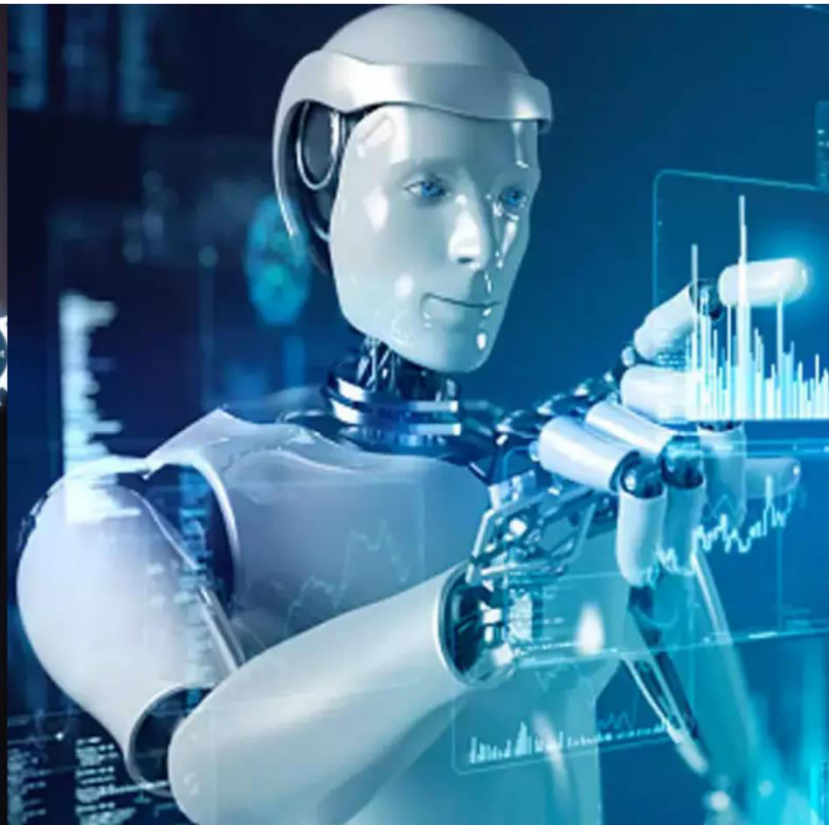
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

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 2, February 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 2, February 2026

|DOI: 10.15680/IJIRSET.2026.1502073|

Intelligent SMS Scam Detection

Blessy Ani Mol V[1], Golda T[1], Subisha M[1], Poora Seetha B[2]

Department of Information Technology, Arunachala College of Engineering for Women, Manavilai, Vellichanthai, Tamil Nadu, India[1]

Assistant Professor, Department of Information Technology, Arunachala College of Engineering for Women, Manavilai, Vellichanthai, Tamil Nadu, India[2]

ABSTRACT: With the rapid growth of mobile communication, Short Message Service (SMS) has become one of the most widely used means of exchanging information. However, the increasing volume of unsolicited and fraudulent messages has raised serious concerns regarding user privacy and security. This project, titled "Intelligent SMS Scam Detection", aims to develop a smart and efficient Android-based SMS application capable of detecting spam messages and protecting users from unwanted communications.

KEYWORDS: SMS Spam Detection, Android Application, Machine Learning, Message Filtering, User Privacy, Scam Prevention, Real-time Analysis, Cloud Integration.

I. INTRODUCTION

With the continuous advancement of mobile communication technology, the use of Short Message Service (SMS) has become an essential means of personal and business communication. Despite its convenience and low cost, SMS has also become a common medium for spam messages, including advertisements, phishing attempts, and fraudulent schemes. These unsolicited messages not only disturb users but can also pose significant security and privacy risks. Traditional SMS applications lack effective mechanisms to identify and filter such unwanted content automatically. As a result, users are often left to manually manage and delete spam messages, which can be both time-consuming and inefficient. To address this issue, there is a growing need for intelligent systems capable of detecting and blocking spam SMS efficiently.

