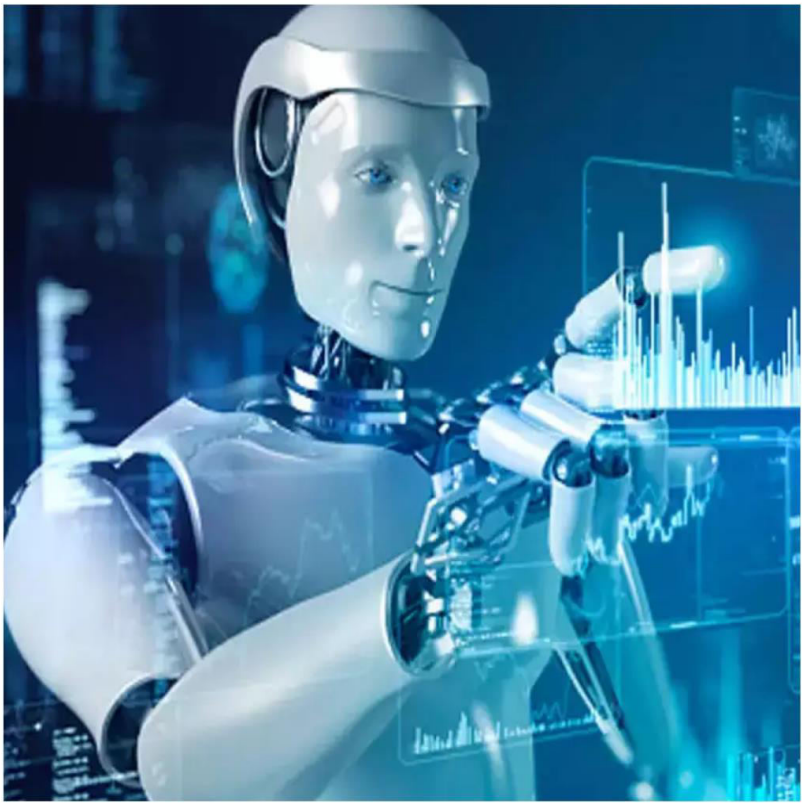
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.524

Volume 14, Issue 1, January 2025

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 1, January 2025

|DOI: 10.15680/IJIRSET.2025.1401046|

SMS Spam Filtering

Prof.Suman Puri[1], Vaibhav Subhash Daundkar[2], Renuka Ajit Ozarkar[3], Aditya Madhukar Karke[4], Sonam Mahendra Wakode[5]

Guide, Department of Computer Engineering, Rajarshi Shahu College of Engineering, Polytechnic, Tathawade, Pune, India [1]

Student, Department of Computer Engineering, Rajarshi Shahu College of Engineering, Polytechnic, Tathawade, Pune, India [2,3,4,5]

ABSTRACT: The number of people using mobile devices increasing day by day. SMS (short message service) is a text message service available in smartphones as well as basic phones. So, the traffic of SMS increased drastically. The spam messages also increased. The hackers try to send spam messages for their financial or business benefits like market growth, lottery ticket information, credit card information, etc. So, spam classification has special attention. In this paper, we applied various machine learning and deep learning techniques for SMS spam detection. we used a dataset to train the machine learning and deep learning models like LSTM and NB. The SMS spam collection data set is used for testing the method. The dataset is split into two categories for training and testing the research. Our experimental results have shown that our NB model outperforms previous models in spam detection with an accuracy of good.

I. INTRODUCTION

Prediction of SMS spam has been an important area of research for a long time. the goal is to apply different machine learning algorithms to SMS spam classification problem, compare their performance to gain insight and further explore the problem, and design an application based on one of these algorithms that can filter SMS spams with high accuracy. The current work proposes a gamut of machine learning and deep learning-based predictive models for accurately predicting the sms spam movement. The predictive power of the models is further enhanced by introducing the powerful deep learning-based long- and short-term memory (LSTM) network into the predictive framework.

1. The Proposed mode is based on the study of sms text data and technical indicators. Algorithm selects best free parameters combination for LSTM to avoid over-fitting and local minima problems and improve prediction accuracy.
2. Our dataset consists of one large text file in which each line corresponds to a text message. Therefore, preprocessing of the data, extraction of features, and tokenization of each message is required. After the feature extraction, an initial analysis on the data is done using label encoder and then the models like naive Bayes (NB) algorithm and LSTM are used on next steps are for prediction.
3. The two methods used to predict the spam messages that are Fundamental and technical analyses. .

