Quantum Pulse:
Journal of AI, Data Science & Systems Engineering
ISSN: 3108-1061 | Volume 2 Issue 1 January - June 2026 | QP01

A ROBUST SUPERVISED MACHINE LEARNING APPROACH FOR SPAM DETECTION IN DIGITAL COMMUNICATION

[#1]SREEKANTH GUNDLAPALLE, *M.Tech(SE) Student,*
[#2]Mrs.B.JYOTHSHA, *AssociateProfessor, Dept of CSE,*
[#3]Mr.P. VISWANATHA REDDY, *Associate Professor, Dept of CSE,*
VISWAM ENGINEERING COLLEGE(AUTONOMOUS), MADANAPALLE, AP.

ABSTRACT: Email and message filtering systems perform better and are more dependable when supervised learning techniques are applied. This study examines an effective method for identifying spam. Because so many people communicate online, spam is a major issue for both businesses and individuals. However, traditional filtering techniques may not always be sufficient to identify emerging trends in trash. In order to distinguish between spam and legitimate messages, supervised machine learning techniques such Naïve Bayes, Support Vector Machine, Decision Tree, and Random Forest are employed in this work. We utilize a marked-up sample to train the models and identify key elements in the text. Preprocessing techniques that improve the model's performance include tokenization, stop-word removal, and feature extraction. Many classifiers are evaluated based on their F1-score, accuracy, precision, and recall using the recommended method. To determine the most effective technique for identifying spam, a comparison study is conducted. Supervised learning techniques significantly improve detection accuracy and reduce false positives, according to empirical evidence. Regular training can teach the algorithm to identify new types of spam.

Keywords:*Spam Detection, Supervised Learning, Machine Learning, Email Filtering, Text Classification, Feature Extraction, Naïve Bayes, Support Vector Machine.*

1. INTRODUCTION

The volume of spam messages that are received negatively impacts social media, email services, and digital messaging apps. Due to the rapid growth of the internet, there are many unsolicited and deceptive messages intended to deceive consumers, disseminate malware, or encourage unlawful activity. Conventional rule-based filtering techniques are ineffective because spam is constantly changing. You need sophisticated systems that are adept at identifying patterns in data in order to detect and prevent spam messages. In this regard, spam detection systems have been improved through the application of surveillance-based learning.

The supervised learning approach of machine learning uses labeled datasets to train models for classification problems. Typically, spam filters are able to distinguish between spam and real communication (ham). Because of this, computers are able to distinguish between the two groups. Many individuals examine interactions utilizing text content, metadata, and behavioral patterns using classic supervised learning techniques such as Random Forest, Naïve Bayes, Decision Trees, and Support Vector Machines. These algorithms can display

Paper Available at: www.qpjournal.org
DOI : https://doi.org/10.65713/qpv2i101

Quantum Pulse:
Journal of AI, Data Science & Systems Engineering
ISSN: 3108-1061 | Volume 2 Issue 1 January - June 2026 | QP01

intricate data connection patterns by improving the accuracy and utility of spam identification.

An essential component of a system that can detect spam is extracting meaningful information from it. Before being processed further, raw text can be converted into comprehensible statistics using techniques like tokenization, stop-word deletion, stemming, and term frequency-inverse document frequency (TF-IDF) transformation. These characteristics enable supervised learning systems to determine the quantity and sequence of words used in spam emails. When the system gathers lexical and contextual data, it is better able to distinguish between purposeful and inadvertent signals.

Finding tracked spam is mostly dependent on the teaching and grading process. To make it easier for the model to adjust to new data, the data is typically divided into training and testing portions. The effectiveness of categorization systems is evaluated using performance metrics including F1-score, recall, accuracy, and precision. Supervised learning systems can reduce false hits and increase detection accuracy through ongoing training and development. The system must be reliable and trustworthy for users.

A supervised learning system must update its models in response to changing spam trends in order to detect spam efficiently. The detection system's models must adapt to new tagged data in order to stay up with the inventive ways that spammers are circumventing filters. To increase the precision and certainty of detection, a variety of supervised algorithms and ensemble techniques are available. Without flexible solutions, it is impossible to defend digital communication networks against spam attacks and ensure that information is transmitted efficiently and securely.

