**Research Scope: Exploration of AI for Social Engineering Detection**

**Objective:**

* To examine how AI is currently used for detecting social engineering attacks, identify gaps, and propose recommendations for improvement.

**Focus Areas:**

1. **Existing AI Techniques**
   * Study AI models like machine learning (ML) classifiers (e.g., SVM, Random Forest) and deep learning approaches (e.g., BERT, GPT).
   * Explore their application in detecting phishing emails, fake messages, and other social engineering attack types.
2. **Feature Analysis**
   * Identify features commonly used in AI detection systems, such as linguistic cues, metadata, or sender behavior.
   * Evaluate the effectiveness of these features in differentiating legitimate and malicious communications.
3. **Challenges and Limitations**
   * Investigate challenges like data scarcity, false positives, adversarial attacks, and ethical concerns.
   * Explore how attackers exploit AI vulnerabilities (e.g., bypassing detection systems).
4. **Case Studies**
   * Analyze real-world use cases of AI in social engineering detection, such as email security solutions or anti-phishing platforms.
   * Compare the performance of different AI tools and algorithms.
5. **Future Trends**
   * Explore emerging techniques, such as reinforcement learning or adversarial training, in combating social engineering.
   * Discuss the implications of AI-enhanced social engineering attacks (e.g., deepfake scams) on detection strategies.

**Research Methodology**

1. **Literature Review:**
   * Study research papers, journals, and industry reports on AI in social engineering detection.
   * Examples of sources:
     + IEEE Xplore
     + SpringerLink
     + ResearchGate
     + Government and industry publications (e.g., CyberSecurity Malaysia, ENISA).
2. **Comparative Analysis:**
   * Compare existing AI-based detection methods based on metrics like accuracy, robustness, and scalability.
   * Evaluate their effectiveness in different contexts (e.g., phishing emails, SMS scams).
3. **Interviews/Surveys:**
   * Interview cybersecurity professionals in Malaysia to understand the local landscape of social engineering threats and AI applications.
   * Conduct surveys to gauge user awareness and effectiveness of current AI-powered tools.
4. **Case Study Research:**
   * Analyze specific tools or systems (e.g., AI-based email filtering solutions).
   * Investigate their implementation, performance, and real-world impact.