II. LITERATURE SURVEY

TITLE: SMS Spam Detection Based on Long Short-Term Memory and Gated Recurrent Unit
Author: Pumrapee Poomka, Wattana Pongsena, Nittaya Kerdprasop, and Kittisak Kerdprasop YEAR: - 2019
Abstract: An SMS spam is the message that hackers develop and send to people via mobile devices targeting to get their important information. For people who are ignorant, if they follow the instruction in the message and fill their important information, such as internet 19 banking account in a faked website or application, the hacker may get the information. This may lead to loss their wealth. The efficient spam detection is an important tool in order to help people to classify whether it is a spam SMS or not. In this research, we propose a novel SMS spam detection based on the case study of the SMS spams in English language using Natural Language Process and Deep Learning techniques. To prepare the data for our model development process, we use word tokenization, padding data, truncating data and word embedding to make more dimension in data. Then, this data is used to develop the model based on Long Short-Term Memory and Gated Recurrent Unit algorithms. The performance of the proposed models is compared to the models based on machine learning algorithms including Support Vector Machine and Naïve Bayes. The experimental results show that the model built from the Long Short-Term Memory technique provides the best overall accuracy as high as

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 1, January 2025

|DOI: 10.15680/IJIRSET.2025.1401046|

98.18%. On accurately screening spam messages, this model shows the ability that it can detect spam messages with the 90.96% accuracy rate, while the error percentage that it misclassifies a normal message as a spam message is only 0.74%.

TITLE: SMS Spam Message Detection using Term Frequency-Inverse Document Frequency and Random Forest Algorithm
Author: Haslina Md Sarkan, Yazriwati Yahya, Suriani Mohd Sam
YEAR: - 2019
Abstract: The daily traffic of Short Message Service (SMS) keeps increasing. As a result, it leads to dramatic increase in mobile attacks such as spammers who plague the service with spam messages sent to the groups of recipients. Mobile spams are a growing problem as the number of spams keep increasing day by day even with the filtering systems. Spams are defined as unsolicited bulk messages in various forms such as unwanted advertisements, credit opportunities or fake lottery winner notifications. Spam classification has become more challenging due to complexities of the messages imposed by spammers. Hence, various methods have been developed in order to filter spams. In this study, methods of term frequency-inverse document frequency (TF-IDF) and Random Forest Algorithm will be applied on SMS spam message data collection. Based on the experiment, Random Forest algorithm outperforms other algorithms with an accuracy of 97.50% 20

TITLE: Spam Detection Approach for Secure Mobile Message Communication Using Machine Learning Algorithms
Author: Shah Nazir,2 Habib Ullah Khan,3 and Amin Ul Haq
YEAR: - 2020
Abstract: The spam detection is a big issue in mobile message communication due to which mobile message communication is insecure. In order to tackle this problem, an accurate and precise method is needed to detect the spam in mobile message communication. We proposed the applications of the machine learning-based spam detection method for accurate detection. In this technique, machine learning classifiers such as Logistic regression (LR), K-nearest neighbor (K-NN), and decision tree (DT) are used for classification of ham and spam messages in mobile device communication. The SMS spam collection data set is used for testing the method. The dataset is split into two categories for training and testing the research. The results of the experiments demonstrated that the classification performance of LR is high as compared with K-NN and DT, and the LR achieved a high accuracy of 99%. Additionally, the proposed method performance is good as compared with the existing state-of-the-art methods.

III. SYSTEM ARCHITECTURE

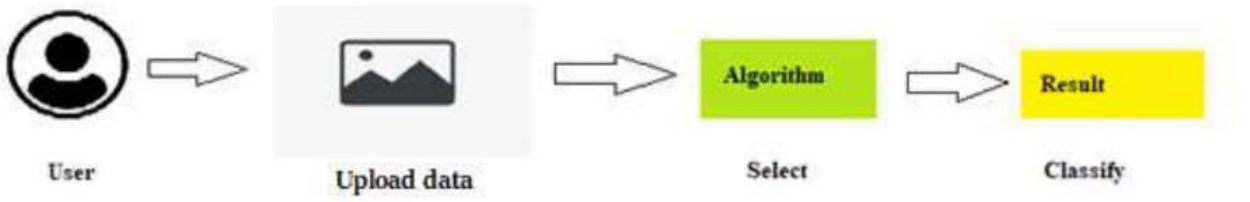


Fig 1. System Architecture

The SMS spam message problem is plaguing almost every country and keeps increasing without a sign of slowing down as the number of mobile users increase in addition to cheap rates of SMS services. Therefore, this paper presents the spam filtering technique using various machine learning algorithms. Based on the experiment, TF-IDF with Nave bayes classification algorithm outperforms good compare to other algorithm like LSTM in terms of accuracy percentage. However, it is not enough to evaluate the performance based on the accuracy alone since the dataset is imbalanced. After some examinations, NB algorithm still manages to provide good precision and fmeasure with 0.98 of precision while 0.97 for f-measure. Different algorithms will provide different performances and results based on the features used. For future works, adding more features such as message lengths might help the classifiers to train data better and give better performance.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 1, January 2025

