

**4IIR**

**Cahier des charges :**

**Application web de détection des emails frauduleux et tentatives de phishing**



Réalisé par :

AL ARHWANY Fatima Ezzahra

ENNADIRI Ichrak

Supervisé par :

Dr.A .BAKHOUYI

2024/2025

**Sommaire :**

1. **Contexte et Problématique**

**2. Objectifs du projet**

### 3. Fonctionnalités principales

**4. Règles de détection des Emails Frauduleux**

**5. Sécurité et Protection des Données**

**1. Contexte et Problématique**

Les attaques par phishing sont de plus en plus fréquentes et représentent une menace majeure pour les entreprises et les particuliers. Ces attaques exploitent des emails frauduleux pour tromper les utilisateurs et obtenir des informations sensibles (identifiants, données bancaires, etc.).

L’objectif de cette application est de permettre aux utilisateurs de soumettre un email et d’obtenir une évaluation basée sur des critères de détection avancés afin de prévenir les cyberattaques. En complément de l’analyse des emails, l’application proposera des recommandations de sécurité et un module de formation interactive pour sensibiliser les utilisateurs aux bonnes pratiques contre le phishing.

**2. Objectifs du projet**

* Développer une API REST d’analyse et de prévention des emails frauduleux.
* Analyser les liens et pièces jointes des emails pour identifier les menaces.
* Alerter les utilisateurs en cas de risque et proposer des actions de prévention.
* Offrir un module de formation et sensibilisation aux attaques de phishing.
* Proposer une interface intuitive pour soumettre un email, consulter les analyses et alertes.
* Permettre la génération de rapports d’analyse (PDF/CSV).

1. **Fonctionnalités principales**

3.1 API REST

* Analyser un email en appliquant des règles prédéfinies.
* Vérifier les liens et pièces jointes contre des bases de données de menaces.
* Fournir des réponses détaillées et personnalisées au format JSON.
* Intégrer une intelligence artificielle pour améliorer la détection des menaces.

3.2 Interface Utilisateur

* Soumission d’email : possibilité de soumettre un email sous forme de texte ou en pièce jointe.
* Affichage des résultats : présentation des résultats d’analyse sous forme de rapport clair et compréhensible.
* Alerte utilisateur : notification en cas de risque détecté avec recommandations.
* Génération de rapports : possibilité d’exporter les résultats en PDF ou CSV.
* Module de formation : plateforme interactive proposant des quiz et exercices pratiques pour améliorer la sensibilisation aux cyberattaques.

1. **Règles de détection des Emails Frauduleux**

L’analyse des emails repose sur plusieurs critères :

* 1. **Analyse des liens**
* Vérification des URLs avec des services de liste noire.
* Comparaison du domaine avec l’expéditeur déclaré.
* Analyse du certificat SSL et de l’historique du domaine.
  1. **Analyse du contenu**
* Détection de mots-clés suspects (ex. : “urgent”, “votre compte est bloqué”).
* Analyse grammaticale pour repérer des erreurs typiques du phishing.
  1. **Analyse des expéditeurs**
* Vérification de la réputation du domaine.
* Comparaison entre l’adresse d’expédition et l’adresse de réponse.
* Détection des adresses emails usurpées.
  1. **Analyse des en-tetes d’email**
* Vérification des champs Reply-To, From et Return-Path pour détecter des incohérences.
* Détection des techniques avancées d’usurpation d’identité.
  1. **Analyse des pièces jointes**
* Vérification des extensions de fichiers suspectes (.exe , .scr , .bat ).
* Détection de fichiers compressés protégés par mot de passe.

1. **Sécurité et Protection des Données**

* Chiffrement des données sensibles.
* Protection contre les injections SQL et attaques XSS.
* Implémentation d’un mécanisme de limitation des requêtes pour éviter les abus.
* Utilisation d’APIs externes reconnues (Google Safe Browsing, VirusTotal) pour améliorer la détection.
* Anonymisation des emails traités pour garantir la confidentialité des utilisateurs.