BTP Proposal

Patel Shahil Manishbhai - 200010039

Abstract:

In the combat against phishing attacks, a pervasive threat that targets web users to elicit sensitive information, numerous strategies for phishing attack detection have been advanced. With the evolution of attackers employing novel tactics to circumvent existing detection mechanisms, researchers have increasingly turned to the integration of machine learning and deep learning techniques. Deep learning, in particular, plays a crucial role in scrutinizing the visual aspects of websites, which malicious actors exploit to deceive users into revealing sensitive information. This research project focuses on applying deep learning techniques to classify websites as phishing or legitimate. Additionally, it aims to provide comprehensive insights into categorizing websites as either phishing or legitimate, thus serving as an educational resource for users to enhance their awareness of phishing vulnerabilities. The methodology employed encompasses the examination of favicon similarity between suspicious websites and well-established legitimate websites. The presence of input fields, essential for gathering sensitive data, is identified through screenshot processing. Subsequently, text extraction from the screenshot generates a search query for a search engine. The domain of the suspicious website is then scrutinized within the top 3 results retrieved from the search engine for presence verification. A weighted average scoring system is implemented to evaluate these key features individually, ultimately facilitating categorizing websites as either phishing or legitimate. This multifaceted approach effectively enhances web security and user awareness in the face of ever-evolving phishing threats.