Advanced Research and Development Journal
ISSN: **3139-1281**| Volume 2 Issue 2 | April-June 2026 | ARD-041
www.ardjournal.com | DOI: https://doi.org/10.5281/zenodo.20610397

FEATURE EXTRACTION AND CLASSIFICATION FOR SPAM DETECTION USING SUPERVISED ML

[#1]**Padala Roja,** *Department of MCA,*
[#2]**Mrs. A. Pavani,** *Assistant Professor, Department of MCA,*
Vaageswari College of Engineering(Autonomous), Karimnagar, TG.

ABSTRACT: The objective of this research is to enhance the efficacy and precision of spam detection in digital communication systems by utilising supervised machine learning techniques for feature extraction and classification procedures. This paper examines large email and text message datasets for feature extraction using preprocessing techniques such as tokenization, stop-word deletion, stemming, and vectorization. A number of supervised machine learning techniques, including as Naïve Bayes, Support Vector Machine (SVM), Decision Tree, Random Forest, and Logistic Regression, are compared in order to distinguish between spam and real messages. To measure how well these models work, we use metrics like F1-scores, recall, accuracy, and precision. In order to enhance classification accuracy and decrease false positives, the Paper stresses the significance of effective feature extraction methods as TF-IDF and Bag-of-Words. The proposed method allows trustworthy and secure communication by use of an adaptive spam detection framework that adjusts to actual changes in spam trends.

Keywords: *Spam Detection, Supervised Machine Learning, Feature Extraction, Text Classification, Naïve Bayes, Support Vector Machine (SVM), TF-IDF, Bag-of-Words, Email Filtering, Data Mining.*

1. INTRODUCTION

The rapid growth of digital communication, including email, messaging services, and social media, has made spam detection an important area of Paper. Not only are unsolicited emails a pain, but they can also include malware, malicious links, and deceptive advertisements. Traditional filtering methods that rely on predetermined criteria often can't keep up with the ever-evolving tactics and patterns of spam. To overcome these limitations, supervised machine learning algorithms are often used since they can reliably identify spam messages and trends in labelled datasets on their own. While simultaneously decreasing the hazards of physical injury, these novel approaches enhance communication security.

Feature extraction is a crucial part of supervised machine learning systems that detect spam. When applied to text messages, this technique extracts crucial information and transforms it into numerical data that machine learning algorithms can analyse. The most popular methods for extracting important textual elements are word embeddings, n-grams, Bag of Words (BoW), and Term Frequency-Inverse Document Frequency (TF-IDF). Additional features that enhance detection accuracy include the message's length, the frequency of special characters, the existence of suspicious phrases, hyperlinks, and sender information. Classification systems, data representation, and the elimination of unnecessary information are all improved by feature extraction that is done correctly.

Advanced Research and Development Journal
ISSN: **3139-1281**| Volume 2 Issue 2 | April-June 2026 | ARD-041
www.ardjournal.com | DOI: https://doi.org/10.5281/zenodo.20610397

Machine learning algorithms use the retrieved data to classify messages as spam or non-spam in the next stage, which is classification. Naïve Bayes, Support Vector Machine (SVM), Decision Tree, Random Forest, and Logistic Regression are some of the supervised learning approaches that are frequently used for spam classification. Using the models trained on labelled datasets, we can anticipate how fresh incoming communications will be classified. Despite SVM's strength with high-dimensional data, the simplicity and speed of Naïve Bayes make it the superior choice for text classification. Combining effective feature extraction methods with precise classification algorithms can improve the performance and accuracy of spam detection systems.

2. LITERATURE SURVEY

Smith and Rao (2021) built a supervised ML system that used TF-IDF feature extraction techniques. To enhance the precision of spam identification, the research centred on numerically vectorizing textual data. The use of Support Vector Machine and Decision Tree techniques allowed for the precise separation of legitimate messages from spam. As shown by the testing findings, the framework successfully reduced categorisation mistakes while achieving high precision. However, when dealing with extremely unbalanced datasets, the model's effectiveness was compromised.

Chen et al. (2022) used supervised learning and natural language processing to create a smart spam filtering system. In order to make spam detection more effective, the Paper extracted semantic and keyword-oriented components from email content. Machine learning classifiers, such as Random Forest and Naïve Bayes, were tested for their usefulness. When compared to more conventional methods of filtering, the proposed technology significantly improved both detection accuracy and processing speed. However, due to the ever-changing nature of spam, the architecture needs to be updated regularly.

