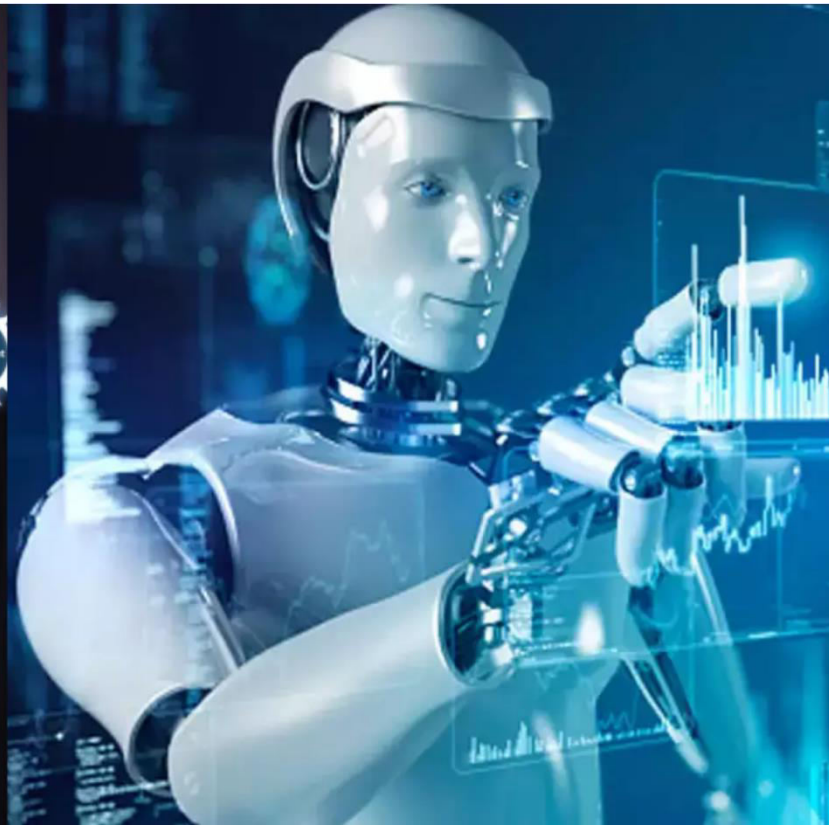
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

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: 8.699

Volume 15, Issue 3, March 2026

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

Impact Factor 8.699

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

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503107|

Cognitive Unified Multi-Model Spam Detection System

P Ashok Kumar[1], M Sai Krishna Yadav[2], K Manikanta[3], J Nithish[4], J Keerthi Chandra[5]

Assitant Professor, Department of CSE (Data Science), ACE Engineering College, Hyderabad, Telangana, India[1]

IV B.Tech. Students, Department of CSE (Data Science), ACE Engineering College, Hyderabad, Telangana, India[2,3,4,5]

ABSTRACT: The rapid expansion of digital communication has led to a noticeable increase in spam messages across various platforms such as emails, SMS, voice calls, and malicious web links. Most existing spam detection systems are designed to work within a single communication channel, which makes it difficult for them to identify spam activities that occur across multiple platforms. To address this challenge, this study introduces a **Cognitive Unified Multi-Model Spam Detection System**, an intelligent framework that detects spam across different communication mediums using machine learning and natural language processing techniques. The system combines multiple detection components, including text-based spam classification for emails and SMS messages, speech-to-text conversion for analyzing voice calls, and machine learning-based URL analysis for identifying potentially harmful links. By converting voice data into text and applying NLP models, the system can analyze spoken content in the same way as written messages. Additionally, heuristic and machine learning methods are used to evaluate URLs and detect phishing attempts. All detection results are presented through a centralized dashboard, allowing users to easily review alerts and analyze suspicious content in one place. Experimental evaluation shows that integrating multiple detection approaches improves the overall accuracy of spam detection while offering a more reliable and practical solution for protecting users from modern multi-platform spam threats.