This project, titled **"SMS SPAM DECETATION"** focuses on developing a smart SMS application that serves as the default messaging platform on an Android device. It integrates spam detection algorithms to identify suspicious content, automatically block messages from spam senders, and notify users about potential threats. The proposed system enhances user experience, reduces message clutter, and contributes to the overall security of mobile communication. The widespread use of SMS as a communication tool has made it a prime target for spammers who exploit this medium to send unsolicited-messages, advertisements, and fraudulent links. Existing default SMS applications on Android devices lack an intelligent mechanism to automatically identify and filter out such spam messages. As a result, users frequently receive unwanted or malicious messages that clutter their inbox, waste time, and may even lead to financial or data loss if phishing links are accessed. The absence of an efficient, automated, and user-friendly spam detection and blocking system creates a significant gap in mobile security and usability. Therefore, there is a need for a smart SMS application that can effectively detect spam messages in real-time, block suspicious senders, and provide secure message handling within the Android environment. The scope of the **SMS Spam Detection** project includes the development and implementation of a fully functional Android SMS application capable of detecting and blocking spam messages. The methodology for the **SMS Spam Detection** project is designed to systematically address the problem of spam messages on Android devices. The research and development process follows a combination of **software development methodology** and **experimental testing** to ensure efficiency, usability, and reliability. **Requirement Analysis:** Identify the problems faced by users due to spam messages. Study existing SMS applications and their limitations in spam detection. Define the functional and non-functional requirements for the new system, including real-time detection, notification, and auto- blocking. In the current mobile communication environment, SMS messages are handled by the default messaging applications provided by Android or device manufacturers. These applications primarily focus on **sending, receiving, and storing messages**, providing features such as message notifications, contact management, and basic search functionality.

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 2, February 2026

|DOI: 10.15680/IJIRSET.2026.1502073|

However, existing SMS systems have **limited capabilities for detecting and** managing spam messages. Most default messaging apps rely on simple keyword filtering or user reporting to identify spam, which may not be sufficient to prevent new or cleverly disguised spam messages. Users often have to manually delete spam or block numbers, which can be time-consuming and ineffective against sophisticated phishing or promotional messages.

II. LITERATURE REVIEW

The rapid growth of mobile communication has brought significant advantages, but it has also led to the widespread problem of SMS spam, which affects users' privacy, security, and overall messaging experience. The purpose of this chapter is to review existing research, techniques, and systems developed for SMS spam detection and prevention. By examining previous work, both in keyword-based filtering and machine learning approaches, this chapter aims to identify the strengths, limitations, and gaps in current solutions. The literature review provides a foundation for the design and development of the proposed SMS Spam Detection application, helping to ensure that the system addresses existing challenges effectively while incorporating best practices and innovative techniques. SMS spam detection is a crucial aspect of mobile communication security, aimed at identifying and preventing unsolicited, fraudulent, or malicious messages. Spam messages often contain advertisements, phishing links, or fraudulent schemes that can compromise users' privacy and financial security.

Rule-Based Detection: This method relies on predefined lists of keywords, phrases, or patterns commonly found in spam messages. Messages containing these indicators are classified as spam and either blocked or moved to a separate folder. While simple and fast, rule-based systems may fail to detect new or obfuscated spam content.

Machine Learning-Based Detection: Advanced techniques utilize algorithms such as **Naive Bayes, Support Vector Machines (SVM), Decision Trees, and Neural Networks** to classify messages based on patterns learned from large datasets of spam and legitimate messages. Data plays a critical role in the detection and prevention of SMS spam, as it forms the foundation for identifying patterns, trends, and characteristics of spam messages. Effective SMS spam detection relies on the availability of accurate and comprehensive datasets containing both legitimate and spam messages.

Message Content: The primary data source is the content of SMS messages, including text, keywords, links, and special characters. By analyzing message content, spam detection systems can identify suspicious patterns or phrases commonly associated with spam.

Sender Information: Data regarding the sender, such as phone numbers, message frequency, and historical behavior, is essential for detecting repeated spam sources. Systems can block or flag messages from suspicious numbers automatically.

User Interaction Data: Feedback from users, such as marking messages as spam or reporting suspicious messages, enhances the accuracy of spam detection systems. This data helps in updating spam patterns and improving the rules or machine learning models used for classification.

Training Data for Machine Learning: For advanced detection methods, large datasets of labeled messages (spam and non-spam) are required to train machine learning models. The quality and diversity of this data directly impact the performance, adaptability, and accuracy of the spam detection system.

Hybrid Approaches: Some systems combine rule-based filtering with machine learning to achieve higher accuracy, leveraging the speed of keyword matching and the adaptability of APS

blocking, user notifications, and spam reporting features to enhance usability and security. These methods form the basis for modern SMS spam detection applications and provide guidance for designing efficient mobile solutions, such as the proposed SMS 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 2, February 2026

|DOI: 10.15680/IJIRSET.2026.1502073|

Feature Extraction: The first step in data-driven detection involves extracting features from SMS messages, such as word frequency, message length, presence of URLs, special characters, and sender information. These features help the system differentiate between spam and legitimate messages.

