**Phishing URL Classification Using Machine Learning**

**Abstract:**

The exponential growth of digital world providing great opportunities for both positive advancements and malicious activities. While the internet facilitates seamless communication, collaboration, and innovation, it has also become a breeding ground for cyber threats, with phishing attacks being a prominent concern. Phishing, a deceptive practice where attackers masquerade as trustworthy entities to trick individuals into revealing sensitive information, poses a significant risk to online security.

In response to the ever-evolving landscape of cyber threats, this project introduces a cutting-edge approach to identify phishing attack URLs using machine learning. Leveraging the power of machine learning, the proposing Phishing URL Classification System aims to dynamically adapt to the latest tactics employed by malicious actors. By extracting and analyzing a diverse range of features from URLs, including lexical, structural, and content-based attributes, the system enhances its ability to distinguish between legitimate and phishing URLs. I am working to train the Machine Learning model over 5,49,346 distinct URLs to make the system more accurate.

Submitted By,

SHAIK SUBHAN SAHEB

20A81A05I3