Comparison: Expert Systems With Applications (Phishing Paper) vs. PhishGuard AI Chrome Extension

This project was developed by:

- **Tejas Santosh Paithankar (24BCY10104)**
- **Ashwin C (24BCY10218)**
- **Sudhanshu Singh (24BCY10410)**
- **Aashish Kumar Singh (24BCY10182)**
- **Niyati Agarwal (24BCY10293)**

1. Overview

Expert Systems With Applications (Paper)

The paper presents a new rule-based system for detecting phishing attacks, especially in internet banking, using a set of novel features such as page resource identity and resource protocol. It uses SVM for model training, and extracts rules to build a Chrome extension called PhishDetector. The approach is independent of third-party services, and aims for high accuracy on zero-day phishing.

PhishGuard AI Extension Codes

The codes (background.js, popup2.js, content.js, etc.) implement a Chrome extension for real-time phishing detection. Approaches include domain blacklist checks via API, AI (Gemini API), SSL validation, allowlist handling, and blocking warnings. Code structure supports user reporting, notification, and allowlist management via popup.

2. Detection Approach Comparison

Aspect/Feature	Expert Systems Paper	PhishGuard AI Extension
Detection Method	Rule-based, SVM-based feature vector, extracted rules	Combination: Blacklist API, AI (Gemini), SSL check, allowlist
Novelty	Two new feature sets: resource identity and protocol; page DOM focus	Parallel threat checks, AI integration, user interaction
Machine Learning	SVM for model, then rules extracted for interpretability, extension	AI analysis (external, Gemini), no SVM or model rules
Feature Engineering	17 features incl. IP, SSL, URL length, Levenshtein similarity	Blacklist, AI prompt, SSL; no explicit feature engineering
Blocking Action	Extension popup warns/block, rules embedded directly	Block page, custom blocked.html, Chrome notifications, allowlist
Zero-Day Phishing	Claimed yes, via feature engineering	AI analysis could detect novel threats
User Reporting	Not specified in paper	User can report; notification; reported list stored
Allowlist	Not specified in paper	Explicit allowlist function in popup & backend

3. Strengths & Limitations

Paper (Expert Systems)

- **Strength:** Carefully engineered features and validation; interpretable rules; high accuracy; zero-day detection.

- **Limitation:** Relies on manual feature extraction; SVM rules require conversion; some false positives. Evaluation is research focused, not user experience.

PhishGuard AI Extension Code

- **Strength:** Real-time, in-the-wild protection; combines multiple strategies (API, AI, SSL, whitelist); user-friendly popups & notifications.
- **Limitation:** Depends on external APIs (APIVoid, Gemini); AI analysis may not be as interpretable; lacks custom rule adaptation; feature extraction less granular.