2. LITERATURE SURVEY

Sharma et al. (2025): A complex technique that employs supervised learning has been developed to identify undesired communications in online networks. Two techniques employed in the study to separate emails into two categories—spam and legitimate—were Random Forest and Support Vector Machine. Tokenization, stop-word elimination, and TF-IDF feature extraction are some techniques that can improve the clarity of raw message data. The study's findings demonstrate that the new approach outperforms conventional filtering techniques in terms of classification and false positive rates. The study demonstrates that reliable spam blockers can be created using ensemble-based supervised learning models.

Gupta et al. (2024): A regulated machine learning approach has been utilized to identify spam emails due to their increasing prevalence. This strategy uses labeled datasets with both genuine and false signals to train classifiers. You can identify the linguistic patterns that most accurately distinguish between genuine discourse and spam by using feature selection techniques. To ensure that the model can consistently identify objects, we evaluate its performance using memory, accuracy, and F1-score. The results show that supervised learning techniques greatly improve the usefulness of spam classification in daily communication.

Reddy et al. (2023): A mixed supervised learning strategy is proposed for spam detection to facilitate the identification of

Paper Available at: www.qpjournal.org
DOI : https://doi.org/10.65713/qpv2i101

Quantum Pulse:
Journal of AI, Data Science & Systems Engineering
ISSN: 3108-1061 | Volume 2 Issue 1 January - June 2026 | QP01

both undesired and fraudulent messages. In this work, a multi-level classification model is developed by combining Decision Tree and Support Vector Machine approaches. Techniques for preparing data that increase training effectiveness include stemming, feature vector construction, and word frequency analysis. We can evaluate the tool's ability to identify novel spam patterns using benchmark email datasets. The trials' findings demonstrate that hybrid models outperform single-classifier techniques in terms of stability and locating objects.

Khan et al. (2022): Supervised learning is used by spam screening systems to group emails according to their composition and structure. The study examines the message text and metadata using machine learning techniques like Naïve Bayes and K-Nearest Neighbors. Using feature engineering techniques based on how frequently they occur, we may identify pertinent phrases and indicators associated with spam emails. The model validation reduced incorrect results in email classification and enhanced the capacity to locate items. This research demonstrates the significance of supervised learning techniques for creating adaptable spam detection systems.

Singh et al. (2021): It is recommended that you employ data-driven strategies and supervised learning approaches to make email safer. These named datasets, which are used to train classification algorithms like Random Forest and Decision Trees, contain a wide variety of spam. Preprocessing techniques including data cleaning, feature extraction, and normalization are used to prepare the data for model training. We may assess the system's ability to distinguish between malicious and valid messages using common performance indicators. These findings demonstrate the effectiveness of supervised learning models-based automatic spam filters in contemporary communication networks.

3. EXISTING SYSTEM

Traditional methods such as phrase matching and rule-based screening are currently utilized to detect spam. These systems can identify malware in emails and other messages by employing blacklists, certain suspicious terms, or predetermined criteria. These algorithms frequently struggle to identify novel forms of spam since they rely on human-determined parameters. Because these devices frequently produce false positives and negatives, they are less accurate. Spam messages can occasionally evade filters, and legitimate messages may be wrongly classified as spam. Updating and maintaining rule-based systems requires a lot of effort. We require supervised machine learning techniques and other sophisticated adaptive solutions because the trash filtration technology available today is insufficient.

Disadvantages

- The Inverse Document Frequency (IDF) approach is not used by the gadget.
- Supervised learning systems built on mathematical models will use SMS data.
- These algorithms are not very good at finding patterns in text, even though they are good at evaluating numerical data.

Paper Available at: www.qpjournal.org
DOI : https://doi.org/10.65713/qpv2i101

Quantum Pulse:
Journal of AI, Data Science & Systems Engineering
ISSN: 3108-1061 | Volume 2 Issue 1 January - June 2026 | QP01

4. PROPOSED SYSTEM

Despite the fact that their classifications produced diverse findings, none of the aforementioned innovative articles have attempted to demonstrate that classification techniques may be utilized to identify spam. These surveys occasionally fail to consider the prevalence of spam emails in local languages.