KEYWORDS: Spam Detection, Multi-Modal Spam Detection, Natural Language Processing (NLP), Machine Learning, Speech-to-Text Processing, Phishing URL Detection, Cybersecurity, Text Classification

I. INTRODUCTION

With the rapid growth of internet services and digital communication, spam has become a major cybersecurity concern for both individuals and organizations. Spam messages are usually unwanted communications sent through platforms such as emails, SMS, voice calls, and websites. These messages often contain phishing links, fake offers, malware downloads, or attempts to steal sensitive personal information.

Most traditional spam detection systems are designed to work only within a single communication channel. For example, email filters, SMS blockers, caller identification apps, and browser security tools operate independently and do not share information with each other. As attackers increasingly use multiple platforms to spread spam, these isolated systems struggle to detect coordinated spam activities effectively.

Recent advancements in machine learning and natural language processing have made it possible to analyze textual data more intelligently by identifying patterns, word usage, and contextual meaning to classify messages as spam or legitimate. Similarly, speech-to-text technologies allow voice content to be converted into text, enabling voice messages to be analyzed using text-based spam detection methods.

To overcome the limitations of existing approaches, this work proposes a **Cognitive Unified Multi-Model Spam Detection System** that integrates spam detection across multiple communication channels into a single platform. The system combines NLP-based text classification, speech-to-text processing for voice messages, and machine learning techniques for detecting malicious URLs. By bringing these components together in a unified framework, the system aims to improve spam detection accuracy and provide users with a centralized and more efficient way to analyze suspicious communications.

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

Impact Factor 8.699

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

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503107|

II. LITERATURE SURVEY

Spam detection has become an important research area in the fields of cybersecurity, machine learning, and natural language processing. With the rapid increase in digital communication through emails, text messages, phone calls, and online platforms, spam attacks have also become more sophisticated. Researchers have proposed various techniques to automatically identify spam messages and protect users from phishing, fraud, and malicious content.

One of the earliest approaches used for spam detection is the **Naïve Bayes classification technique**. Sahu and Mishra (2020) applied this method for detecting spam in email communication using TF-IDF feature extraction. Naïve Bayes works by calculating the probability of a message being spam based on the occurrence of specific words within the text. Because of its simplicity and computational efficiency, it became one of the most widely used algorithms in early spam filtering systems. However, the model has certain limitations. It assumes independence between words, which is not always true in natural language. As a result, its performance can decrease when handling short messages or when spam patterns change frequently.

With the advancement of deep learning, researchers began exploring neural network-based approaches for spam detection. Manjunatha et al. (2023) proposed an **LSTM-based model** for detecting spam in SMS messages. Long Short-Term Memory networks are a type of recurrent neural network that can capture sequential patterns in textual data. Unlike traditional machine learning models, LSTM networks are capable of understanding context and relationships between words in a sentence. This ability makes them highly effective for analyzing short messages where contextual meaning plays an important role. Their work showed that deep learning models can achieve higher accuracy compared to traditional methods, although they require larger datasets and more computational resources.

Another important area of research focuses on detecting **malicious or phishing URLs**. Phishing attacks often involve sending fraudulent links that redirect users to fake websites designed to steal personal information. Sinha and Sandeep (2019) proposed a machine learning approach to identify phishing URLs using lexical and host-based features. These features include characteristics such as the length of the URL, presence of unusual characters, number of subdomains, and the age of the domain. Algorithms such as Random Forest and Support Vector Machines were used to classify URLs as safe or malicious. Although these methods show promising results, they often struggle when attackers generate new domains or use URL obfuscation techniques.