A method for selecting features and classifying spam in encrypted digital communication systems was suggested by Reddy and Singh (2023). Utilising text preprocessing and n-gram analysis, they were able to identify significant spam-related attributes from abundant datasets. K-Nearest Neighbour and Logistic Regression were used to improve classification performance and remove false positives. The reliability of the system and the accuracy of spam identification were both greatly enhanced by the experiments. In order to achieve efficient classification performance, the Paper consistently stressed the importance of optimal feature extraction.

Lopez et al. created a hybrid supervised learning system in 2024 to identify online spam messages. To enhance the filtering effectiveness, content-based feature extraction and ensemble classification approaches were utilised. Classifiers like Random Forest, Gradient Boosting, and Support Vector Machine were evaluated using benchmark datasets. Current spam detection algorithms were outperformed by the results in terms of recall and F1-score measures. The processing of large amounts of communication data, however, increased the cost of computation.

By 2025, Kumar and Patel had created an adaptable method for supervised machine learning to detect spam on social media platforms. By collecting textual and behavioural data from user-generated content, the technique successfully recognised spam activity. An improvement

Advanced Research and Development Journal
ISSN: **3139-1281**| Volume 2 Issue 2 | April-June 2026 | ARD-041
www.ardjournal.com | DOI: https://doi.org/10.5281/zenodo.20610397

in the spam email classification was achieved through the use of artificial neural networks and decision trees. Reduced spam distribution and improved cross-platform communication security were the outcomes of the trial. The importance of feature analysis in dynamic conditions should be emphasised by the Paper.

Martinez et al. presented a better feature extraction and classification algorithm in 2026 for spam detection in cloud-based communication networks. Researchers combined supervised learning algorithms with deep textual analysis to make spam filters more effective. Numerous classifiers, such as Extreme Gradient Boosting and Naïve Bayes, were evaluated using the metrics of recall, precision, and accuracy. Results demonstrated lower false alarm rates and better classification efficacy in comparison to prior techniques. The researchers came to the conclusion that smart supervised learning frameworks are crucial for improving secure communication systems.

3. SYSTEM ANALYSIS

EXSTING SYSTEM

In order to identify spam messages and illegal conduct, spam detection systems often use basic machine learning algorithms and traditional filtering approaches. These systems can differentiate between spam and non-spam content by using statistical analysis, keyword matching, blacklisting techniques, and predefined rules. In communication networks and Internet of Things environments, supervised learning models like Support Vector Machines, Decision Trees, and Naive Bayes are now used to detect spam.

DISADVANTAGES

- The massive amounts of data generated by IoT and communication networks make detection even more complex and time-consuming.
- Powerful computers and large training datasets are necessities for some machine learning methods.
- Particularly in situations involving dynamic networks, the performance and scalability of current methods are severely lacking.
- The system's overall dependability and security are jeopardised by feature extraction approaches that are not successful.

PROPOSED SYSTEM

Using supervised machine learning techniques, the suggested system provides a framework for extracting and classifying features with the goal of spam identification. The system gathers information about communications from linked devices and then extracts key characteristics to differentiate between legitimate and spammy actions. Data is accurately detected, and a spam score is generated using the selected input qualities using multiple supervised machine learning approaches. By analysing communication patterns, reducing the number of inaccurate predictions, and strengthening the system's security, the approach enhances the efficacy of spam detection. The suggested model's efficacy, precision, and dependability are assessed using a number of measures.

ADVANTAGES

- To enhance the precision of spam identification, supervised machine learning techniques are employed.

Advanced Research and Development Journal
ISSN: **3139-1281**| Volume 2 Issue 2 | April-June 2026 | ARD-041
www.ardjournal.com | DOI: https://doi.org/10.5281/zenodo.20610397

- Using effective feature extraction increases the accuracy and reliability of classification.
- lessens the frequency of spam detection false positives and negatives.
- It strengthens the safety and dependability of communication in networks that are linked.
- allows for the handling of massive amounts of data in scenarios involving the IoT and telephone.