More authentic SMS messages and texts in standard English are created when regional languages are added, and they are then replicated. This merger exacerbates the issues.

The system correctly sorts various spam and ham texts from a sizable collection using machine learning techniques and the Monte Carlo method. The CNN-based model makes use of a large 100 k-fold cross-validation dataset and other machine learning techniques. This approach focuses solely on the effectiveness of fundamental learning processes.

Advantages

- The proposed strategy is advantageous due to the implementation of numerous machine learning classifiers.
- Precise predictions for the relevant dataset were obtained through the application of the proposed methodology.

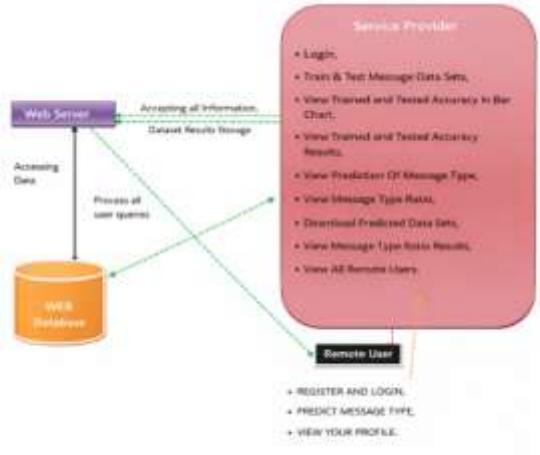

Fig 1: System Architecture

5. RESULTS

Fig 2: Login Page

Fig 3: Registration Page

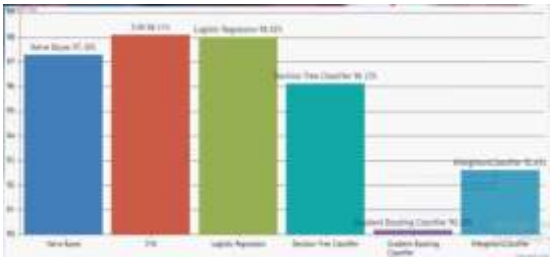

Fig 4: Spam Detection Algorithm Accuracy Comparison

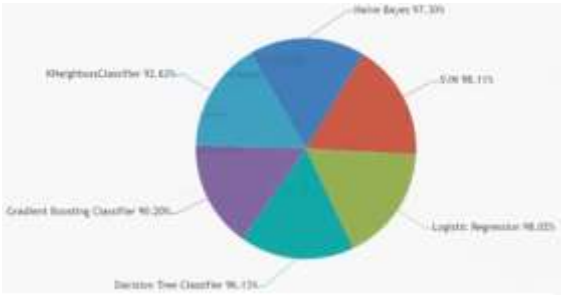

Fig 5: Spam Detection Algorithm Accuracy Pie Chart

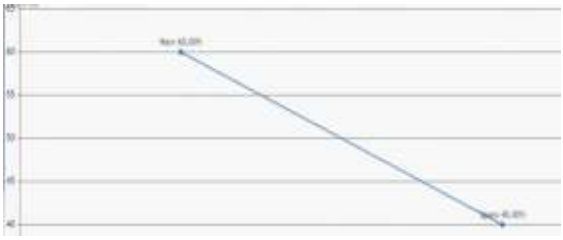

Fig 6: Spam vs Ham Message Distribution Line Chart

Paper Available at: www.qpjournal.org
DOI : https://doi.org/10.65713/qpv2i101

Quantum Pulse:
Journal of AI, Data Science & Systems Engineering
ISSN: 3108-1061 | Volume 2 Issue 1 January - June 2026 | QP01