To further improve detection performance, some researchers have explored **hybrid approaches** that combine rule-based analysis with machine learning models. Patil and Deshmukh (2022) introduced a system that integrates heuristic rules with machine learning algorithms to identify phishing websites. Their approach examines various factors such as SSL certificate validity, URL structure, domain information, and webpage behavior. By combining multiple detection strategies, the system becomes more effective in identifying both known and unknown phishing attacks. Hybrid models are particularly useful in dealing with zero-day attacks where traditional detection methods may fail.

Despite these advancements, most existing spam detection systems are designed to operate within a **single communication channel**. Email filters only detect spam emails, SMS detection systems focus on text messages, and URL scanners analyze web links separately. In real-world scenarios, attackers often use multiple communication channels simultaneously. For example, a phishing campaign may begin with an email containing a malicious link, followed by an SMS reminder or a fraudulent phone call. Since traditional systems operate independently, they are unable to correlate information across different communication platforms.

Therefore, there is a clear need for a **unified spam detection framework** that can analyze spam activities across multiple communication channels in a coordinated manner. The proposed **Cognitive Unified Multi-Model Spam Detection System** addresses this limitation by integrating several detection techniques into a single platform. By combining natural language processing for text analysis, speech-to-text processing for voice messages, and machine learning models for URL analysis, the system provides a comprehensive approach to detecting spam across emails, SMS messages, voice calls, and web links.

This integrated approach not only improves spam detection accuracy but also offers a centralized and user-friendly solution for monitoring suspicious communication activities across different digital platforms.

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

Impact Factor 8.699

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

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503107|

III. METHODOLOGY

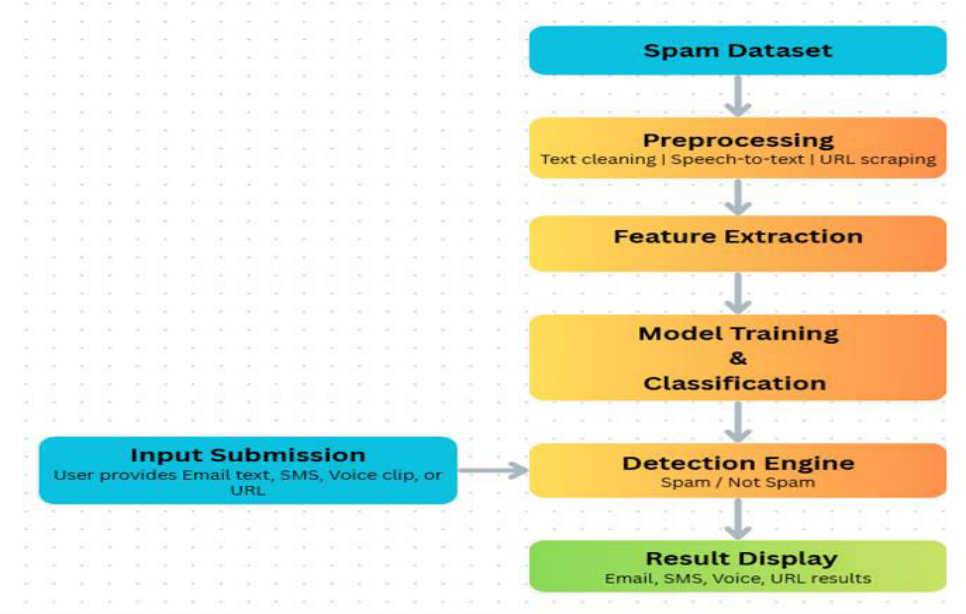


Fig. 1. Methodology

The proposed system, **Cognitive Unified Multi-Model Spam Detection System**, utilizes machine learning, natural language processing, and speech processing techniques to identify spam across multiple communication platforms. The methodology follows a structured pipeline that processes various types of user inputs such as emails, SMS messages, voice recordings, and URLs, and analyzes them through multiple detection modules to determine whether the content is spam or legitimate, as illustrated in Fig. 1.

The process begins at the **Input Submission Interface**, where users provide the content they want to analyze. This input may include email text, SMS messages, voice clips, or suspicious URLs. The system collects this data and forwards it to the preprocessing stage for further analysis.

