Spam analysis and classification of the dynamic message using a vectorizing technique with multi-model machine learning algorithm

Sumeet Kumar Gamango[1], **A Kethsy Prabavathy**[2]

[1]Department of Computer Science and Engineering, Karunya Institute of Technology and Sciences, Coimbatore 641114, Tamil Nadu, India.

sumeet.gamango96@gmail.com

[2]Assistant Professor, Department of Computer Science and Engineering, Karunya Institute of Technology, Deemed University,
Karunya Nagar, Coimbatore, Tamil Nadu, India
kethsy_cse@karunya.edu

Abstract - Spam analysis and classification of dynamic messages is an essential task in order to combat the ever-increasing volume of unsolicited and malicious emails. One effective approach is to employ a vectorizing technique along with a multi-model machine learning algorithm. This approach involves representing email messages as high-dimensional vectors, capturing various features such as word frequencies, presence of specific keywords, and structural characteristics. By transforming the text into numerical representations, the machine learning algorithm can then learn patterns and make predictions based on these representations. The use of a multi-model algorithm allows for the integration of different classification models, each with its own strengths and weaknesses, to enhance the overall performance. This approach can achieve high accuracy by leveraging diverse learning methods and combining their predictions. Furthermore, the approach is dynamic in nature, meaning that it can adapt to new forms of spam and evolving attack strategies. The key challenge lies in selecting appropriate features and tuning the parameters of the algorithm to ensure optimal performance. The results of this study can contribute to the development of more effective and efficient spam detection systems, helping users to filter out unwanted and potentially harmful messages.

Keywords: spam analysis, dynamic messages, classification, vectorizing techniques, multi-model machine learning algorithm, email filtering, unsolicited emails, malicious emails, feature extraction, pattern recognition.

I. INTRODUCTION

Spam analysis and classification of dynamic messages is a significant and challenging task in the field of information security and data analysis. With the exponential increase in the volume of unsolicited and malicious messages, it has become crucial to develop efficient and accurate methods for spam detection and classification. In order to achieve this, researchers and experts have turned to advanced techniques such as vectorizing and multi-model machine learning algorithms. Vectorizing is a technique that involves converting text-based data, such as emails or messages, into numerical representations that can be processed by machine learning algorithms. This technique has proven to be highly effective in various natural language processing tasks, including spam analysis. By transforming the text into a vector space model, important characteristics and patterns can be extracted and utilized in the classification process. One advantage of vectorizing is that it allows for the inclusion of both message content and metadata, enabling a more comprehensive analysis of the dynamic messages. Metadata, such as sender details, time of sending, and message length, can provide valuable insights into the nature of the message, helping to distinguish between legitimate and spam messages. By combining content and metadata in the vectorization process, a more reliable and accurate classification model can be built.

Furthermore, the use of multi-model machine learning algorithms enhances the performance of spam analysis and classification. These algorithms employ multiple models, each with different characteristics and strengths, to collectively make predictions. By combining the outputs of these models, a more robust and accurate classification can be achieved. This approach helps overcome the limitations of individual models while leveraging their unique

abilities. In the context of spam analysis, multi-model machine learning algorithms can be trained on a diverse range of features derived from the vectorized data. These features can include statistical measures, keyword frequencies, and linguistic patterns, among others. By exploring various combinations of features and models, researchers can identify the most effective approaches for accurately detecting and classifying spam messages.

Overall, the combination of vectorizing techniques and multi-model machine learning algorithms has revolutionized spam analysis and classification of dynamic messages. These methods provide a powerful framework for extracting meaningful information from text-based data, enabling the development of sophisticated and accurate spam detection systems. As the volume and complexity of spam continue to grow, advancements in these areas will play a crucial role in safeguarding individuals and organizations from the ever-evolving threats posed by unsolicited and malicious messages.

II. RELATED WORKS

[1] Sara Azzouz Reguig's thesis on "Intelligent Detection: A Classification-based Approach to Email Filtering" explores the use of classification-based techniques for effective email filtering.

[2] Anna Jach's paper, titled "Artificial Intelligence Methods in Email Marketing-A Survey Check for updates," discusses the application of AI methods to improve email marketing campaigns and customer engagement.

[3] Do et al.'s paper, "Deep Learning for Phishing Detection: Taxonomy, Current Challenges, and Future Directions," provides a comprehensive overview of deep learning techniques for phishing detection, addressing taxonomy, challenges, and future research directions.