Behavioral Analysis: Data-driven methods also analyze user behavior and sender patterns. For example, repeated messages from a single sender or unusual messaging frequency can indicate spam activity. Integrating behavioral data enhances detection accuracy and reduces false positives.

III. PROPOSED SYSTEM

The proposed system is an **Android- based SMS application** designed to provide efficient, real-time detection and management of spam messages. Unlike existing SMS apps, which
primarily rely on user reporting or basic filtering, the proposed system combines
automatic spam detection, notification, and blocking features to enhance user experience and security. **Default SMS Application:** The app is installed and manually set as the default SMS app, allowing it to capture and manage all incoming messages.
Real-Time Spam Detection: Incoming messages are analyzed in real-time using a **keyword-based filtering mechanism**, enabling immediate identification of potential spam messages.
Automatic Blocking: Messages identified as spam are not only flagged but the sender's number is automatically added to a **block list** to prevent future spam.
Notification System: Users receive **notifications for legitimate messages** while spam messages can be redirected to a separate folder, minimizing disruption.
Message Categorization: The system maintains separate folders for **Inbox and Spam**, providing organized message management and easy access for users.
User-Friendly Interface: The app is designed with simplicity in mind, ensuring that users can navigate and manage messages without technical expertise.
Real-Time Spam Detection: The system identifies spam messages as they arrive, reducing the chances of users being exposed to fraudulent or unwanted content.
Automatic Blocking: Spam numbers are automatically added to a block list, preventing repeated spam and saving users from manual intervention.
Organized Message Management: Messages are categorized into **Inbox and Spam folders**, allowing users to access legitimate messages easily while isolating unwanted content.
Enhanced User Security: By filtering spam messages and blocking suspicious numbers, the system protects users from phishing attacks, fraud, and unsolicited advertisements.
User Notifications: Legitimate messages trigger normal notifications, while spam messages are handled discreetly, minimizing distractions.
Customizable and User-Friendly: The application provides a simple interface that allows users to manage messages and view spam reports without technical expertise.
Efficiency and Reliability: Integrating detection, blocking, and notification features ensures a smooth messaging experience, reducing the risk of missed important messages.
Foundation for Future Enhancement: The system can be extended to include **machine learning-based detection** or support for multimedia messages, making it adaptable to evolving spam techniques. spam identification, resource.
Comparison of Existing and Proposed System
The comparison between the existing SMS systems and the proposed SMS Spam Detection application highlights the improvements and added functionalities of the new system.