In the **Preprocessing Module**, the input data undergoes several cleaning and preparation steps. For textual inputs such as emails and SMS messages, the system performs text normalization, removal of unnecessary characters, tokenization, and stop-word filtering to prepare the text for analysis. Voice inputs are processed using a **speech-to-text conversion module**, which transforms spoken content into textual format. Similarly, URLs are analyzed using scraping and lexical analysis techniques to extract relevant structural information.

After preprocessing, the cleaned data is passed to the **Feature Extraction Module**, where important patterns and characteristics are identified. For textual data, linguistic features such as word frequency, keyword patterns, and contextual relationships are extracted and converted into numerical representations suitable for machine learning models. For URLs, structural features such as domain length, suspicious characters, and domain properties are extracted to assist in identifying phishing links.

The extracted features are then provided to the **Model Training and Classification Module**, where machine learning models analyze the data to identify spam patterns. These models learn from labeled datasets and identify relationships between features that commonly appear in spam communications. During classification, the trained models evaluate the input and determine whether the content is spam or legitimate.

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

Impact Factor 8.699

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

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503107|

The classification results are processed by the **Spam Detection Engine**, which serves as the central decision-making component of the system. This engine integrates predictions from different models and generates a final classification outcome indicating whether the submitted content should be considered spam.

Finally, the detection results are presented through the **Result Display Module**, where the system provides clear feedback to the user. The dashboard displays the classification outcome along with relevant details for each input type, including email analysis, SMS classification, voice message evaluation, and URL safety status. This integrated approach allows users to easily understand the results and take appropriate actions against suspicious communications.

The System Architecture is as follows –

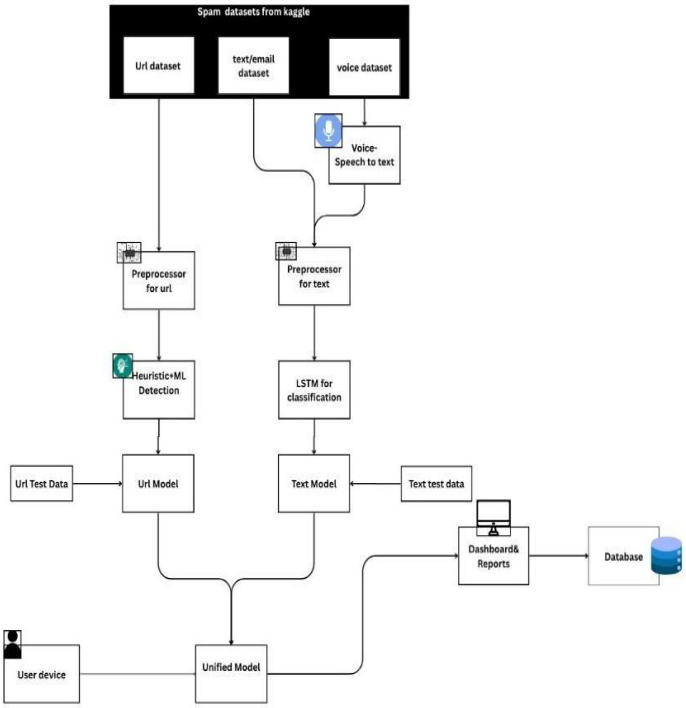


Fig. 2. System Architecture

The architecture of the **Cognitive Unified Multi-Model Spam Detection System** is designed to analyze spam across multiple communication channels such as emails, SMS messages, voice recordings, and URLs. The system integrates different datasets, preprocessing modules, machine learning models, and a centralized dashboard to create a unified spam detection framework, as illustrated in Fig. 2.

The process begins with **data acquisition**, where spam datasets are collected from sources such as Kaggle. These datasets include URL data, text or email messages, and voice recordings. The collected datasets are used for training and evaluating the detection models. Since voice data cannot be directly analyzed as text, it is first processed using a **speech-to-text module**, which converts audio recordings into textual format for further analysis.

