Deep Learning Based Phishing Websites Detection

Vaibhav Handge¹, Shubham Pokale², Saurabh Lavhate³, Shubham Nalkol⁴, Prof G. B. Kote⁵
Students, Department of Computer Engineering¹,²,³,⁴
Guide, Department of Computer Engineering⁵
Pravara Rural Engineering College, Loni, Maharashtra, India

Abstract: Phishing is a crime that involves the theft of confidential user information. Those targeted by phishing websites include individuals, small businesses, cloud storage providers, and government organisations and websites. The majority of phishing prevention techniques involve hardware-based solutions, although software-based options are preferred due of cost and operational considerations. There is no answer to the problem of zero-day phishing assaults from the present phishing detection approaches since there is no solution to the problem. The Phishing Attack Detector based on Web Crawler, a three-phase attack detection system, was designed to handle these issues and accurately detect phishing incidences using a recurrent neural network in order to resolve these issues. It covers the input aspects of web traffic, web content, and Uniform Resource Locator (URL) based on the classification of phishing and non-phishing pages, as well as the output features of phishing and non-phishing pages.

Keywords: Recurrent Neural Network, Deep Learning, illegitimate URLs, cyber attacks

REFERENCES
[2]. Jian Mao, Wenqian Tian, Pei Li, Tao Wei, Zhenkai Liang, “Phishing-Alarm: Robust and Efficient Phishing Detection via Page Component Similarity”.