MALIGNANT URL DETECTION USING MACHINE LEARNING TECHNIQUES

124003018 : Ajay N
124003396 : Sathya Prakash S
124003209 : Suraaj Vikas Raju PA

Abstract

A malicious URL is a web address created with the purpose of promoting scams, attacks, and frauds. When clicked on, malicious URLs can download ransomware, lead to phishing or spear phishing emails, or cause other forms of cybercrime. Malicious URLs are often disguised and easy to miss, making them a serious threat to the digital world. Creating and spreading malicious URLs and domain names through popups, email, messages etc. is an advanced cyber-attack technique used by hackers and cyber criminals.
The main intentions of such attacks could be to carry out phishing attacks to gain access to users' personal information to carry out identity theft or other types of fraud, gain access to users' login credentials to gain access to their personal or professional accounts, to trick users into downloading malicious software that cybercriminals can use to spy on victims or take over their devices or to get into victims' computers to encrypt their files for a ransomware attack.

It is mandatory to reconcile the system to detect malicious URLs and prevent attacks. In this Project, Machine learning based models like Logistic Regression, K-Nearest Neighbors, Naive Bayes, Random Forest and Support Vector Classification are used in the detection and classification of three kinds of malicious URLs namely phishing, spam and malware.

References:

Base paper (sciencedirect.com site link)
https://www.sciencedirect.com/science/article/pii/S2214785321028947

Base paper (PDF)
https://drive.google.com/file/d/1WSr-JKkoVM4vQ-bTBSaAdodt88PRT3Um/view?usp=share_link

Base paper authors : Saleem Raja A, Vinodini R, Kavitha A
Base paper volume : ScienceDirect (materialstoday proceedings, vol. 47 part 1)
Base paper year of publication : 2021

Guide Name:
Dr. Priyadarsini PLK