Chapter 10
Benchmarking Traditional ML Approaches in Phishing URL Detection

T. S. Sangeetha
http://orcid.org/0009-0008-9723-7819
College of Engineering, Thiruvananthapuram, India

G. L. Swathi Mirthika
http://orcid.org/0000-0002-4591-7811
SRM Institute of Science and Technology, India

Keerthi Jayan
http://orcid.org/0000-0002-3668-8500
SRM Institute of Science and Technology, Kattankulathur, India

Nisha Thorakkattu Thorakattil Madathil
http://orcid.org/0000-0002-4074-4421
UAE University, UAE

Sreya John
http://orcid.org/0000-0002-7700-0602
Kristu Jayanti University, India

K. S. Jishnu
http://orcid.org/0000-0003-2667-4858
SRM Institute of Science and Technology, Kattankulathur, India

D. Vetriselvi
SRM Institute of Science and Technology, India

ABSTRACT

Phishing attacks continue to pose a major cybersecurity challenge by exploiting deceptive URLs to obtain sensitive information. Although deep learning approaches such as CNNs, RNNs, and Transformers have demonstrated state of the art detection performance, traditional machine learning classifiers remain widely utilized because of their efficiency,interpretability, and relatively low resource requirements. In this study, we implement and evaluate ten machine learning models including Logistic Regression, Gradient Boosting, CatBoost, XGBoost, and Multi-Layer Perceptron on

DOI: 10.4018/979-8-3373-6786-6.ch010

a publicly available phishing URL dataset from Kaggle. Experimental results show that ensemble based models,particularly XGBoost and Random Forest, achieve the highest accuracy, while Logistic Regression offers competitive performance with the advantages of simplicity, interpretability, and low computational overhead. The findings highlight the tradeoffs between accuracy, interpretability, and computational cost,providing practical guidance for selecting appropriate models in real world phishing detection systems.

I. INTRODUCTION

While the rapid development of the Internet and online services has opened up new avenues for communication, business, and information sharing, it has simultaneously provided an arena for cyber threats, among which one of the most prominent and dangerous includes phishing(A. Ashok et al., 2024) . In general, phishing is a type of cybercrime characterized by attempts to make users reveal their login credentials, financial data, or personal information through fake websites or devious links. According to different reports provided by leading cybersecurity organizations, phishing is the top way of conducting social engineering attacks and accounts for a substantial portion of data breaches happening around the world. The low cost of initiating phishing campaigns and the high success rate thereof render this attack strategy a lasting challenge (T. Kumaresan et al.,2025).

Among different phishing detection approaches, the analysis of Uniform Resource Locators is one of the best methods (S. Uplenchwar et al.,2022). Most phishing URLs mimic legitimate websites by adding extra subdomains, inserting typographical errors, or encoded characters similar to the trusted domains. The traditional defenses based on blacklists and rule-based systems cannot detect new or unknown phishing URLs being generated each day (A. Khan et al.,2025). This has motivated the application of machine learning techniques that can automatically learn patterns distinguishing phishing from legitimate URLs. In recent years, deep learning and traditional machine learning have been adopted for phishing detection. Deep learning models, including Convolutional Neural Networks, Recurrent Neural Networks, and Transformers, have achieved high accuracy by extracting features automatically from raw URLs. However, they require considerable computational resources, large training datasets, are complicated to interpret, and hence less practical in resource-constrained environments. On the other hand, conventional machine learning models such as Logistic Regression, K Nearest Neighbors, Support Vector Machine, Decision Tree, Random Forest, and boosting-based methods provide competitive performance with lower resource requirements and greater interpretability. Of these, ensemble learning