Next, the system performs **data preprocessing** to prepare the inputs for machine learning models. Text data from emails and SMS messages is cleaned and normalized by removing unnecessary characters and organizing the text into tokens. For URLs, the preprocessing module extracts important structural features such as domain characteristics and suspicious patterns.

After preprocessing, the system applies **machine learning models for spam detection**. Text data is analyzed using an **LSTM-based classification model**, which can capture contextual relationships between words and identify spam

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

Impact Factor 8.699

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

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503107|

patterns in messages. URL inputs are analyzed using a **hybrid approach combining heuristic rules and machine learning techniques** to detect phishing or malicious links.

The outputs from both the text model and the URL model are combined in a **Unified Detection Model**, which produces the final classification result indicating whether the content is spam or legitimate. Users interact with the system through a dashboard where they can submit data and view the analysis results. The results are also stored in a **database**, allowing the system to maintain records for reporting and future analysis.

This architecture enables efficient processing of multiple communication formats and provides a centralized platform for spam detection across different digital channels.

IV. EXPERMENTAL RESULTS

Figures 3–5 illustrate the output generated by the proposed **SpamGuard Unified Multi-Modal Detection System** for different types of spam analysis. **Fig. 3** shows the login interface where users enter their credentials to securely access the system. This authentication step ensures that only authorized users can use the spam detection platform.

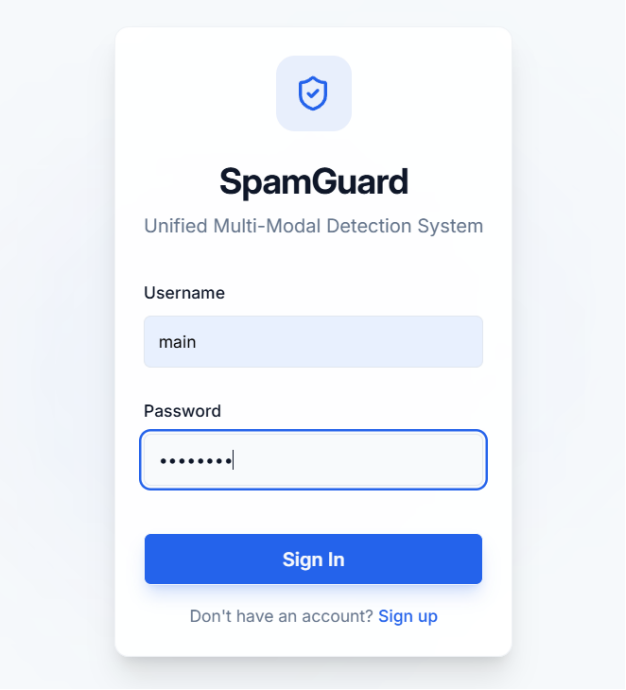


Fig. 3. User Login Interface

Fig. 4 shows the main dashboard interface of the system. Users can submit different types of content such as text messages, audio inputs, or URLs for spam analysis. The system processes the input through preprocessing and machine learning based detection modules.

