IJARSCT

ISSN (Online) 2581-9429

IJARSCT

Impact Factor: 7.301

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

Volume 3, Issue 3, April 2023

Suspicious Link Detection using AI

Prof. Amar Palwankar[1], Afiya Borkar[2], Pranali Shingare[3], Rifah Solkar[4], Shreya Khedaskar[5]

Assistant Professor, Department of Information Technology[1]

Students, Department of Information Technology[2,3,4,5]

Finolex Academy of Management and Technology, Ratnagiri, Maharashtra, India

Abstract: *With the increase in internet usage, cybersecurity has become a major concern for computer systems, as malicious URLs can release different forms of malware and attempt to collect user data. The global lockdown in 2020 led to a significant rise in the use of internet services for business, which in turn resulted in a surge of cybercrimes committed by cybercriminals and significant data losses for businesses. To prevent such attacks, it is important to identify malicious URLs and understand the types of threats they pose. Signature-based approaches are often used to find such websites, and security tools are deployed to impose access restrictions on them. This chapter proposes using the linguistic aspects of related URLs to enhance the effectiveness of classifiers for identifying dangerous websites through Machine Learning algorithms such as Logistic Regression and Random Forest Technique. The study shows that being able to identify spam URLs solely based on URLs and categorizing them without relying on page content can lead to significant resource savings and a safer browsing experience for users.*

Keywords: Suspicious URL Detection, Machine Learning, Supervised Learning, Logistic Regression, Random Forest ,Cybersecurity.

REFERENCES

[1]. Mohammed Alsaedi, Fuad A. Ghaleb, Faisal Saeed, Jawad Ahmad_(2022) Cyber Threat Intelligence-Based Malicious URL Detection Model Using Ensemble Learning. International article in (Sensors 2022, 22, 3373.https://doi.org/10.3390/s22093373).

[2]. Shantanu, Janet B, Joshua Arul Kumar R_(2021) Malicious URL Detection. (International Conference on Artificial Intelligence and Smart Systems (ICAIS) | 978-1-7281- 9537-7/20/ ©2021 IEEE).

[3]. Zhiqiang Wang, Xiaorui Ren, Shuhao Li, Bingyan Wang, Jianyi Zhang, Tao Yang_(2021) A Malicious URL Detection Model Based on Convolutional Neural Network. (Hindawi Security and Communication Networks Volume 2021, Article ID 5518528, https://doi.org/10.1155/2021/5518528).

[4]. Jino S Ganesh, Niranjan Swarup.V, Madhan Kumar.R, Harinisree.A and Dr. Giri Raj.M_(2020) Machine Learning based Malicious Website Detection. (International Journal of Scientific & Engineering Research Volume 11, Issue 7, July-2020).

[5]. Doyen Sahoo, Chenghao Liu, Steven C.H. Hoi_(2019) Malicious URL Detection using Machine Learning: A Survey International article (Vol. 1 August 2019, https://doi.org/10.1145/nnnnnnn.nnnnnnn).

[6]. Ayon Gupta, Sanghamitra Giri, R. Naresh_(2020) Malicious URL Detection System using combined SVM and Logistic Regression Model. (International Journal of Advanced Research in Engineering and Technology, JARET Volume 11, Issue 4, April 2020).

[7]. Cho Do Xuan, Hoa Dinh Nguyen_(2020) Malicious URL Detection based on Machine Learning. (IJACSA International Journal of Advanced Computer Science and Applications, Vol. 11, No. 1, 2020).

[8]. Mr. Ferhat Ozgur Catak professor of University of Stavenger, Ms. KevserSahinbas from Istanbul Medipol University and Mr. Volka Dortkardes from Turkey_(2020) (USA by IGI Global Engineering Science Reference).

DOI: 10.48175/IJARSCT-9171