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 5, May 2024

PHISHWIPER: Real Time Scam Website Detection and Blocking using Predictive Attention Model

M. K. Siva Prakash[1] and A. Poongodi[2]

PG Student, Department of Computer Applications[1]

Professor, Department of Computer Applications[2]

Vels Institute of Science Technology and Advanced Studies, Pallavaram, Chennai, India

mgmsivaprakash @vistas.ac.in and poongodimca1979@gmail.com

Abstract: *A data breach is a security event, where sensitive data is accessed without any permission from a website or an organization. An information breach will be considered as the purposeful or accidental gathering of secure or personal data from an organization. A breach can be an accession of a data without any permission, these kinds of regulations should be provided with safe and secured framework but this is not happening in many corporations. So, by analyzing the previous attempts (successful or unsuccessful attacks), the proposed model can be trained to adapt to new scenarios and predict the next breach. Further, this research work has designed a model by using machine learning to defend a website from security breaches. The primary aim of this research work is to create a machine learning model, which trains in Real-time and monitors the website or a system and trains from the state-of-art attacks. The proposed model has created a web application, which takes the data from multiple sources such as Amazon, Flipkart, Snapdeal, and Shop clues, which shows the data that is safe to obtain from the website.*

Keywords: Data breach, personal data, Real time, state-of-art attacks, framework

Copyright to IJARSCT
www.ijarsct.co.in

DOI: 10.48175/IJARSCT-18413

ISSN 2581-9429 IJARSCT