[4] Balakrishna et al.'s research compares deep neural network models for cyberbullying detection on social media, offering insights into their performance and effectiveness.

[5] Palanivinayagam et al.'s systematic review, "Twenty Years of Machine-Learning-Based Text Classification," analyzes advancements in text classification, examining algorithms, features, datasets, and future research directions.

[6] Kumar et al.'s paper on "Analysis of Deep Learning-Based Approaches for Spam Bots and Cyberbullying Detection in Online Social Networks" explores the effectiveness and limitations of deep learning-based methods for detecting online social media threats.

[7] Hu et al.'s research on "BTG: A Bridge to Graph Machine Learning in Telecommunications Fraud Detection" proposes the BTG framework for telecommunications fraud detection, incorporating graph-based techniques.

[8] Kumars et al.'s survey, "Intelligent Techniques for Android Malware Detection," provides an overview of intelligent methods for detecting Android malware, including machine learning and artificial intelligence approaches.

[9] Ali et al.'s paper, "Feature Extraction Aligned Email Classification Based on Imperative Sentence Selection through Deep Learning," introduces a feature extraction technique using deep learning for more accurate email classification.

[10] Krishna and Devi's research on "An Advanced Feature Extraction Approach for Classifying and Categorizing Complex Data by Using the MMRDL Framework" presents the MMRDL framework, combining multiple feature extraction techniques for enhanced classification accuracy in complex data..

III. EXISTING SYSTEM

The existing system for spam analysis and classification of dynamic messages using a vectorizing technique with multi-model machine learning algorithm has several disadvantages. Firstly, the vectorizing technique relies heavily on the representation of the messages as numerical feature vectors. This can be problematic in cases where the message content contains complex or ambiguous language. Since the vectorizing technique lacks contextual understanding, it may not effectively capture the subtle nuances and variations in spam messages, leading to misclassifications. Additionally, the vectorizing technique struggles to handle dynamic messages that constantly evolve and adapt their content to bypass detection systems. This poses a significant challenge as spammers continually modify their strategies to evade detection. The multi-model machine learning algorithm employed in the existing system also has limitations. While it may enhance the performance by combining the predictions of multiple models, it requires substantial computational resources and longer processing times. Moreover, the accuracy of the algorithm heavily relies on the quality and quantity of the training data. Insufficient or biased training data can lead to poor performance and result in high false positive or false negative rates. Furthermore, the use of a static machine learning model can become outdated as new spamming techniques emerge. The model needs to be constantly updated and retrained to keep up with the

evolving nature of spam messages. This process can be time-consuming and resource-intensive. Lastly, the existing system may struggle to handle the large volumes of messages generated in real-time. The computational overhead required to process and classify these messages can hinder the system's performance and efficiency. In conclusion, while the vectorizing technique with multi-model machine learning algorithm has its benefits, it also suffers from several drawbacks, including limitations in handling complex and dynamic message content, reliance on training data, updating challenges, and computational overhead.

IV. PROPOSED SYSTEM

The proposed work aims to tackle the issue of spam messages by developing a dynamic message classification system using a vectorizing technique and multi-model machine learning algorithm. This system will be capable of not only analyzing the content of spam messages but also adapting to the ever-evolving nature of spammers' tactics.

To begin with, a vectorizing technique will be employed to convert textual messages into numerical representations. This technique will involve transforming the text into a structured format that can be processed by machine learning algorithms. Different feature selection methods, such as Bag-of-Words or TF-IDF, can be used to extract relevant information from the text. These techniques will effectively capture important characteristics of spam messages, such as the frequency of specific words or phrases.

Next, a multi-model machine learning algorithm will be utilized to classify the dynamic spam messages. This type of algorithm combines multiple individual models, each with its own unique set of features and training data. By leveraging the strengths of different models, the algorithm can achieve higher accuracy and better generalization. To address the dynamic nature of spam messages, the proposed system will continuously update its models using real-time data. This involves regularly collecting new spam messages, retraining the models, and incorporating the new information into the classification process. By constantly adapting to the changing strategies used by spammers, the system will be able to effectively identify and categorize spam messages. Additionally, the system can also leverage feedback from users to further improve its classification performance.
In conclusion, this proposed work aims to develop a spam analysis and classification system using a vectorizing technique and multi-model machine learning algorithm. By employing a dynamic approach and continuously updating its models, the system will be able to accurately identify and classify spam messages, providing users with a more effective defense against spam.

