SMS Phishing Analyzer Project

Project Name: SMS Phishing & Spam Detection System

Language: Java

Date: 14-Oct-2025

Prepared by: Heena Farheen Kolimi(CH.SC.U4CYS24026), A Salai Neranjana(CH.SC.U4CYS24032), Samridhi Rauthan(CH.SC.U4CYS24047)

# 1. Objective

The purpose of this project is to develop a Java application capable of analyzing SMS messages for potential phishing, spam, or malicious content. The system uses multiple analysis techniques, including keyword matching, link verification, and sender identification, to assign a risk score to each message and generate a detailed report.

# 2. System Overview

Functional Modules:

1. Keyword Analysis – Identifies suspicious words commonly found in spam or phishing messages.

2. Link Analysis – Detects URLs in SMS content and flags known suspicious domains.

3. Sender Analysis – Evaluates the sender’s ID for numeric or generic patterns indicative of spam.

4. Report Generation – Summarizes analysis results in TEXT, JSON, or CSV formats.

5. Encryption/Decryption – Optional Caesar cipher-based encryption for reports.

6. User Feedback – Allows end-users to provide feedback on the system’s assessment.

Class Hierarchy:

- SMSAnalyzer (Abstract Base Class) – Contains sender ID, message content, timestamp, and risk score. Enforces the analyze() method.

- KeywordMatcher – Checks for suspicious keywords.

- LinkAnalyzer – Extracts URLs and compares them with suspicious domains.

- SenderAnalyzer – Evaluates sender patterns.

- Reporter – Combines analyses, generates reports, and calculates final risk scores.

- EncryptionModule – Provides encryption/decryption.

- UserFeedback – Records user input.

# 3. Risk Scoring Logic

|  |  |  |
| --- | --- | --- |
| Component | Criteria | Score Contribution |
| Keywords | Number of suspicious words | 1 point per keyword |
| Links | Number of flagged URLs | 3 points per link |
| Sender | Numeric or generic sender ID | 2 points each |

Total Risk Classification:

- HIGH RISK: ≥ 7 points – Likely spam or phishing

- MEDIUM RISK: 4–6 points – Suspicious content

- LOW RISK: < 4 points – Likely legitimate

# 4. User Interaction / Menu Options

1. Create New Report

2. View Reports (TEXT, JSON, CSV)

3. Encrypt / Decrypt Reports

4. Save Reports to File

5. User Feedback

# 5. Sample SMS Analysis

Input:

- Sender: BANK

- Timestamp: 14-Oct-2025 10:30

- Message: 'Urgent! Verify your account now: https://fake-bank.com/login'

TEXT Report:  
=== SMS Security Report ===  
Sender: BANK  
Time: 14-Oct-2025 10:30  
Risk Score: 9  
Keyword Score: 3  
Link Score: 3  
Sender Score: 3  
Summary: Message from BANK scored 9 risk points. HIGH RISK - Likely spam/phishing.

JSON Report:  
{  
 "SenderID": "BANK",  
 "Timestamp": "14-Oct-2025 10:30",  
 "RiskScore": 9,  
 "ComponentScores": {  
 "Keyword": 3,  
 "Link": 3,  
 "Sender": 3  
 },  
 "Summary": "Message from BANK scored 9 risk points. HIGH RISK - Likely spam/phishing."  
}

CSV Report:  
SenderID,Timestamp,RiskScore,KeywordScore,LinkScore,SenderScore,Summary  
BANK,14-Oct-2025 10:30,9,3,3,3,"Message from BANK scored 9 risk points. HIGH RISK - Likely spam/phishing."

# 6. Conclusion

The SMS Analyzer system provides a comprehensive solution for detecting spam and phishing messages through multi-layered analysis. It supports reporting, encryption, and user feedback mechanisms to enhance reliability and usability.