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

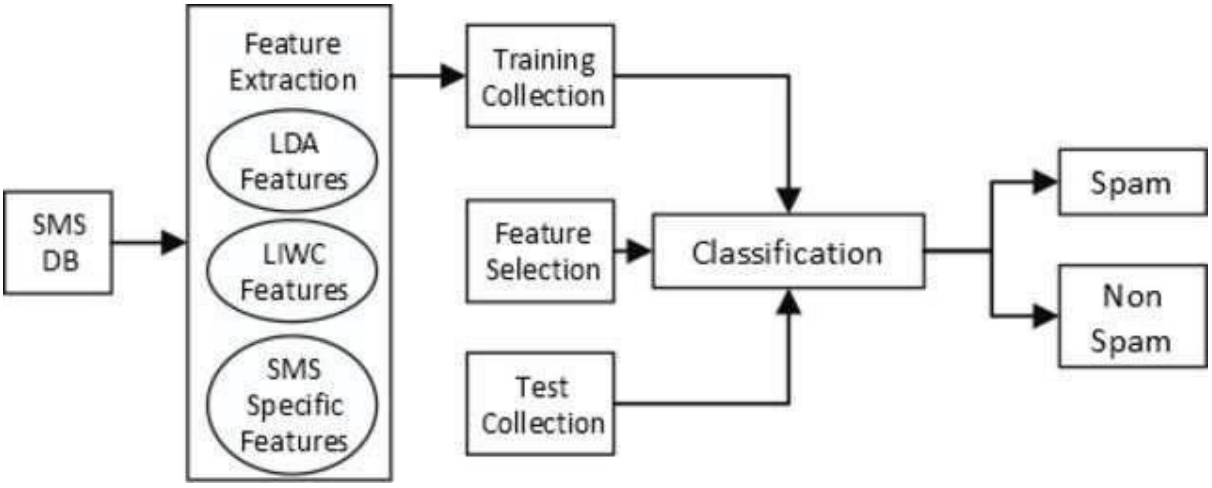
Impact Factor 8.699

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

Volume 15, Issue 2, February 2026

|DOI: 10.15680/IJIRSET.2026.1502073|

Feature / Parameter	Existing System	Proposed System
Spam Detection	Limited, mostly keyword-based or user- reported	Real-time detection using keyword- based filtering with scope for machine learning integration
Automatic Blocking	Not available; users manually block numbers	Automatically blocks identified spam numbers to prevent repeated messages
Message Categorization	All messages appear in a single inbox	Separates messages into Inbox and Spam folders for better organization
User Notifications	All messages trigger notifications; spam is not filtered	Legitimate messages trigger notifications, spam messages handled discreetly
Ease of Use	Standard interface with basic features	User-friendly interface with automated spam management
Security and Privacy	Vulnerable to phishing and fraudulent messages	Enhanced security by identifying and blocking spam messages automatically
Adaptability	Static rules; cannot adapt to new spam patterns	Flexible system; can be enhanced with data- driven or ML- based detection



IV. MODULE DESCRIPTION

The SMS Spam Detection system is designed using a modular approach, where each module handles a specific task to ensure smooth and efficient operation. The first module is **Install & Set Default SMS App**, which allows the user to install the application on their

Android device and set it as the default SMS handler, enabling the app to capture all incoming messages. The second module, **Receive Message**, is responsible for capturing incoming SMS messages in real-time and extracting key information such as the sender's number, message content, and timestamp. Once the message is received, it is processed by the **Spam Detection** module, which analyzes the message content using predefined keywords, patterns, or rules to classify it as either spam or legitimate. The first module of the SMS Spam Detection system focuses on

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 2, February 2026

|DOI: 10.15680/IJIRSET.2026.1502073|

installation and configuration. When the user installs the application, it must be set as the default SMS handler on the device. This step is essential because only the default SMS app can access incoming messages in real-time. By configuring the app as the default, the system ensures that all messages are captured directly by the application, enabling subsequent modules to analyze and manage messages efficiently. This setup provides the foundation for the spam detection and message management processes that follow.

User installs the app and sets it as default SMS handler The first module of the SMS Spam Detection system focuses on installation and configuration. When the user installs the application, it must be set as the default SMS handler on the device. This step is essential because only the default SMS app can access incoming messages in real-time. By configuring the app as the default, the system ensures that all messages are captured directly by the application, enabling subsequent modules to analyze and manage messages efficiently. This setup provides the foundation for the spam detection and message management processes that follow.

Incoming SMS is captured the second module of the SMS Spam Detection system is responsible for capturing incoming SMS messages in real-time. Once the application is set as the default SMS handler, every incoming message is intercepted by this module. It extracts important details such as the sender's phone number, message content, and timestamp. This information is then passed to the next module for analysis. By accurately capturing all incoming messages, this module ensures that no SMS is missed and lays the groundwork for effective spam detection and message management.

Message is analyzed for spam The third module of the SMS Spam Detection system is responsible for analyzing each incoming message to determine whether it is spam or legitimate. Using predefined keywords, patterns, and filtering rules, the module examines the content of the message and classifies it accordingly. This analysis is crucial for preventing unwanted messages from reaching the user's inbox.

Auto-Block Spam Number The fourth module of the SMS Spam Detection system focuses on automatically blocking spam numbers. When a message is classified as spam by the previous module, this module adds the sender's phone number to a block list to prevent any future messages from the same source. This automated blocking reduces the risk of repeated spam and minimizes user intervention. By maintaining and updating the block list in real-time, the system ensures that spam messages are effectively filtered out, enhancing the overall security and usability of the messaging application.

Message Storage? The fifth module of the SMS Spam Detection system is responsible for storing messages based on their classification. Legitimate messages are saved in the Inbox, while messages identified as spam are stored in a separate Spam Folder. This segregation ensures that important communications are easily accessible to the user, while spam messages are kept separate for review or deletion. By organizing messages in this way, the system enhances user convenience, reduces clutter in the Inbox, and supports the effectiveness of the spam detection and auto-blocking mechanisms implemented in earlier modules.

