IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 8, March 2025

Intelligent Machine Learning Algorithms for Reliable Phishing URL Identification: Review

Sonali Dawange[1] and Dr. Prashant Yawalkar[2]
Student, MET's Institute of Engineering, Bhujbal Knowledge City, Nashik[1]
Associate Professor, MET's Institute of Engineering, Bhujbal Knowledge City, Nashik[2]
sonaliwaje91@gmail.com

Abstract: *Phishing attacks continue to pose a significant threat to cybersecurity, with attackers using deceptive techniques to lure unsuspecting users into divulging sensitive information such as login credentials, financial details, and personal data. As the volume and sophistication of phishing attacks increase, there is a growing need for effective detection mechanisms to thwart these malicious activities. Machine learning (ML) has emerged as a promising approach for detecting phishing URLs due to its ability to analyze large datasets and identify patterns indicative of malicious intent. This study presents a comprehensive literature review focusing on the methodologies employed in detecting phishing URLs using ML models. The review encompasses various ML techniques such as supervised learning, unsupervised learning, and deep learning, highlighting their strengths and limitations in the context of phishing URL detection. Additionally, the study explores the challenges faced in this domain, feature extraction techniques, and the dynamic nature of phishing attacks. Furthermore, the study examines the types of features commonly used in ML-based phishing URL detection, such as lexical features (e.g., URL length, domain age), content-based features (e.g., presence of keywords), and structural features (e.g., URL hierarchy). The analysis considers the relevance of these features in differentiating between legitimate and malicious URLs and discusses strategies for feature selection and extraction. This research provides valuable insights into the state-of-the-art methodologies, technologies, features, and datasets in ML-based phishing URL detection.*

Keywords: phishing URL detection, machine learning models, detection technologies, feature selection, datasets, cybersecurity defenses, malicious intent

ISSN 2581-9429 IJARSCT

DOI: 10.48175/IJARSCT-24519