IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.021 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 6, June 2026

DOI: 10.17148/IJIREEICE.2026.14617

AI BASED SPAM TEXT DETECTOR

MANJUPRIYA.A[1], Mr. P. LOGAIYAN[2]

P.G Student, Department of Master Computer Application,

Sri Manakula Vinayagar Engineering College, Pondicherry-605 107[1]

Associate Professor, Department of Master Computer Application,

Sri Manakula Vinayagar Engineering College, Pondicherry-605 107[2]

Abstract: The idea of Artificial Intelligence belongs to Computer Science. The idea here is to develop machines which can perform tasks done by humans. I intend to discuss Artificial Intelligence. The technology has been adopted by many industries including health care and education. Artificial Intelligence is really useful, in these areas. Artificial Intelligence is also used in finance and cyber security. Artificial Intelligence is really useful, in places. Spamming has increased tremendously through the usage of such means. The content of spam consists of malicious ads, fake links, phishing, and misleading information. It could lead to many problems for an individual as well as for the organization. Most of the conventional techniques used in detecting spam content have proven themselves inefficient in identifying complex patterns of spam. Therefore, it is proposed to use AI-Based Spam Text Detection System for the identification and classification of spam as well as non-spam texts by using machine learning and Natural Language Processing. Machine learning techniques are trained using big datasets consisting of both types of messages to ensure greater accuracy in prediction. Due to the usage of technology in NLP, it gets extremely easy for the computer to interpret the meaning that is concealed within the messages.

Keywords: Artificial Intelligence, Spam Filter Technique, Machine Learning, Natural Language Processing, Text Categorization, Computer Security.

INTRODUCTION

Definition

ARTIFICIAL INTELLIGENCE is one branch among many branches of Computer Science. In simple terms, this means the creation of machines that can think in the way that human beings do. Artificial intelligence has various applications, including medicine and education. Artificial Intelligence is also used in finance and cyber security. There are other areas where Artificial Intelligence is used. Artificial Intelligence is really changing how things are done in these areas. Spam text detection is one of the areas where artificial intelligence technology has been applied. Spam texts refer to unwanted or malicious messages. Such messages could consist of advertisements, fake deals, phishing websites, malware, or misleading information. Spam messages are not only wastage of users' valuable time, but they also present considerable security threats. Spam filters used traditionally rely heavily upon pre-defined rules and keyword matching technologies, both of which are not very effective against spam. This AI-Based Spam Text Detector is intended to automatically detect whether or not a message belongs to a category of spam messages or not. It relies upon machine learning algorithms which can help recognize the pattern of spams through past available data sets NLP techniques are used for processing and analysis of the text-based data.

PROBLEM STATEMENT

Traditional anti-spam software works on the basis of manual filtering procedures and fixed keyword criteria. Such an approach fails to effectively detect spam messages since they keep changing their characteristics. A significant number of such spam messages employ misleading phrases, symbols, and shortened links to bypass filters. A constant update of filters, along with monitoring activities, complicates maintenance tasks. Traditional systems may also trigger errors by tagging legitimate messages as spam. Moreover, processing a high volume of spam messages through traditional systems poses serious problems. There is a clear necessity to develop an intelligent and automated spam detector. It is essential to build a system that would operate effectively without any need for human intervention. It should be noted that there is a need for higher detection accuracy and efficiency. Hence a system that uses intelligence is built to find spam messages. It uses Machine Learning and Natural Language Processing technologies. The system detects spam messages. It uses Machine Learning. It uses NLP technologies.

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.021 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 6, June 2026

DOI: 10.17148/IJIREEICE.2026.14617

OBJECTIVES

The primary objective of the study is to develop a system called Spam Text Detector using artificial intelligence. This system will assist in classifying text messages into two categories; either spam or non-spam text messages. This system tries to minimize efforts spent on message classification and provides more secure communication. The goals of this system are as follows:

- To process text messages.
- To use Machine Learning techniques to classify spam messages.
- To utilize Natural Language Processing techniques.
- To achieve high accuracy rates of spam detection.
- To minimize the number of false results.
- To perform real-time spam message prediction.
- To provide cybersecurity solutions.

