IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 1, June 2025
Impact Factor: 7.67

ML-Based Classification of Malicious and Legitimate Messages

Dr. Rachana P, Akash Pujari, Surabhi, Asha H. D, Guruprasad
Department of Information Science and Engineering
Alvas Institute of Engineering and Technology, Mijar, Mangalore, India

Abstract: *The fact that SMS spam is still a major problem highlights the need for study into creating systems that may thwart the evasive tactics utilized by spammers. Protecting the public from the negative impacts of SMS spam requires this kind of study. The main obstacles in the existing SMS spam detection and filtering environment are highlighted in this study. We present a new SMS dataset with around 68,000 messages, 39% of which are classified as spam and 61% as valid (ham) in order to aid study in this field. Notably, this dataset which has been made freely available for research purposes represents the biggest dataset of SMS spam that has been made available thus far. To investigate how spam strategies have changed over time, we do a longitudinal analysis. Furthermore, in order to assess and contrast the effectiveness of various SMS spam detection models—from conventional shallow machine learning techniques to sophisticated deep neural networks we extract both semantic and syntactic data. Our study evaluates how effectively these models and well-known commercial antispam services withstand typical spammer evasion techniques. The findings show that most shallow learning methods and existing anti-spam programs have trouble correctly identifying spam communications, particularly when confronted with complex obfuscation techniques.*

Keywords: detection of SMS spam, anti-spam services, evasive tactics, robustness study of machine learning, spamdataset, and development of SMS spam

DOI: 10.48175/IJARSCT-27305