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 12, April 2025
Impact Factor: 7.67

A Review on Phishing Detection using AI and ML

Prof. Pratiksha Prakash Pansare[1], Lokhande Ritesh Motiram[2], Thakre Prathmesh Sanjay[2], Zolekar Avishkar Bharat[2]

[1] Assistant Professor, [2]Students, Department of Computer Engineering,
Samarth College of Engineering and Management, Belhe, Junnar, Pune, Maharashtra, India

Abstract: *Phishing websites are a major threat to online security, aiming to deceive users into revealing confidential information by imitating legitimate websites. Detecting such fraudulent websites is crucial to safeguarding users from potential harm. This paper proposes an intelligent model for detecting phishing websites based on Extreme Learning Machine (ELM). Phishing websites exhibit various distinguishing features, and therefore, detecting them requires an appropriate set of URL features. Our model employs machine learning techniques to classify web pages as phishing or legitimate, utilizing a dataset containing phishing and legitimate URLs. The methodology involves preprocessing a dataset of URLs, followed by the extraction of features from four key categories: domain-based, address-based, abnormal behavior-based, and HTML/JavaScript-based features. These features are processed to generate values for each URL attribute, which are then analyzed using machine learning algorithms, including ELM, Random Forest, and Support Vector Machines (SVM). The system computes range and threshold values for URL attributes to aid in classification..*

Keywords: Phishing detection, Extreme Learning Machine (ELM), Machine learning, URL feature extraction, Phishing websites, Legitimate websites, Web security, Phishing classification

DOI: 10.48175/IJARSCT-25950