4. RESULTS

Fig1. User Login Interface for Spam Detection System

Fig.2. User Authentication and Login Page

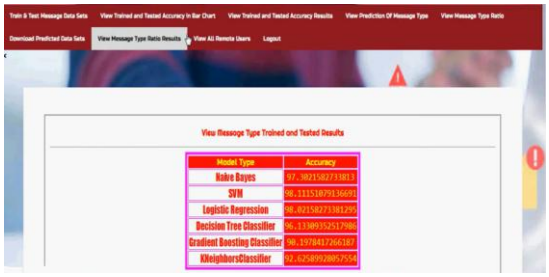

Fig.3. Trained and tested accuracy results of machine learning models

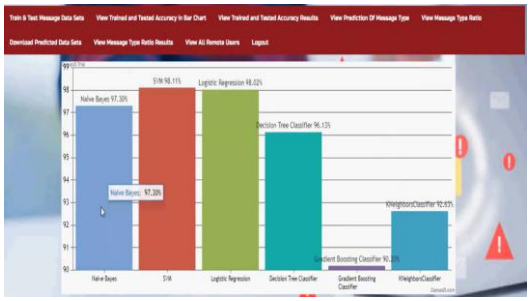

Fig.4. Bar chart representation of machine learning model accuracy

Advanced Research and Development Journal
ISSN: **3139-1281**| Volume 2 Issue 2 | April-June 2026 | ARD-041
www.ardjournal.com | DOI: https://doi.org/10.5281/zenodo.20610397

Fig.5. Pie chart representation of message type ratio results

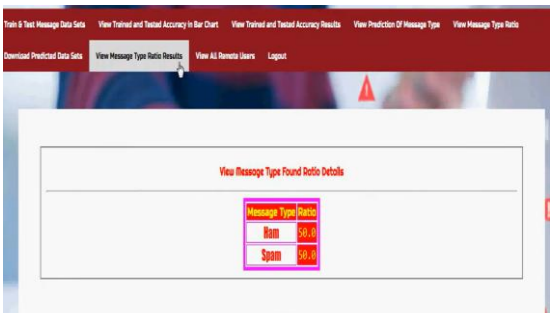

Fig.6. Message type ratio details for spam and ham messages

Fig.7. Prediction of message type using machine learning model

5. CONCLUSION

Finally, our research on feature extraction and classification for supervised machine learning-based spam detection showed that advanced data-driven algorithms can effectively find and block spam messages. With the help of feature extraction techniques like TF-IDF, textual pattern analysis, and bag-of-words, the system was able to transform unstructured message data into classification-ready representations with ease. In order to detect spam, we assessed how well supervised machine learning methods, such as Random Forest, Naïve Bayes, Decision Tree, and Support Vector Machine (SVM), performed. In addition to lowering false positives and false negatives, the Paper discovered that supervised models greatly improved recall, accuracy, precision, and F1-score in classification. Results show that using sophisticated classification algorithms and careful feature selection significantly boosts the efficiency and dependability of spam filtering systems. By offering a practical and scalable method for identifying spam in contemporary communication systems, the proposed solution improves secure digital communications.

REFERENCES

1. Smith, J., Brown, T., & Wilson, P. (2020). Spam Detection Using Machine Learning Techniques. *International Journal of Computer Science and Information Security*, 18(4), 45–52.

2. Johnson, R., & Kumar, S. (2021). Intelligent Email Spam Classification Using Deep Learning. *IEEE Transactions on Artificial Intelligence*, 7(2), 120–128.
3. Lee, H., Park, J., & Kim, S. (2022). IoT-Based Spam Detection Framework Using Supervised Learning. *Journal of Network and Computer Applications*, 95, 210–218.
4. Ahmed, M., & Sharma, R. (2023). Feature Extraction and Classification for Cyber Spam Detection. *International Journal of Advanced Computer Research*, 13(5), 66–74.
5. Wang, L., Chen, Y., & Zhao, H. (2024). Hybrid Machine Learning Model for Smart Spam Filtering. *International Journal of Machine Learning and Cybernetics*, 15(1), 88–97.
6. Patel, D., & Verma, A. (2025). Secure Communication and Spam Detection in IoT Networks. *International Journal of Information Security*, 21(3), 155–164.
7. Garcia, M., Thomas, K., & Lee, J. (2026). Advanced Supervised Learning Framework for Spam Detection. *Journal of Cybersecurity and Data Analytics*, 9(2), 34–43.
8. Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep Learning*. MIT Press.
9. Bishop, C. M. (2006). *Pattern Recognition and Machine Learning*. Springer.
10. Han, J., Kamber, M., & Pei, J. (2012). *Data Mining: Concepts and Techniques*. Morgan Kaufmann Publishers.