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

Impact Factor 8.699

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

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503107|

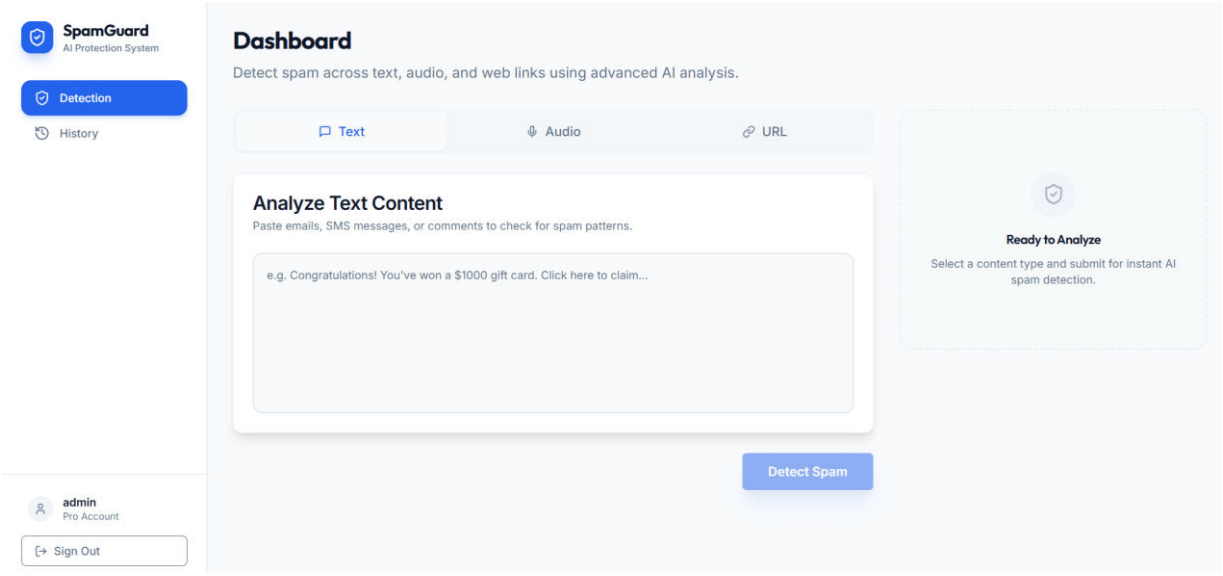


Fig. 4. User Dashboard Interface

Fig. 5 shows the spam detection result generated by the system. After analyzing the submitted text, the model identifies spam patterns and displays the result along with a confidence score and explanation indicating why the content is classified as spam.

