Create an intelligent system using AI/ML to detect phishing domains which imitate look and feel of genuine domains

Abstract :

Phishing attacks, which involve deceptive attempts to steal sensitive information such as login credentials and financial data, continue to pose a significant threat to online security. Phishing URLs serve as a primary vector for these attacks, making their detection a critical cybersecurity task.The system leverages cutting-edge AI/ML techniques to analyse various aspects of domain characteristics, content, and user behaviour patterns. It employs feature engineering, natural language processing, and deep learning algorithms to identify subtle nuances in website structure and content that distinguish phishing domains from genuine ones. By incorporating real-time data feeds and continuously learning from evolving threats, this system adapts to new phishing techniques and ensures robust detection capabilities.

Proposed Solution:

AI Agent is developed to enhance user safety and privacy during internet browsing. This AI Agent is designed to monitor users' browsing activities, analyze URLs in real-time, and provide cautionary messages through a browser plugin whenever it detects potentially malicious or harmful websites. And the system includes a complementary web application for in-depth analysis of past attacks and reports user and database can be connected to check newly registered domains.

Features:

The AI Agent continuously scans and analyses URLs accessed by users during their web browsing sessions. It employs advanced machine learning algorithms to assess the safety and trustworthiness of each website.

When the AI Agent detects a URL that raises red flags, it instantly communicates with a browser plugin. The plugin then displays a cautionary message to the user, warning them of potential security risks associated with the accessed website.

The accompanying web application serves as a central hub for analysing past attacks and incidents. Users can access detailed reports and insights into the AI Agent's historical threat assessments.

The system encourages user feedback to improve its accuracy and effectiveness. Users can report false positives and false negatives, helping the AI Agent fine-tune its algorithms.

The AI Agent and web application prioritise user privacy and data security. Personal information is protected, and user data is anonymized to ensure confidentiality.

The AI Agent's machine learning models are regularly updated to adapt to emerging threats and evolving attack techniques, ensuring it remains effective in protecting users.

This AI Agent and its accompanying web application provide a robust solution for enhancing user security during web browsing while also offering insights into the evolving threat landscape. By combining real-time URL analysis with historical attack data, it empowers users to make informed decisions and stay one step ahead of online threats