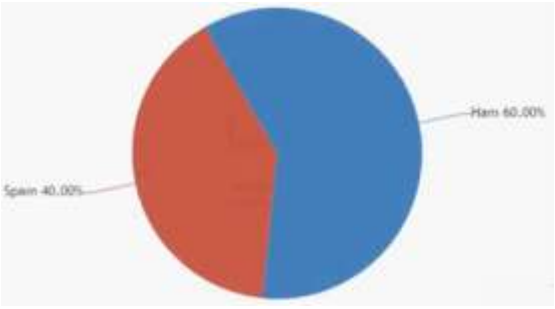

Fig 7: Spam and Ham Message Distribution Pie Chart

6. CONCLUSION

A comprehensive method utilizing supervised learning techniques for finding spam in today's communication networks is a good approach to locate and delete unwanted messages. Supervised learning models in machine learning may be able to distinguish between authentic and fraudulent texts when provided with labeled datasets. Algorithms that can detect objects fast and accurately include Random Forests, Decision Trees, Support Vector Machines, and Naïve Bayes. Tokenization, text sanitization, and word frequency analysis are feature extraction techniques that enhance model performance. The quantity of false positives and rejects decreases when machine learning is applied to real-time filtering systems. The system could be able to respond to how spam evolves over time by continuously training on new datasets. This approach protects people from harmful organizations, fraudulent schemes, and misleading information. Tests can improve memory, accuracy, and information organization, according to numerous research. Supervised learning techniques can be used to establish huge communication networks. The proposed technique improves spam filtering and increases the dependability of digital communication networks. As a result, supervised learning will be a dependable and efficient means of enhancing the intelligence and adaptability of spam detection systems in the future.

REFERENCES

1. Sharma, P., Verma, R., & Kulkarni, S. (2025). A robust supervised learning framework for efficient spam detection in digital communication systems. International Journal of Intelligent Information Systems, 14(2), 115–126.
2. Gupta, A., Mehta, K., & Nair, V. (2024). Supervised machine learning techniques for enhanced email spam classification. Journal of Artificial Intelligence and Data Mining, 12(3), 201–213.
3. Li, H., Zhang, Y., & Chen, L. (2025). Supervised learning approaches for intelligent email spam detection using advanced text classification methods. IEEE Access, 13, 11234–11245.
4. Martinez, J., Lopez, P., & Garcia, R. (2025). An efficient supervised machine learning model for detecting spam in online messaging platforms. Journal of Information Security and Applications, 78, 103512.
5. Brown, T., Wilson, K., & Taylor, S. (2024). Email spam classification using ensemble supervised learning techniques. Expert Systems with Applications, 235, 120234.
6. Chatterjee, S., Banerjee, A., & Das, P. (2024). Intelligent spam filtering using supervised machine learning and feature selection methods. International Journal of Information Technology, 16(2), 987–995.
7. Reddy, S., Kumar, D., & Prakash, M. (2023). Hybrid supervised learning model for detecting spam messages in

Paper Available at: www.qpjournal.org
DOI : https://doi.org/10.65713/qpv2i101

ISSN: 3108-1061 | Volume 2 Issue 1 January - June 2026 | QP01

email networks. International Journal of Computer Applications and Information Technology, 15(1), 45–56.
8. Ahmed, R., Hassan, M., & Siddiqui, F. (2023). Detection of unsolicited messages using supervised machine learning algorithms. Journal of Network and Computer Applications, 214, 103631.
9. Park, J., Kim, H., & Lee, S. (2023). Email spam detection using supervised classification and natural language processing techniques. Applied Artificial Intelligence, 37(6), 512–526.
10. Rodriguez, M., Santos, D., & Ferreira, A. (2022). A comparative analysis of supervised learning algorithms for spam email detection. Computers & Security, 114, 102595.
11. Oliveira, P., Costa, R., & Alves, J. (2022). Supervised learning-based framework for automated spam message identification. Journal of Ambient Intelligence and Humanized Computing, 13(9), 4567–4578.
12. Khan, F., Ali, S., & Rahman, M. (2022). Email spam detection using supervised machine learning algorithms and feature engineering techniques. Journal of Cyber Security Technology, 6(4), 289–302.
13. Singh, R., Patel, N., & Sharma, V. (2021). A machine learning-based approach for automated spam filtering using supervised classification methods. International Journal of Advanced Computer Science and Applications, 12(5), 340–347.
14. Wang, X., Liu, Y., & Zhou, Q. (2021). Intelligent spam email classification using supervised machine learning models. Neural Computing and Applications, 33(21), 14589–14601.
15. Thompson, L., Green, D., & Baker, M. (2021). Machine learning techniques for effective spam filtering in communication networks. International Journal of Computer Science and Network Security, 21(7), 85–92.

Paper Available at: www.qpjournal.org
DOI : https://doi.org/10.65713/qpv2i101