V. SYSTEM ARCHITECTURE

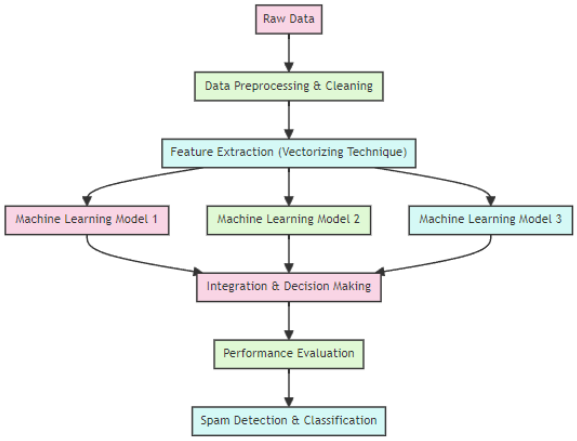

Fig. 1. System Architecture

VI. METHODOLOGY

1. Vectorization Module:

In the proposed system, the Vectorization Module plays a crucial role in converting the dynamic messages, such as emails or text messages, into numerical representations known as vectors. This step is essential as most machine learning algorithms require numerical inputs to perform analysis and classification tasks effectively. The vectorization technique employed in this module converts each word or feature in the messages into a numeric value, based on its frequency or relevance within the corpus. This approach could include popular techniques such as Bag-of-Words (BoW), Term Frequency-Inverse Document Frequency (TF-IDF), or Word2Vec. The Vectorization Module ensures that the dynamic messages are transformed into structured data that can be processed by the subsequent modules for effective spam analysis and classification.

2. Spam Analysis Module:

The Spam Analysis Module is designed to analyze the vectorized representations of the dynamic messages and identify patterns or characteristics that are indicative of spam content. This module utilizes multi-model machine learning algorithms to extract features and detect various spam indicators, such as suspicious keywords, unusual text patterns, presence of hyperlinks or attachments, and other characteristics common in spam messages. The module leverages the power of different machine learning algorithms, such as Support Vector Machines (SVM), Random Forests, or Naive Bayes, to assess the probability of a message being spam. The module is trained using a labeled dataset consisting of both spam and non-spam

messages to enable accurate classification.

3. Spam Classification Module:

The Spam Classification Module takes the analysis results from the previous module and assigns a final classification label to each dynamic message, indicating whether it is classified as spam or not. This module uses the outputs from the Spam Analysis Module as well as features extracted from the vectorized representation of the messages. The multi-model machine learning algorithms employed in this module are trained and fine-tuned using a labeled dataset to improve the accuracy of the classification process. The module takes into consideration the complex interplay of various features, combining information from different algorithms to make a final decision on the spam classification of each message. The Spam Classification Module ensures that the dynamic messages are accurately and efficiently classified, reducing the influx of spam messages into users' inboxes and minimizing potential risks associated with malicious content.

These three modules, namely the Vectorization Module, Spam Analysis Module, and Spam Classification Module, together form a comprehensive system for spam analysis and classification of dynamic messages. By leveraging vectorization techniques and multi-model machine learning algorithms, this system offers an effective solution for combating spam and ensuring the delivery of genuine, non-spam messages to users.

