Madhusanka D.N.V

242/B Wanabada Kanda,

Udumalagala, Nakiyadeniya.

28/05/2023

Title of Invention: Malicious Website Detection Chrome Extension Using Machine Learning

Abstract:

This patent application presents a novel system for detecting malicious websites using machine learning techniques. The system leverages advanced algorithms and features to accurately identify and classify potentially harmful online resources, enhancing cybersecurity measures. By utilizing the OWASP framework, the system performs comprehensive audits and provides actionable recommendations for addressing identified vulnerabilities, ensuring a secure online environment.

Background:

With the increasing number of cybersecurity threats and malicious activities on the internet, it is crucial to develop efficient methods for detecting and mitigating potential risks. Conventional approaches to malicious website detection often lack accuracy and fail to adapt to evolving threats. Therefore, there is a need for an innovative solution that harnesses the power of machine learning to identify and combat malicious websites effectively.

Summary of Invention:

The Malicious Website Detection System is a machine learning-based solution that analyzes various website attributes, network behaviors, and content patterns to identify potential vulnerabilities and malicious activities. The system utilizes a curated dataset comprising known malicious and benign websites to train a machine learning model, enabling it to accurately classify new websites based on learned patterns.

Detailed Description:

The system consists of several modules, including data collection, feature extraction, model training, and vulnerability analysis. The data collection module gathers website data, including URL, HTML content, domain reputation, and network traffic logs. The feature extraction module extracts relevant features from the collected data, such as URL structure, SSL certificates, code patterns, and server responses. The model training module utilizes machine learning algorithms, such as decision trees or neural networks, to train a robust and accurate classification model. The model learns from the curated dataset, identifying patterns and

correlations between website attributes and malicious behaviour. This trained model forms the basis for classifying new websites as either malicious or benign.

The vulnerability analysis module performs a comprehensive assessment of identified malicious websites, applying the OWASP framework to identify specific security vulnerabilities and weaknesses. The system generates detailed audit reports, highlighting the detected vulnerabilities and providing actionable recommendations for remediation.

Advantages:

The Malicious Website Detection System offers several advantages over traditional approaches. By leveraging machine learning algorithms, the system achieves high accuracy in detecting malicious websites, minimizing false positives and false negatives. The integration of the OWASP framework ensures comprehensive vulnerability assessment, aiding in the identification and remediation of potential security risks. The system's automation and scalability enable efficient analysis of a large number of websites, enhancing the overall cybersecurity posture.

Patentability:

The present invention is novel as it introduces a unique approach to malicious website detection using machine learning techniques and the application of the OWASP framework. The combination of data collection, feature extraction, model training, and vulnerability analysis modules provides a comprehensive solution for identifying and addressing security vulnerabilities in websites. This inventive integration sets the system apart from existing solutions, warranting patent protection.

Conclusion:

The Malicious Website Detection System utilizing machine learning techniques and the OWASP framework represents a significant advancement in the field of cybersecurity. The integration of innovative algorithms, comprehensive feature analysis, and vulnerability assessment ensures accurate detection and effective mitigation of malicious websites. By filing this patent application, we seek to protect our intellectual property and establish exclusivity for this inventive solution.

Signature:

(Madhusanka D.N.V)