NAME: MAGDALENA ISAYA MAKWETA
REG NO: RU/BCS/2023/189

Title:
A Machine Learning Approach to Detect Phishing Websites
Author: Mohammad S. Shahraki et al.

Summary of the Introduction.
Phishing attacks are becoming more frequent and dangerous. Traditional anti-phishing methods like blacklists and user reports are reactive and fail to detect newly created phishing websites. The paper introduces a machine learning-based approach that analyzes website features to identify phishing attempts more accurately and in real-time.

Problem Statement.
Existing systems struggle to detect unknown or rapidly changing phishing websites. This gap makes users vulnerable to attacks. There is a clear need for smarter, adaptive systems capable of detecting threats as they emerge using intelligent analysis.

Objectives.
- To develop a machine learning model for phishing website detection.
- To evaluate and compare different ML algorithms for accuracy.
- To reduce false positives and ensure real-time threat identification.

Research Gap.
Most current phishing detection tools are dependent on static methods like blacklists or rule-based filters, which cannot detect newly emerging threats. The paper addresses this gap by introducing a proactive, learning-based method that adapts over time using data patterns.