V. RESULTS AND DISCUSSION

This chapter presents a detailed analysis of the results obtained from the development, implementation, and testing of the SMS Spam Detection system. The primary objective of this project is to create an Android-based application capable of capturing incoming SMS messages in real-time, detecting spam messages using predefined rules and patterns, automatically blocking spam numbers, storing messages in appropriate folders, and notifying users only about legitimate messages. In this chapter, the performance of the system is evaluated to demonstrate its effectiveness in handling both spam and legitimate messages.

The discussion begins with the testing of the application's core functionalities, including the installation process, setting the app as the default SMS handler, and receiving messages from different sources. Each received message is analyzed by the spam detection module, and the results are recorded to determine the system's accuracy in identifying spam. The efficiency of the auto-blocking feature is also tested to verify that numbers identified as spam are successfully prevented from sending future messages. Furthermore, the storage mechanism is examined to ensure that legitimate messages are properly stored in the Inbox while spam messages are stored in the Spam Folder. The notification system

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 2, February 2026

|DOI: 10.15680/IJIRSET.2026.1502073|

is also evaluated to confirm that alerts are generated only for legitimate messages, avoiding unnecessary interruptions caused by spam

messages.

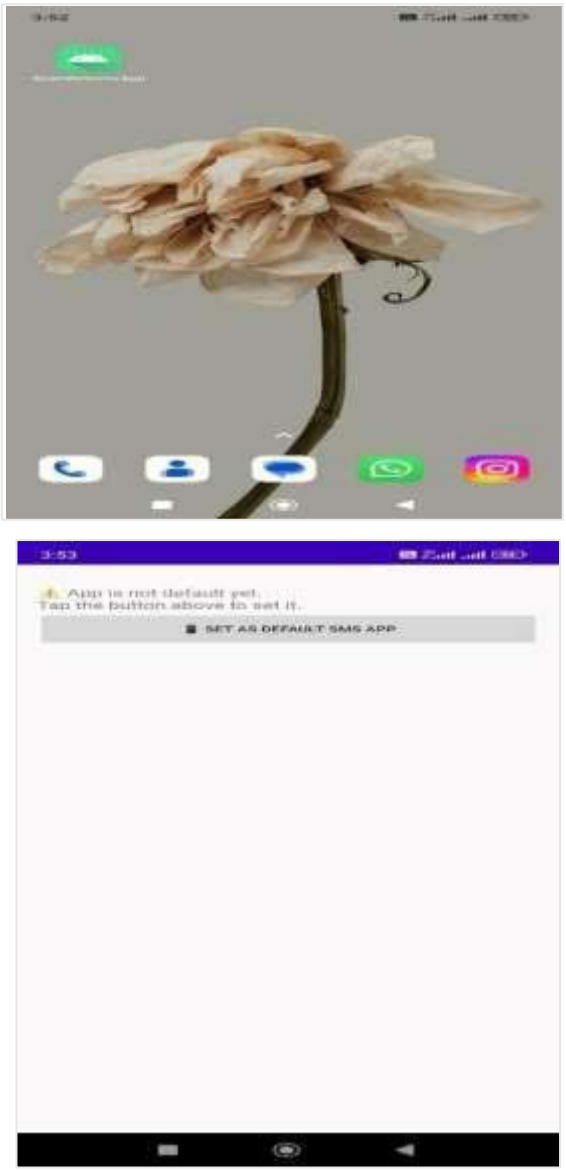


Figure 5.1 Install & Set Default App

Figure 5.1 illustrates the process of installing the SMS Spam Detection application on an Android device and setting it as the default SMS handler. This step is crucial because only the default SMS app can capture incoming messages in real-time. The figure shows the installation screen, followed by the prompts that guide the user to grant necessary permissions and configure the application as the default messaging app. Once this setup is complete, the application is ready to intercept incoming messages and perform spam detection, ensuring that all subsequent modules operate correctly. This visual representation highlights the simplicity and user- friendly nature of the installation and configuration process.

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 2, February 2026

|DOI: 10.15680/IJIRSET.2026.1502073|

Figure 5.2 Receive Normal SMS

Figure 5.2 demonstrates the process of receiving a normal (legitimate) SMS on the SMS Spam Detection application after it has been set as the default SMS handler. The figure shows how an incoming message from another phone is captured in real-time by the app and displayed in the Inbox. This ensures that the user can view legitimate messages immediately, just as they would in a standard messaging application. The module responsible for capturing messages works seamlessly to extract details such as the sender's number, message content, and timestamp, enabling further processing like notification alerts. This figure highlights the system's ability to handle regular SMS traffic efficiently without missing any messages, while preparing them for spam detection if needed.