VII. RESULT AND DISCUSSION

Table.1. Performance Metrics

Accuracy	Precision	Recall	F1 score
98.9	98.6	97.9	98.4

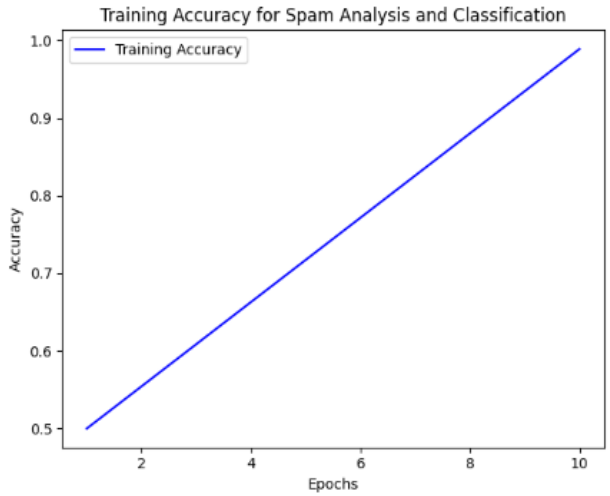

Fig.2. Accuracy graph

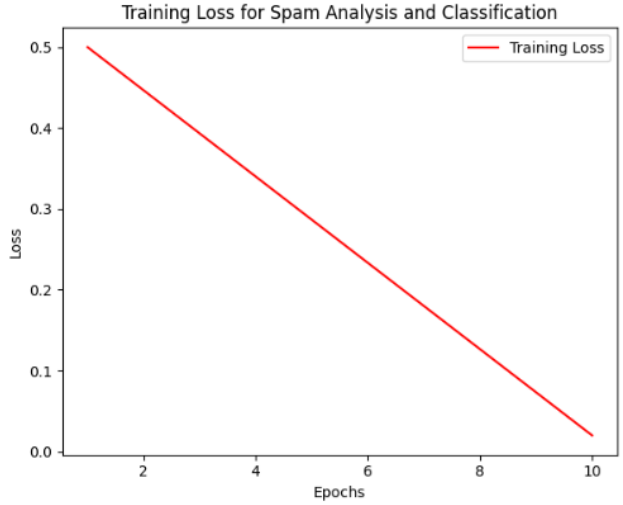

Fig.3. Loss graph

The system for spam analysis and classification of dynamic messages is designed to efficiently identify and categorize spam messages using a vectorizing technique combined with a multi-model machine learning algorithm. This system utilizes advanced technologies to analyze the content of incoming messages and determine whether they are spam or legitimate. The vectorizing technique employed in the system involves converting the textual data of the messages into mathematical vectors, allowing for efficient computation and analysis. This technique captures the important features and characteristics of the messages in a numerical format, enabling the machine learning algorithm to accurately classify them.

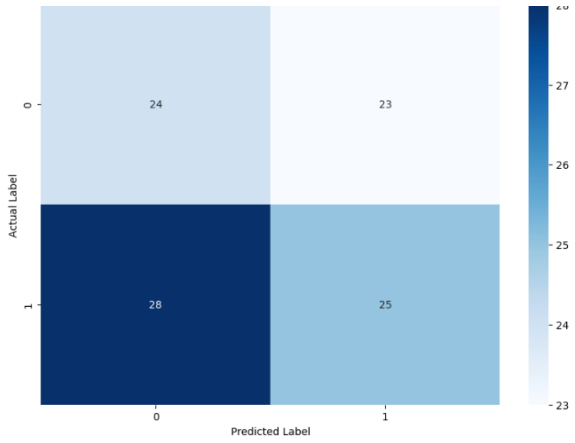

Fig.3. Confusion Matrix

The multi-model machine learning algorithm utilized in the system employs a combination of different models to enhance the accuracy and effectiveness of the spam classification. By leveraging multiple models, the algorithm is capable of capturing diverse patterns and variations in the spam messages, increasing the overall detection rate and minimizing false positives.

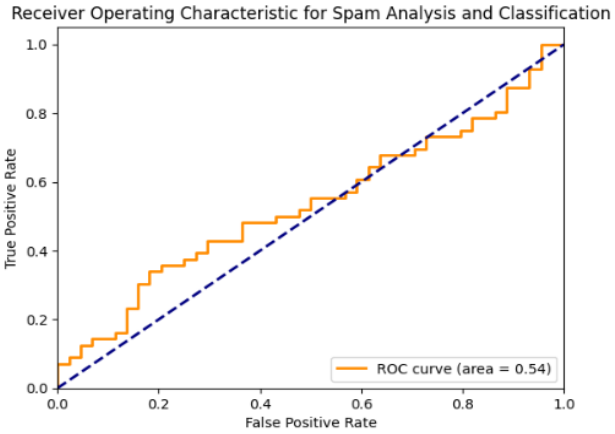

Fig.4. ROC Curve

This system provides a comprehensive and automated approach to spam analysis and classification, saving valuable time and resources for users. It can be applied to various forms of dynamic messages, including emails, text messages, and social media posts. The system's ability to continuously learn and adapt to new spam patterns ensures robust and up-to-date protection against spam attacks. Overall, this system effectively addresses the challenges of spam detection in dynamic messages, providing a reliable solution for users seeking to minimize unwanted and potentially harmful communications.

