**ABSTRACT**

Phishing attacks pose a significant threat in today's digital landscape, resulting in substantial financial losses and the compromise of sensitive personal information. To address this issue, this project proposes a deep learning-based system for detecting phishing websites with high accuracy. The system is integrated into a user-friendly web application, allowing users to paste URLs and receive instant feedback on the authenticity of the site.

The detection mechanism combines Convolutional Neural Networks (CNN) and Bidirectional Long Short-Term Memory (BiLSTM) networks within a meta-learning framework. The CNN component is designed to automatically extract spatial features from the website content and structure, while the BiLSTM network captures sequential patterns in the URLs and associated textual data, incorporating bidirectional context for enhanced feature understanding. The meta-learning approach, specifically employing the Reptile algorithm, enables the system to generalize effectively across diverse phishing attack scenarios by adapting quickly to new patterns with minimal data.

This hybrid CNN-BiLSTM model, enhanced with meta-learning, is evaluated on a comprehensive dataset of phishing and legitimate URLs. The results demonstrate that this advanced approach achieves superior accuracy and robustness compared to traditional methods and standalone deep learning models. The system's scalability and adaptability make it an effective solution for real-world cybersecurity challenges. By providing a reliable and accessible tool for identifying and mitigating phishing attacks, this project aims to enhance user security and contribute to broader efforts in combating cyber threats.