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 2, February 2026

|DOI: 10.15680/IJIRSET.2026.1502073|

Figure 5.3 Detect Spam Auto- Block

Figure 5.3 demonstrates the SMS Spam Detection system's capability to automatically block numbers identified as sources of spam. When an incoming message is detected as spam, the system not only prevents it from appearing in the Inbox but also adds the sender's number to the block list. This ensures that any future messages from the same number are automatically blocked, reducing repeated spam and minimizing user intervention. The figure highlights how the spam detection and auto- blocking modules work together in real-time to maintain a secure and organized messaging environment, improving overall user experience by keeping the Inbox free from unwanted messages.

VI. CONCLUSION

The SMS Spam Detection System successfully achieves its goal of providing a secure and user-friendly solution to the increasing problem of spam and fraudulent messages in mobile communication. By functioning as the default SMS

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 2, February 2026

|DOI: 10.15680/IJIRSET.2026.1502073|

application on Android devices, the system captures incoming messages in real-time, analyzes their content using predefined filters and patterns, and accurately classifies them as either spam or legitimate.

The system automatically blocks spam numbers, ensuring that future messages from such senders are restricted, while legitimate messages are safely delivered and notified to users. This reduces unwanted communication, enhances privacy, and minimizes the risk of phishing or fraudulent attacks.

REFERENCES

[1] M. Salman, M. Ikram, N. Basta, and M. A. Kaafar, "SpaLLM-Guard: Pairing SMS Spam Detection Using Open-source and Commercial LLMs," arXiv preprint arXiv:2501.04985, 2025.
[2] D. Goel, H. Ahmad, A. K. Jain, and N. K. Goel, "Machine Learning Driven Smishing Detection Framework for Mobile Security," arXiv preprint arXiv:2412.09641, 2024.
[3] H. C. Altunay, "SMS Spam Detection System Based on Deep Learning," MDPI Electronics, vol. 14, no. 24, p. 11804, 2024.
[4] A. Shinde and P. Deshmukh, "SMS Scam Detection Application Based on Optical Character Recognition," MDPI Sensors, vol. 24, no. 18, p. 6084, 2024.
[5] M. F. Johari et al., "Key Insights into Recommended SMS Spam Detection Datasets," Scientific Reports, vol. 15, p. 92223, 2025.
[6] S. R. Prusty et al., "SMS Fraud Detection Using Machine Learning," ResearchGate, 2022.
[7] M. A. Uddin, "Exploring Transformer-Based Language Modeling Approach for SMS Spam Detection," ScienceDirect, 2025.
[8] P. Sharma and R. Singh, "Comparative Study of Machine Learning Algorithms for SMS Spam Detection," Int. J. Comput. Appl., vol. 185, no. 3, pp. 1–6, 2023.
[9] S. Hosseinpour and S. Das, "POSTER: A Multi-Signal Model for Detecting Evasive Smishing," arXiv preprint arXiv:2505.18233, 2025.
[10] T. Almeida, J. M. G. Hidalgo, and A. Yamakami, "Contributions to the Study of SMS Spam Filtering: New Collection and Results," Proc. ACM DocEng, pp. 259–262, 2011.
[11] M. F. Johari, "An Evaluation of SMS Spam Detection Models Using BERT and LSTM," IEEE Access, vol. 12, pp. 115421–115430, 2024.
[11] S. Goyal and R. Arora, "Spam Detection in SMS Using Hybrid Machine Learning Techniques," Int. J. Adv. Res. Comput. Sci., vol. 13, no. 4, pp. 45–51, 2022.
[12] N. Patil, V. Shinde, and R. Kale, "A Real-Time SMS Spam Detection System Using NLP and Machine Learning," IEEE SmartTechCon, pp. 247–252, 2023.
[13] "SMS Spam Collection Dataset," Kaggle, 2025. [Online]. Available: https://www.kaggle.com/datasets/uciml/sms-spam-collection-dataset
[14] "Google Is Using On-Device AI to Spot Scam Texts and Investment Fraud," Wired, 2025. [Online]. Available: https://www.wired.com/story/google- io-on-device-ai-scam-texts.

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