IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, November 2024

Illegitimate Websites Detection Using Deep Learning Framework

Dr. P. C. Latane[1] Vikas Ramdas Takale[2], Prathamesh Kailas Shirke[3], Mugdha Govardhan Khobare[4]
Department of Information Technology[1-4]
Sinhgad Institute of Technology, Lonavala, Maharashtra, India

Abstract: *Phishing is a crime involving robbery of confidential user data. The phishing websites are aimed at individuals, businesses, and cloud storage and government websites. Hardware- based anti-phishing methods are generally used, but software- based approaches are favored because of costs and operational factors. There is no solution to the problem such as zero-day phishing attacks from current phishing detection approaches. A three-phase attack detection called the Phishing Attack Detector based on Web Crawler was proposed to resolve these problems and precisely detect phishing incidences using recurrent neural network. It includes the input features Web traffic, web content and Uniform Resource Locator (URL) based on the classification of phishing and non-phishing pages.*

Keywords: Recurrent Neural Network, Deep Learning, illegitimate URLs, cyberattacks

DOI: 10.48175/IJARSCT-22156