DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

MAJOR PROJECT-ACADEMIC YEAR 2023-2024

PROJECT TITLE: DETECTION OF PHISHING WEBSITES USING MACHINE LEARNING

Group Members:

S. No	Roll No.	Name
1	20EG105120	K. VAISHNAVI
2	20EG105139	P. SHILPA
3	20EG105143	S. NAVEEN
4	20EG105718	CH. UDAY GOUD

Project Guide	Dr. K. SHAILAJA

Signature of Guide

Abstract:

In today's world of widespread internet use, the rise of cyber threats, especially phishing attacks, is a big worry. Phishing is when someone tries to trick you into sharing private info like usernames, passwords, or financial details by pretending to be someone you trust. This poses a serious risk for both individuals and organizations.

This project introduces a smart way to quickly find and stop phishing websites using machine learning. We use a mix of different examples of phishing in our training data to make our system smart. The system uses advanced computer algorithms, like decision trees and neural networks, to learn and spot subtle signs that show if a website is trying to trick you.

We carefully design the system to tell the difference between real and fake websites by looking at things like what the website says and how it behaves. We then test it thoroughly, including in real-world situations, to make sure it works well and can handle different challenges.

Our research is part of the ongoing efforts to make online activities safer. By using machine learning, we aim to stay a step ahead of cybercriminals, making it harder for them to fool people online and helping to keep users safe from tricky online schemes.

Problem Statement:

With the increasing prevalence of online activities, there has been a significant rise in cyber threats, particularly phishing attacks. Phishing websites attempt to deceive users by mimicking legitimate websites to steal sensitive information such as login credentials, personal details, and financial data. Traditional methods of detecting phishing websites are often reactive and lag behind the evolving tactics of cybercriminals. Therefore, there is a pressing need for a proactive and automated approach to identify and mitigate phishing threats.

Problem Domain Analysis: Python, Machine Learning

References:

[1]. Alswailem, A., Alabdullah, B., Alrumayh, N., & Alsedrani, A. (2019). Detecting Phishing Websites Using Machine Learning. 2019 2nd

International Conference on Computer Applications & Information Security (ICCAIS).

[2]. Razaque, A., Frej, M. B. H., Sabyrov, D., Shaikhyn, A., Amsaad, F., & Oun, A. (2020). Detection of Phishing Websites using Machine Learning. 2020 *IEEE* Cloud Summit.

[3]. Alkawaz, M. H., Steven, S. J., & Hajamydeen, A. I. (2020). Detecting Phishing Website Using Machine Learning. 2020 16th IEEE International Colloquium on Signal Processing & Its Applications (CSPA).

[4]. Patil, V., Thakkar, P., Shah, C., Bhat, T., & Godse, S. P. (2018). Detection and Prevention of Phishing Websites Using Machine Learning Approach. 2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA).