**1.Paper: Rule Based Framework for detection of Smishing messages in Mobile Environment**

**Author: Ankit Kumar Jain, from the Department of Computer Engineering, National Institute of Technology.**

**Advantages:**

Utilizes rule-based classification algorithms for efficient detection.

Applies nine specific rules for identifying phishing attacks, enhancing precision.

Designed for mobile devices, addressing a critical security need.

**Disadvantages:**

Relies on predefined rules, which may not cover new or evolving phishing techniques.

Requires continuous updates and maintenance to remain effective against new threats.

**2.Paper:** Rule-Based Framework for Detection of Smishing Messages in Mobile Environment

**Author:** BB Gupta

**Advantages:**

Proposes a novel rule-based data mining classification technique for smishing detection.

Utilizes specific characteristics of smishing messages for effective filtering.

Demonstrates significant contributions to mobile security by effectively detecting threats.

**Disadvantages:**

Like most rule-based systems, may not adapt well to new or evolving smishing techniques.

Relies on continuous updates and maintenance to address new threats effectively

**3.Paper:** DSmishSMS-A System to Detect Smishing SMS

**Author:** Sandhya Mishra and Devpriya Soni, published in Springer in 2021:

**Advantages:**

Integrates a two-phase approach: Domain Checking and SMS Classification for comprehensive smishing detection.

Utilizes the Backpropagation Algorithm for efficient machine learning classification.

Employs heuristic analysis for detecting typical characteristics of smishing SMS, improving accuracy.

**Disadvantages:**

May require significant computational resources for real-time domain checking and classification.

Effectiveness heavily dependent on the constantly updated and accurate heuristic database to combat evolving smishing techniques.

**4.Paper:** Implementation of ‘Smishing Detector’: An Efficient Model for Smishing Detection Using Neural Network

**Author:** Sandhya Mishra and Devpriya Soni:

**Advantages:**

Utilizes a comprehensive approach combining Content Analyzer, URL Filter, and Source Code Analyzer Modules for detailed message scrutiny.

Employs Neural Networks, outperforming traditional machine learning models with a higher accuracy rate in smishing detection.

Leverages multiple features (URL, phone number, email ID, smishing keywords, and leet words) for robust feature analysis.

**Disadvantages:**

Neural network models require substantial computational resources for training and inference, which might limit deployment in resource-constrained environments.

Relies on an extensive and up-to-date dataset for training to maintain high detection rates, which may involve continuous data collection and labeling efforts.

**5.Paper:** Detecting Phishing SMS Based on Multiple Correlation Algorithms

**Author:** Gunikhan Sonowal, published in Springer in 2020:

**Advantages:**

High Accuracy: The method achieves a high accuracy rate (98.40% with Kendall rank correlation) in detecting smishing messages, which is crucial for effectively identifying and preventing phishing attacks.

Feature Reduction: Utilizing correlation algorithms for feature ranking significantly reduces the dimensionality of the feature set (by 61.53% with Kendall rank correlation), making the model more efficient without sacrificing performance.

**Disadvantages:**

Complexity: The multi-step process, including feature collection, feature ranking, and feature selection, can be complex and time-consuming, which may pose challenges for real-time applications.

Data Dependency: The effectiveness of the model might be highly dependent on the quality and variety of the data used for training, which can limit its applicability in different contexts or languages.

**6.Paper:** SMS Spam Detection and Classification to Combat Abuse in Telephone Networks Using Natural Language Processing

**Author:** Dare Azeez Oyeyemi and Adebola K. Ojo:

**Advantages:**

High Accuracy and Speed: The integration of BERT with Naïve Bayes classifier achieved a high accuracy of 97.31% with a rapid execution time of 0.3 seconds, indicating a significant improvement in both efficiency and classification performance.

Reduction in False Positives: The approach addresses the common issue of high false positives in spam detection, thus reducing unwarranted blocking of legitimate messages.

**Disadvantages:**

Complexity and Resource Intensiveness: BERT and other deep learning models require significant computational resources for training and inference, which may not be accessible to all users or applicable in all environments.

Overfitting Potential: Despite efforts to create a comprehensive dataset, the risk of overfitting still exists, particularly if the model is exposed to a narrow range of message types.

Data Privacy Concerns

**7.Paper:** SmishSMS- The Latest Detection of SMS Phishing Trends

**Author:** Anisha Asirvatham, Dr.C.Meenakshi

**Advantages:**

Addresses a prevalent form of fraud causing significant financial losses.

Utilizes a comprehensive approach analyzing SMS content, checking domains and contacts, and identifying sources.

Employs machine learning models for spam detection with high accuracy.

**Disadvantages:**

Lacks a publicly available benchmark dataset for smishing messages, complicating validation efforts.

Source identification accuracy is relatively low (35%), indicating room for improvement.

The reliance on manual filtering to separate smishing messages from general spam may introduce bias or errors.

**8.Paper:SMS Spam Classification–Simple Deep Learning Models With Higher Accuracy Using BUNOW And GloVe Word Embedding**

**Author:** Surajit Giri, Sayak Das, Sutirtha Bharati Das, and Siddhartha Banerjee

**Advantages:**

High Accuracy: Achieves up to 99.46% accuracy, demonstrating effectiveness in spam detection.

Effective Word Embedding: Utilizes BUNOW and GloVe for improved text representation and context understanding.

Versatile Models: Proposes both CNN and CNN-LSTM models, offering flexibility based on application needs.

**Disadvantages:**

Complexity for Real-Time Application: Deep learning models may be computationally intensive for real-time spam detection.

Dataset Dependency: Performance might vary significantly with different datasets or languages.

Overfitting Risk: High accuracy could lead to overfitting, especially with very specific datasets.

**9.Paper: SMS Spam Detection Using Machine Learning, Flask and Flutter**

**Author:** Akshay Sable, Nilesh Urkude, Vaibhav Bhade, Shubham Dongare, Chetan Morey

**Advantages:**

High accuracy in separating ham and spam messages.

Effective in high-dimensional spaces and with clear margin of separation.

Relatively memory efficient.

**Disadvantages:**

Requires thorough parameter tuning.

High memory requirement as it stores all training data.

Requires a large amount of data to perform well.

**10.Paper: SMS Spam Detection using Relevance Vector Machine**

**Author:** Shushanta Pudasaini, Aman Shakya, Sanjeeb Prasad Pandey

From ELSEIVER

**Advantages:**

Combines the strengths of multiple models to enhance prediction accuracy.

Useful for telecom providers to identify spam sources without infringing on privacy.

Utilizes algorithms like SVM, NB, KNN, logistic regression, and Winnow for spam detection based on message content.

**Disadvantages:**

May inadvertently remove important content, impacting the model's ability to correctly classify messages.

Requires careful tuning to avoid negatively impacting the classification performance.

**11.Paper: A deep learning method for automatic SMS spam classification: Performance of learning algorithms on indigenous dataset**

**Author: Olusola Oluwakemi Abayomi-Alli, Sanjay Misra, Abayomi-Alli Adebayo**

**From Research Gate, Wiley**

**Advantages:**

BiLSTM outperforms traditional ML classifiers in accuracy, precision, recall, and F-measure.

Demonstrates improved classification accuracy and reduced computational time compared to other ML classifiers.

Provides effective sequence processing in both directions due to its bidirectional structure.

**Disadvantages:**

Limited by the datasets available and high preprocessing time.

Requires fine-tuning of parameters for optimal performance​.

**12.Paper: SMS Phishing and Mitigation Approaches**

**Author: Sandhya Mishra, Devpriya Soni**

**Advantages:**

Reduces the risk of smishing by ensuring apps are safe and verified.

Decreases the likelihood of falling for smishing by avoiding suspicious links in SMS.

Provides an additional layer of security by warning users about malicious sites.

**Disadvantages:**

Users may find it restrictive and may not always distinguish between authorized and unauthorized apps.

Inconvenient for users; requires extra steps to verify website authenticity.

Cannot block new, unknown sources; requires constant updates.