|DOI: 10.15680/IJIRSET.2025.1401046|

IV. PROPOSED SYSTEM

Mobile spam messages are a common problem faced by mobile device users globally, causing inconvenience and harm. Traditional methods of spam detection on mobile devices have typically relied on rule-based filters and keyword blocking, limiting their ability to detect new and emerging spam messages. Therefore, the problem formulation of this research is to propose an innovative spam detection application in Flutter that uses machine learning algorithms and natural language processing techniques to accurately identify and filter spam messages on mobile devices. The goal of the proposed spam detection application is to develop an efficient, effective, and user-friendly solution to help mobile device users filter out unwanted spam messages without requiring manual intervention. This application will be developed using Flutter, enabling it to run seamlessly on both Android and iOS devices, and the spam detection algorithm will use supervised and unsupervised machine learning algorithms to classify messages as spam or genuine messages. The application's spam filter database will be continuously updated with emerging spam patterns to optimize the spam detection algorithm's accuracy and efficiency. The problem formulation of the proposed spam detection application includes the following steps:

1. Data Collection - Collecting raw data from mobile device users to build a comprehensive dataset of spam and genuine messages.
2. Feature Extraction - Extracting the relevant features such as metadata and content from the collected dataset and transforming them into a numerical format for input into machine learning algorithms.
3. Machine Learning Algorithm Development - Developing a robust machine learning algorithm that effectively classifies spam and genuine messages with high accuracy.
4. Integration with Flutter - Developing the application's user interface using Flutter and integrating the machine learning algorithm into the application that runs seamlessly in the background without affecting the device's performance.
5. Testing and Validation - Testing and validating the spam detection application's performance on various real-world datasets to ensure accuracy and efficiency. Hence, the problem formulation of the proposed spam detection application aims to develop a cutting-edge solution to the problem of spam on mobile devices, which can enhance the user's privacy and improve their overall mobile experience

V. CONCLUSION

In conclusion, the proposed spam detection application in android is a state-of-the-art solution developed to effectively tackle spam messages on mobile devices. The application employs machine learning algorithms and natural language processing techniques to accurately identify and filter spam messages in real-time, making mobile users more secure and enhancing their mobile experience.

REFERENCES

[1]. D. Barrera et al., “A Methodology for Empirical Analysis of Permission-Based Security Models and Its Application to Android,” Proc. 17th ACM Conf. Computer and Communications Security (CCS 10), ACM, pp. 73-84, 2010.
[2]. Stefan Frei, Thomas Duebendofer, Gunter Ollman, and Martin May, Understanding the Web browser threat: Examination of vulnerable online Web browser populations and the insecurity iceberg Archived September 11, 2016, at the Wayback Machine, Communication Systems Group, 200.
[3]. I. Burguera, U. Zurutuza, and S. Nadjm-Tehrani, “Crowdroid: Behavior-Based Malware Detection System for Android,” Proc. ACM Workshop Security and Privacy in Mobile Devices (SPMD 11), ACM, pp. 15-26, 2011.
[4]. Kanaris I, Kanaris K, Houvardas I, Stamatatos E (2006) Words vs. Character n-grams for Anti-spam Filtering. International Journal on Artificial Intelligence Tools XX(X):1–20.
[5]. J. Drew, Malware growth maintains rapid pace as mobile threats surge, found 10 September 2012, Accessible via: http://www.journalofaccountancy.com/News/20126400.htm.
[6]. Bhowmick, Alexy & Hazarika, Shyamanta. (2018). E-Mail Spam Filtering: A Review of Techniques and Trends. 10.1007/978-981-10-4765-7_61.
[7]. Yerazunis WS (2003) Sparse Binary Polynomial Hashing and the CRM114 Discriminator Rough Guide to this Talk. In: MIT Spam Conference.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 1, January 2025

|DOI: 10.15680/IJIRSET.2025.1401046|

[8]. Siefkes C, Assis F, Chhabra S, Yerazunis WS (2004) Combining Winnow and Orthogonal Sparse Bigrams for Incremental Spam Filtering. In: European Conference on Machine Learning (ECML), pp 410–421.
[9]. Zhu, Yuanchun & Tan, Ying. (2011). A Local-Concentration-Based Feature Extraction Approach for Spam Filtering. Information Forensics and Security, IEEE Transactions on. 6. 486 - 497. 10.1109/TIFS.2010.2103060.
[10].C. Mulliner, C. Miller, “Injecting SMS Messages into Smart Phones for Security Analysis,” in Proceedings of the 3rd USENIX Workshop on Offensive Technologies (WOOT), 2009

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details