SCOPE OF THE SYSTEM

The AI-Based Spam Text Detector could be used on many other channels of communication, including emails, SMS text messages, social networking sites, and online messaging services. This system can automatically detect spam text in real time. It can handle big datasets and process many messages at a time. This system could also be embedded in web-based and mobile applications The main purpose of this study is to build a Spam Text Detector system based on Artificial Intelligence that will classify text messages into two types – spam and non-spam messages. This will allow companies to avoid phishing attacks and spam messages that can potentially ruin their reputation and do harm to the business. Some additional features that might be included later include multilingual spam detection, voice message detection, and application of deep learning algorithms.

LITERATURE REVIEW

The growing trend of digital communications is resulting in researchers conducting research related to intelligent spam detection mechanisms. Machine Learning and NLP algorithms have been used extensively in improving accuracy in spam classification processes. Blacklist filtering and keyword matching were some of the traditional approaches used for spam filtering. However, these traditional methods did not work for current spam messages. The researchers proposed using Machine Learning algorithms including Naïve Bayes, SVM, Decision Tree, and Random Forest algorithms for spam classification. Machine learning algorithms can classify spams based on their features learned from the training datasets. The natural language processing techniques are applied to process text data. It involves techniques including removal of stop words, tokenization, and semantic analysis of sentences. Current trends involve the use of advanced machine learning approaches such as RNN and LSTM.

METHODS OF ARTIFICIAL INTELLIGENCE APPLIED

Machine Learning

Machine learning is really useful because it lets the system learn from the messages it has seen before. This means the system can look at spam and non-spam messages and get better at figuring out what is what. The machine learning algorithms are taught using a set of messages that are labeled as spam or not spam. Then when a new message comes in the system can use what it has learned to say whether the message is spam or okay to read. The process improves the capabilities of the system in detecting spam.

Natural Language Processing (NLP)

The process acts as an enabler since it helps the system to comprehend the natural language used by users. The system uses techniques like breaking down words and getting rid of extra words that do not matter. This helps the system get the messages ready to check if they are spam. The system is then a lot faster and better at finding spam messages and saying what kind of message they are. Machine. Natural Language Processing work together to make the system really good, at finding spam. Neural Networks Artificial neural networks are used to find complex patterns and hidden dependencies in messages. They are used for increasing the predictability and reliability of the spam detection algorithm.

Deep Learning

LSTM, RNN, and other deep learning models that detect sequential data in text messages are used. Deep learning makes possible to predict spam texts efficiently.

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.021 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 6, June 2026

DOI: 10.17148/IJIREEICE.2026.14617

TECHNOLOGIES USED

AI-Based Spam Text Detector employs modern technologies during development.

Frontend Technologies

- HTML
- CSS
- JavaScript

Backend Technologies

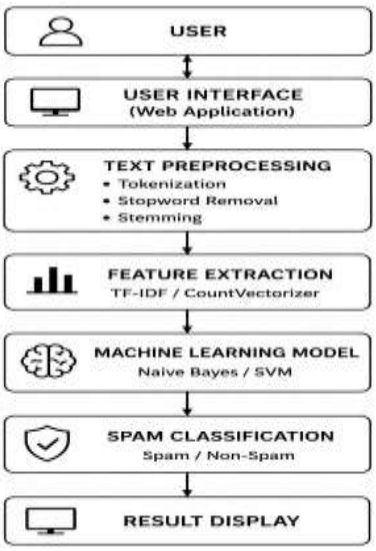
- Python
- Flask / Django
- Machine Learning Libraries
- Scikit-learn
- TensorFlow
- Keras
- Natural Language Processing
- NLTK
- SpaCy
- Databases
- MySQL
- MongoDB

It allows making the development of spam detection systems more efficient.

