

TP – API “Digital Social Score”

De l’analyse de texte à l’infrastructure Cloud sécurisée, scalable et conforme

1 - Objectif global

Vous devez concevoir et déployer une interface de programmation (API) qui :

- Déetecte la toxicité d'un texte (injure, racisme, harcèlement, propos haineux).
- Attribue un score numérique de 0 à 100 à chaque texte.
- Respecte le RGPD : aucune donnée personnelle stockée en clair.
- Est capable de varier d'échelle (scalabilité, passage de quelques utilisateurs à des milliers sans rupture).
- Est observable et auditable (logs, métriques, alertes).
- Est documentée avec un schéma d'architecture Cloud lisible et justifié.

Étape 1 : Exploration, analyse et anonymisation des données

Objectifs pédagogiques :

- Repérer et traiter les données personnelles dans des textes, comprendre le cadre RGPD.
- Mettre en œuvre l'anonymisation et la pseudonymisation.

Exercice :

- Télécharger un jeu de données adapté (ex : Toxic Comment Classification Dataset ou GameTox).
- Utiliser un algorithme NER (ex : spaCy) pour anonymiser les données.
- Comparer la version initiale et anonymisée et justifier chaque choix.
- Documenter votre registre de traitement des données.

Étape 2 : Préparation et entraînement d'un modèle IA

Objectifs pédagogiques :

- Appréhender le nettoyage de texte et les modèles d'IA.
- Entraîner et comparer un modèle simple et un modèle avancé (BERT).

Exercice:

- Nettoyage des textes (ponctuation, emojis, casse).
- Entraîner deux modèles : statistique et avancé (LSTM ou BERT).
- Comparer précision, rappel, et temps de traitement.

Étape 3 : Déploiement du modèle en API Cloud

Objectifs pédagogiques :

- Transformer le modèle IA en service accessible.
- Utiliser FastAPI, Flask ou un service Cloud (Vertex AI, Scaleway, AWS...).

Exercice:

- Exporter le modèle et le déployer dans le Cloud.
- Créer une API recevant un texte et renvoyant un score.
- Tester plusieurs exemples de requêtes.

Étape 4 : Sécurisation et conformité RGPD

Objectifs pédagogiques :

- Mettre en place authentification et chiffrement.
- Garantir la conformité RGPD (validation, logs pseudonymes).

Exercice:

- Configurer JWT ou clé API.
- Mettre en place HTTPS, IAM et registre RGPD.

Étape 5 : Simulation de montée en charge

Objectifs pédagogiques :

- Expérimenter la différence entre un prototype et un service scalable.
- Utiliser Apache Bench, Locust ou k6 pour tester la charge.

Exercice:

- Simuler croissance progressive, stress test et failover.
- Mesurer latence moyenne, P95/P99, taux d'erreur.
- Proposer des améliorations (cache, load balancer, redondance).

Étape 6 : Sécurité et supervision

Objectifs pédagogiques :

- Observer la stabilité du système en cas de stress.

- Tester la supervision Prometheus/Grafana.

Exercice:

- Analyser les logs et les comportements anormaux.
- Simuler panne ou attaque et évaluer la continuité du service.

Étape 7 : Modélisation de l'infrastructure Cloud

Objectifs pédagogiques :

- Schématiser et justifier chaque composant.
- Penser sécurité et conformité (approche zero trust).

Exercice:

- Lister les composants (API, IA, stockage, supervision).
- Dessiner les flux, authentifications, et chiffrement.
- Rédiger un texte explicatif et une légende du schéma.

2 - Livrables globaux du projet

- API fonctionnelle et documentée
- Exemples de requêtes et réponses
- Schéma d'architecture Cloud + texte explicatif
- Registre RGPD
- Tableau de bord / captures supervision
- Rapport simulation de charge
- Grille tests sécurité/stress/failover

3 - Critères d'évaluation

Compétence	Indicateurs
Fonctionnalité	API opérationnelle, scoring correct
Sécurité	Authentification, validation d'entrée, chiffrement
Scalabilité	Test de charge et analyse pertinente
Supervision	Logs/métriques, dashboard
Conformité RGPD	Anonymisation, registre conforme
Présentation	Documentation claire, schéma lisible, code commenté

Ressources / outils recommandés

- Jeux de données :

- Toxic Comment Classification Dataset
- GameTox
- Frameworks:
 - FastAPI
 - Flask
 - spaCy
 - HuggingFace
 - Vertex AI
- Tests de charge:
 - Apache Bench
 - Locust
 - k6
- Supervision:
 - Prometheus
 - Grafana
- Documentation RGPD et modèles de registre:
 - CNIL