International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435 (Online) Volume 15, Issue 04, April 2026)

Securo: An AI-Based SMS Phishing Link Detection and Alert System

Prof. Shahjahan Shaikh[1], Chaudhary Lajina[2], Jha Pratima[3], Zore Sanjana[4]

***Abstract*—Securo is a mobile application for real-time detection of phishing links in SMS messages. It uses rule-based and machine learning techniques to alert users against smishing attacks.**

***Keywords*—Smishing, phishing detection, SMS security, machine learning, mobile application, cybersecurity.**

I. Introduction

With the rise in smartphone usage, SMS-based phishing attacks (smishing) have become a major threat. Securo is a mobile application that detects phishing links in real time and alerts users to improve mobile security.

II. Proposed Work

Health Existing cybersecurity applications mainly focus on spam detection, caller identification, and email phishing prevention.

Truecaller and similar platforms help identify spam calls and suspicious SMS senders but do not provide real-time phishing link analysis within SMS messages. Research in phishing detection has shown that machine learning models such as Logistic Regression, Random Forest, and Naive Bayes can effectively classify malicious URLs.

However, major gaps still remain in mobile-based real-time smishing detection, instant user alerts, and privacy-focused architecture.

III. Methodology

The proposed system, Securo, is designed to detect phishing links in SMS messages in real time. The application is developed using the Flutter framework for the frontend and Flask for the backend. Flutter provides a responsive and user-friendly mobile interface, while Flask handles backend processing and communication with the detection model, efficient performance and smooth data flow.

IV. System Architecture

The Securo system follows a modular architecture for real- time phishing detection in SMS messages. It consists of four main modules: SMS Rec eiver, URL Extractor, Detection Engine, and Alert System.

The SMS Receiver collects incoming messages, after which the URL Extractor identifies and extracts links from the message text. These links are then processed by the Detection Engine using rule-based analysis and machine learning techniques to classify them as Safe, Suspicious, or Phishing. Finally, the Alert System instantly notifies the user about the risk level of the detected link.

After initial screening, the extracted URL is passed to the Machine Learning Analysis Module, where classification algorithms analyze the link patterns and determine the probability of phishing. The Risk Classification Module categorizes the result as Safe, Suspicious, or Phishing.

Finally, the Alert Notification Module instantly displays a warning message to the user, helping prevent cyber fraud and data compromise.

V. Security Features

1. Real-Time SMS Monitoring – Continuously scans inncoming SMS messages for suspicious links.
2. URL Extraction & Analysis – Automatically extracts links and checks for malicious patterns.
3. Rule-Based Filtering – Detects shortened URLs, fake domains, and fraud keywords.
4. Machine Learning Detection – Classifies links as Safe, Suspicious, or Phishing

The proposed Securo system is equipped with multiple security features to protect users from SMS-based phishing attacks. It performs real-time monitoring of incoming SMS messages and automatically extracts any URLs present in the message content. These links are analyzed using rule-based filtering techniques, which check for suspicious keywords, fake domains, and shortened URLs. In addition, machine learning algorithms are used to classify the links as Safe, Suspicious, or Phishing. Based on the analysis, the system provides instant alerts and warning notifications to users, helping them avoid malicious links and improve mobile security.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435 (Online) Volume 15, Issue 04, April 2026)

VI. Results And Discussion

The implementation of Securo shows successful detection of phishing links in SMS messages in real time.

The system is able to accurately extract URLs from incoming messages and analyze them using rule-based and machine learning techniques. During initial testing, suspicious links were successfully classified as Safe, Suspicious, or Phishing, and instant alerts were generated for users. The integration of the Flutter frontend and Flask backend ensured smooth performance and quick response time. These results indicate that the proposed system can effectively improve mobile security and help protect users from smishing attacks.

VII. Conclusion

The proposed Securo system provides an effective solution for detecting phishing links in SMS messages in real time. By combining rule-based filtering with machine learning techniques, the system helps identify malicious links and instantly alerts users. This improves mobile security and protects users from smishing attacks, cyber fraud, and data theft. The initial results show that the system is reliable, user-friendly, and useful for enhancing smartphone security.

REFERENCES

SMS usage has increased rapidly, leading to a rise in smishing attacks. These attacks use malicious links to steal user data.

Existing systems lack real-time detection. Securo helps identify phishing links using smart techniques.

[1] Sahingoz, O. K., Buber, E., Demir, O., & Diri, B. “Machine learning based phishing detection from URLs.” Expert Systems with Applications, 2019. Saxe, J., & Berlin, K.

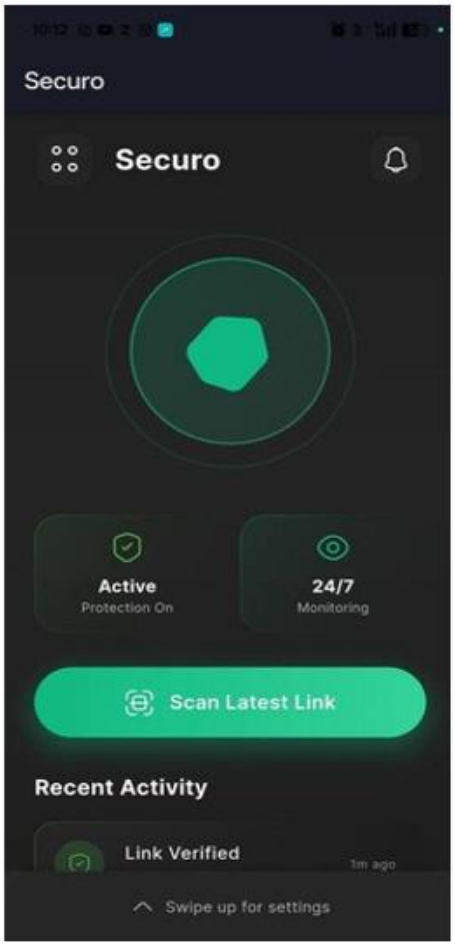
[2] Saxe, J., & Berlin, K.“eXpose: A Character-Level Convolutional Neural Network with Embeddings for Detecting Malicious URLs.” arXiv, 2017.

[3] Smadi, S., Aslam, N., & Zhang, L.“Detection of Online Phishing Email Using Dynamic Evolving Neural Network.”Expert Systems with Applications, 2018.

[4] Aleroud, A., & Zhou, L. “Phishing environments, techniques, and countermeasures: A survey.” Computers & Security, 2017.

[5] Gupta, B. B., Tewari, A., Jain, A. K., & Agrawal, D. P. “Fighting against phishing attacks: state of the art and future challenges.” Neural Computing and Applications, 2017.

[6] Almomani, A., Gupta, B. B., Atawneh, S., Meulenberg, A., & Almomani, E. “A survey of phishing email filtering techniques.” IEEE Communications Surveys & Tutorials, 2013.



International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435 (Online) Volume 15, Issue 04, April 2026)