Detecting Malicious URLs Using Machine Learning Techniques

Abstract:

The digital landscape has seen significant advancements, particularly online, where many activities now take place. However, the increasing creativity of cyber attacks poses a growing risk, with malicious URLs being a major threat. These URLs aim to deceive inexperienced users and extract unauthorized information, leading to system compromise and substantial financial losses. Therefore, the need for website security is paramount. This paper provides a comprehensive literature review, focusing on machine-learning based techniques for detecting malicious URLs, while addressing existing limitations, detection technologies, feature types, and datasets. Additionally, it emphasizes the security of research on detecting malicious Arabic websites and suggests future research directions. Lastly, the paper identifies challenges in malicious URL detection and proposes potential solutions.

Motivation:

The motivation behind choosing this paper is that the paper mainly focused on addressing the increasing threats posed by malicious URLs and the need for advanced techniques to detect and mitigate these threats. Additionally, this paper aims to draw attention to lack of research in the context of detecting malicious Arabic websites, encouraging further exploration in this area.

References:

[1] https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9950508