SYSTEM ARCHITECTURE

Modules included in the architecture of the AI-Based Spam Text Detector are as follows:

1.User Interface: Provides a means for inputting/uploading texts.
2.Text Preprocessor: Processes the inputted texts.
3.Feature Extractor: Translates texts into computer understandable forms.
4.AI Classification Algorithm: Detects spam using ML algorithms.
5.Result Viewer: Presents spam detection results.
6.Datastore: Storing information about users and messages.



SECURITY FEATURES

Authentication is guaranteed to keep hackers out by ensuring secure entry into the program. The user data and message are stored safely by means of security features in databases. Validation of the input data is done to keep away any malicious data being sent from a third party. Encryption methods may be applied to secure communication.

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.021 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 6, June 2026

DOI: 10.17148/IJIREEICE.2026.14617

APPLICATIONS

Email Spam Filtering
The system can be used for the detection and filtering of spam emails from email platforms. The solution secures the users against spam and phishing.
SMS Spam Detection
Mobile phone applications can use the spam detection system to filter out spam SMS messages.
Social Media Platforms
Social media websites can leverage the system for the prevention of scams and harmful contents within their platform.
Cybersecurity Systems
The system can be incorporated into organizations' cybersecurity systems.
E-commerce Websites
Online shopping platforms can employ the system in the identification of fake and spam messages.
Banks and Financial Institutions
Financial institutions can incorporate the system for detecting any spam messages and phishing attempts.

ADVANTAGES & LIMITATIONS

Advantages
- Minimizes efforts in manually filtering messages.
- Ensures accurate and fast detection of spam messages.
- Secures communication between two parties.
- Enables real-time analysis of spam messages.
- Processes huge volumes of data effectively.
- Decreases phishing attacks and cyber crimes.
- Enhances users' experiences.

Limitations
- Necessitates availability of quality datasets for improved accuracy.
- Certain complex spam messages can affect predictive performance.
- Larger computational power is required in model training process.
- Frequent upgrades are necessary to counteract spam trends.

WORKING OF THE SYSTEM

The whole process begins when a user puts in a message within the application. After that, the input message goes to the preprocessing stage, where unnecessary signs, stop words, and other irrelevant parts are filtered out from the message. Subsequently, the pre-processed message is vectorized to numeric values by means of text vectorization methods like TF-IDF.

Afterward the pre-processed and vectorized message goes through a Machine Learning model. This model has been trained on both spam messages and normal messages. The result is then shown to the user. It is also saved in the database for analysis.

FUTURE DEVELOPMENTS

The AI-Based Spam Text Detector may also be improved by integrating even more advanced Deep Learning techniques, which will allow for better prediction accuracy The system can also offer features such as multiple language spam detection and even voice spam detection in the future. Other improvements to be incorporated into the spam detection system include cloud computing technology, which would enable scalability, as well as adaptive learning, which would update the system automatically.

CONCLUSION

The Spam Text Detector that uses intelligence is a really useful tool. It helps find messages that people do not want to see when they are talking to each other online. This tool uses computer programs that get better at finding bad messages over time. This means it can save people a lot of time. The Spam Text Detector helps keep people safe from messages. It makes sure that when people talk to each online, they can do so without worrying about getting hurt. As artificial

DOI: 10.17148/IJIREEICE.2026.14617

intelligence gets better the Spam Text Detector will get even better at finding messages and keeping people safe from cyber threats. The Spam Text Detector will be really good at stopping people from sending mean messages.

REFERENCES

[1]. https://www.javatpoint.com/artificial-intelligence-tutorial
[2]. https://www.geeksforgeeks.org/nlp-tutorial/
[3]. https://www.tensorflow.org/
[4]. https://scikit-learn.org/
[5]. https://ieeexplore.ieee.org/
[6]. https://scholar.google.com/