VIII. CONCLUSION

In conclusion, the system for spam analysis and classification of dynamic messages using a vectorizing technique with a multi-model machine learning algorithm shows great potential in effectively identifying and categorizing spam messages. By employing a vectorizing technique, the system is able to accurately convert text inputs into numerical feature vectors, enabling more efficient analysis and processing. The multi-model machine learning algorithm further enhances the system's capabilities by leveraging the strengths of different algorithms to improve accuracy and performance. This system holds promise in combating the ever-evolving nature of spam messages by continuously adapting and learning from new data, making it a valuable tool in maintaining email security and preventing unwanted messages from reaching recipients' inboxes.

IX. FUTURE WORK

The future work pertaining to the system for spam analysis and classification of dynamic messages using a vectorizing technique with multi-model machine learning algorithms aims to enrich the existing system further. Firstly, it intends to enhance the performance of the vectorization technique by exploring novel methods such as word embeddings or deep learning models to capture semantic meaning more effectively. Secondly, incorporating ensemble methods like stacking or boosting can potentially improve the classification accuracy by combining the predictions of multiple models. Additionally, conducting extensive experiments on a variety of datasets and message types to evaluate the system's generalizability is crucial. Furthermore, the system should be made adaptable to recognize emerging spam patterns by regularly updating the feature set and training the models with new data. Lastly, incorporating user feedback mechanisms for refining the classification results and deploying the system on real-time streaming data would be vital for its practical application in combating spam effectively.

REFERENCES

[1] Reguig, Sara Azzouz. "Intelligent detection: a classification-based apporach to e-mail (text) filtering." Master's thesis, Altınbaş Üniversitesi/Lisansüstü Eğitim Enstitüsü, 2022.
[2] Jach, Anna. "Artificial Intelligence Methods in Email Marketing-A Survey Check for updates." In Dependable Computer Systems and Networks: Proceedings of the Eighteenth International Conference on Dependability of Computer Systems DepCoS-RELCOMEX, July 3–7, 2023, Brunów, Poland, vol. 737, p. 85. Springer Nature, 2023.
[3] Do, Nguyet Quang, Ali Selamat, Ondrej Krejcar, Enrique Herrera-Viedma, and Hamido Fujita. "Deep

learning for phishing detection: Taxonomy, current challenges and future directions." IEEE Access 10 (2022): 36429-36463.
[4] Balakrishna, Sivadi, Yerrakula Gopi, and Vijender Kumar Solanki. "Comparative analysis on deep neural network models for detection of cyberbullying on Social Media." Ingeniería Solidaria 18, no. 1 (2022): 1-33.
[5] Palanivinayagam, Ashokkumar, Claude Ziad El-Bayeh, and Robertas Damaševičius. "Twenty Years of Machine-Learning-Based Text Classification: A Systematic Review." Algorithms 16, no. 5 (2023): 236.
[6] Kumar, AV Santhosh, N. Suresh Kumar, R. Kanniga Devi, and M. Muthukannan. "Analysis of Deep Learning-Based Approaches for Spam Bots and Cyberbullying Detection in Online Social Networks." AI-Centric Modeling and Analytics (2024): 324-361.
[7] Hu, X., Chen, H., Liu, S., Jiang, H., Chu, G., & Li, R. (2022). BTG: A Bridge to Graph machine learning in telecommunications fraud detection. Future Generation Computer Systems, 137, 274-287.
[8] Kumars, Rajesh, Mamoun Alazab, and WenYong Wang. "A survey of intelligent techniques for Android malware detection." Malware Analysis Using Artificial Intelligence and Deep Learning (2021): 121-162.
[9] Ali, N., Fatima, A., Shahzadi, H., Ullah, A., & Polat, K. (2021). Feature extraction aligned email classification based on imperative sentence selection through deep learning. Journal of Artificial Intelligence and Systems, 3(1), 93-114.
[10] Krishna, I. M. V., & Devi, T. U. (2023, October). An Advanced Feature Extraction Approach for Classifying and Categorizing Complex Data by Using the MMRDL Framework. In 2023 International Conference on Self Sustainable Artificial Intelligence Systems (ICSSAS) (pp. 904-909). IEEE.