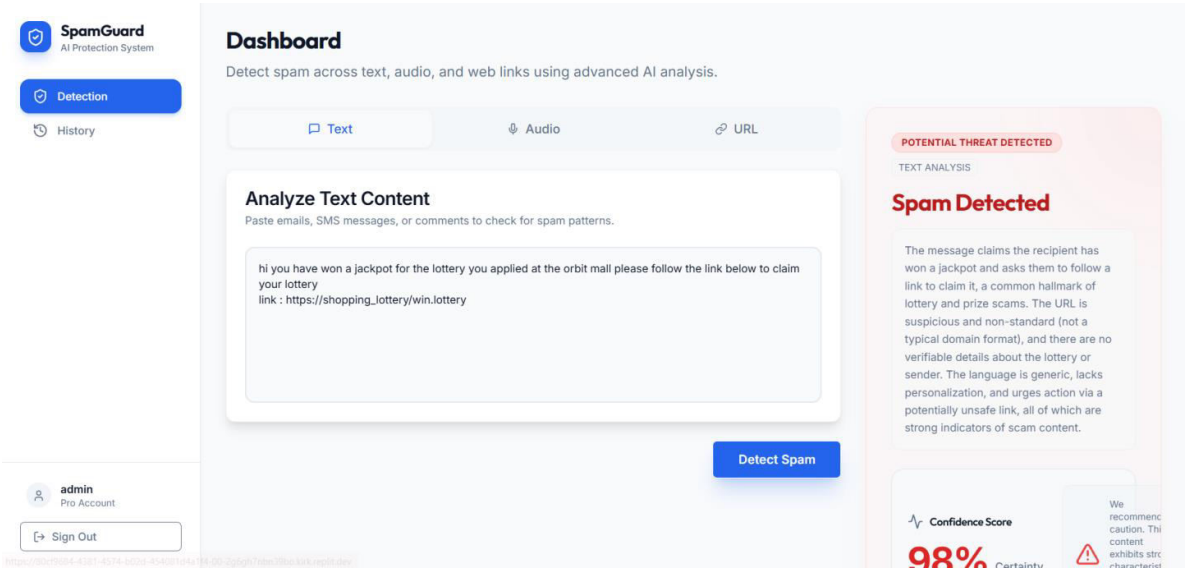


Fig. 5. Spam Detection

The experimental results show that the proposed **SpamGuard Unified Multi-Modal Detection System** is effective in identifying spam across different types of inputs such as text messages, voice content, and URLs. The system successfully analyzes the submitted data using preprocessing and machine learning models to detect suspicious patterns commonly found in spam communications. When spam characteristics such as fraudulent links, misleading claims, or suspicious language are detected, the system accurately classifies the content as spam and provides a confidence score for the prediction. The unified framework improves detection reliability by combining multiple analysis methods,

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

Impact Factor 8.699

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

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503107|

enabling the system to handle different communication formats and provide consistent results across various types of inputs.

V. CONCLUSION

The Cognitive Unified Multi-Model Spam Detection System presents a comprehensive solution for identifying spam across different communication channels such as emails, SMS messages, voice calls, and URLs. Unlike traditional spam detection systems that focus on a single medium, the proposed system integrates multiple detection techniques within one unified framework. By combining machine learning models, natural language processing, and speech-to-text technology, the system can analyze various forms of communication data and identify spam patterns more effectively.

The system processes text-based inputs such as emails and SMS messages using NLP techniques that analyze language patterns, keywords, and contextual relationships to detect suspicious content. Voice recordings are first converted into textual form using speech-to-text processing and then analyzed using the same classification methods. Similarly, URLs are examined using machine learning and heuristic analysis to detect phishing links and malicious websites. By combining these detection modules, the system is able to provide a more reliable and comprehensive spam detection mechanism.

Another key feature of the proposed system is the centralized dashboard, which allows users to submit content for analysis and easily view detection results. The user-friendly interface enables efficient monitoring of suspicious messages and provides clear outputs indicating whether the content is spam or legitimate. This integrated approach improves usability and allows users to manage spam detection activities within a single platform.

The experimental results demonstrate that the system is capable of accurately identifying spam messages and malicious links while maintaining efficient processing performance. The unified framework improves detection accuracy by combining multiple models and analyzing different communication formats. This helps the system handle complex spam patterns that may involve more than one communication channel.

In addition, the modular architecture of the system ensures flexibility and scalability for future improvements. Each detection module, including text analysis, voice processing, and URL verification, operates independently while contributing to the overall spam detection framework. This design makes it easier to update models, integrate new detection algorithms, and adapt to evolving cyber threats without affecting the entire system.

Overall, the proposed system highlights the importance of integrating advanced artificial intelligence techniques to strengthen spam detection and improve digital communication security. As cyber threats continue to evolve, developing intelligent and adaptive spam detection systems becomes increasingly important. In the future, the system can be enhanced by incorporating real-time monitoring, multilingual spam detection capabilities, and integration with communication services such as email platforms and messaging applications. These improvements will further enhance the system's ability to protect users from modern spam and phishing attacks.

REFERENCES

[1] Sahu, S. M., & Mishra, S. R. (2020). Email Spam Detection Using Naive Bayes. International Journal of Computer Applications and Information Technology.
[2] Manjunatha, P. V., et al. (2023). SMS Spam Detection Using LSTM Networks. International Journal of Advanced Computer Science and Applications.
[3] Sinha, D., & Sandeep, A. (2019). Phishing URL Detection Using Machine Learning. International Journal of Computer Science and Information Security.
[4] Zhang, et al. (2021). Deep Learning for Spam Detection in Social Media Messages. IEEE Access.
[5] Patil, P., & Deshmukh, R. (2022). Hybrid Machine Learning and Heuristic System for Phishing Website Detection. International Journal of Information Security and Applications.

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