ENSI CAEN

Apprentissage sur données confidentielles

GREYC – LABORATOIRE DE RECHERCHE EN SCIENCES DU NUMÉRIQUE

Programme

INTRODUCTION

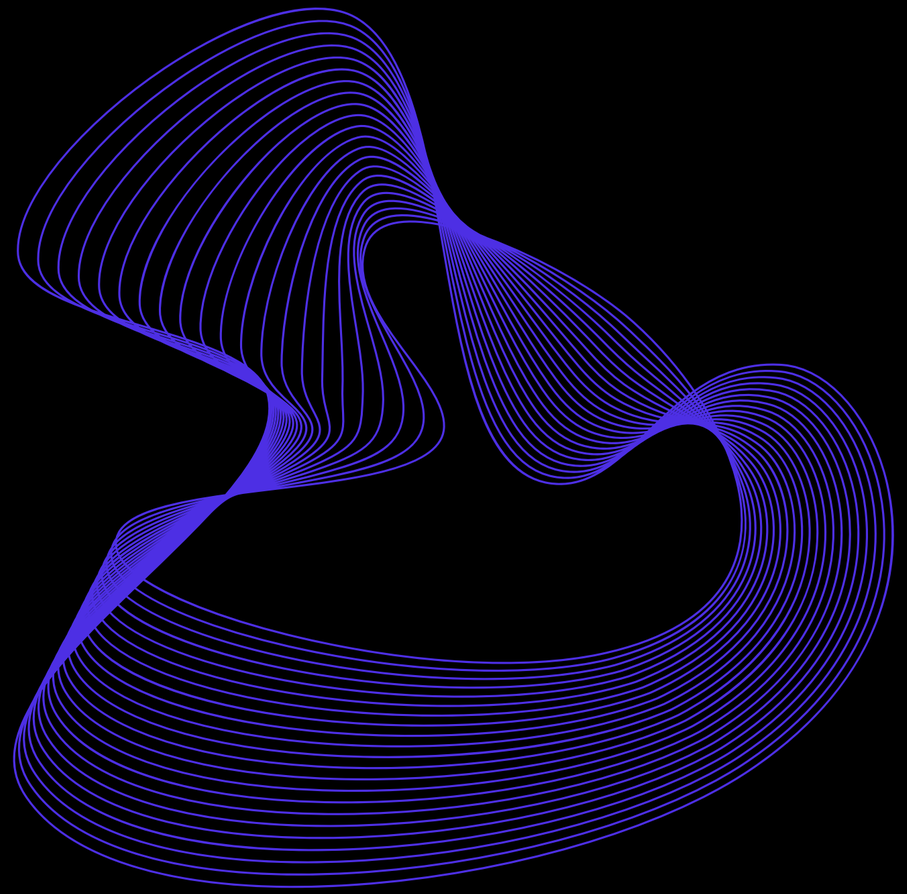
MEMBRES DU PROJET

PRÉSENTATION DU PROJET

PLANIFICATION

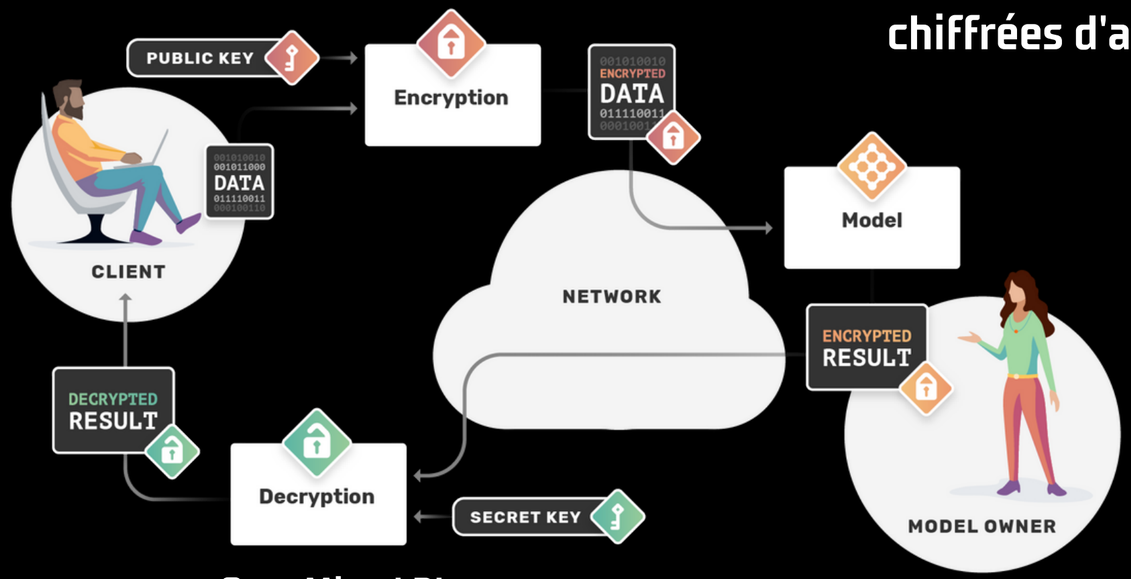
BUDGET

ANALYSE DES RISQUES



Aperçu du projet

Création d'un programme de machine learning à partir de données chiffrées



source : OpenMined Blog

RÉALISATION CONCRÈTE

Notre objectif à long terme consiste à différencier de manière précise, grâce à notre modèle d'apprentissage, une image chiffrée d'un animal parmi d'autres images chiffrées d'animaux.

OBJECTIFS

- Réalisation d'un état de l'art scientifique
- Développer un modèle d'apprentissage automatique
- Atteindre un niveau de précision défini pour les prédictions du modèle
- Ajuster le modèle pour améliorer ses performances et réduire l'erreur de prédiction
- Créer une démonstration web simple pour illustrer le modèle d'apprentissage automatique

L'équipe

CHRISTOPHE ROSENBERGER
TUTEUR

TANGUY GERNOT
TUTEUR

NOURA OUTLIOUA
CHEFFE DE PROJET

PAUL NGUYEN
RELEASE MANAGER

CECILE LU – DÉVELOPPEUSE

ZEYD BOUMAHDI – DÉVELOPPEUR

ANIS AHMED ZAID – DÉVELOPPEUR

Périmètre du projet

Qui

Les membres de l'équipe, en collaboration avec les professeurs encadrants

Quoi

- Prendre connaissance des méthodes de chiffrement et d'apprentissage machine sur des données chiffrées
- Réaliser des tâches de prédiction et d'apprentissage machine sur des données protégées

Où

A l'ENSICAEN

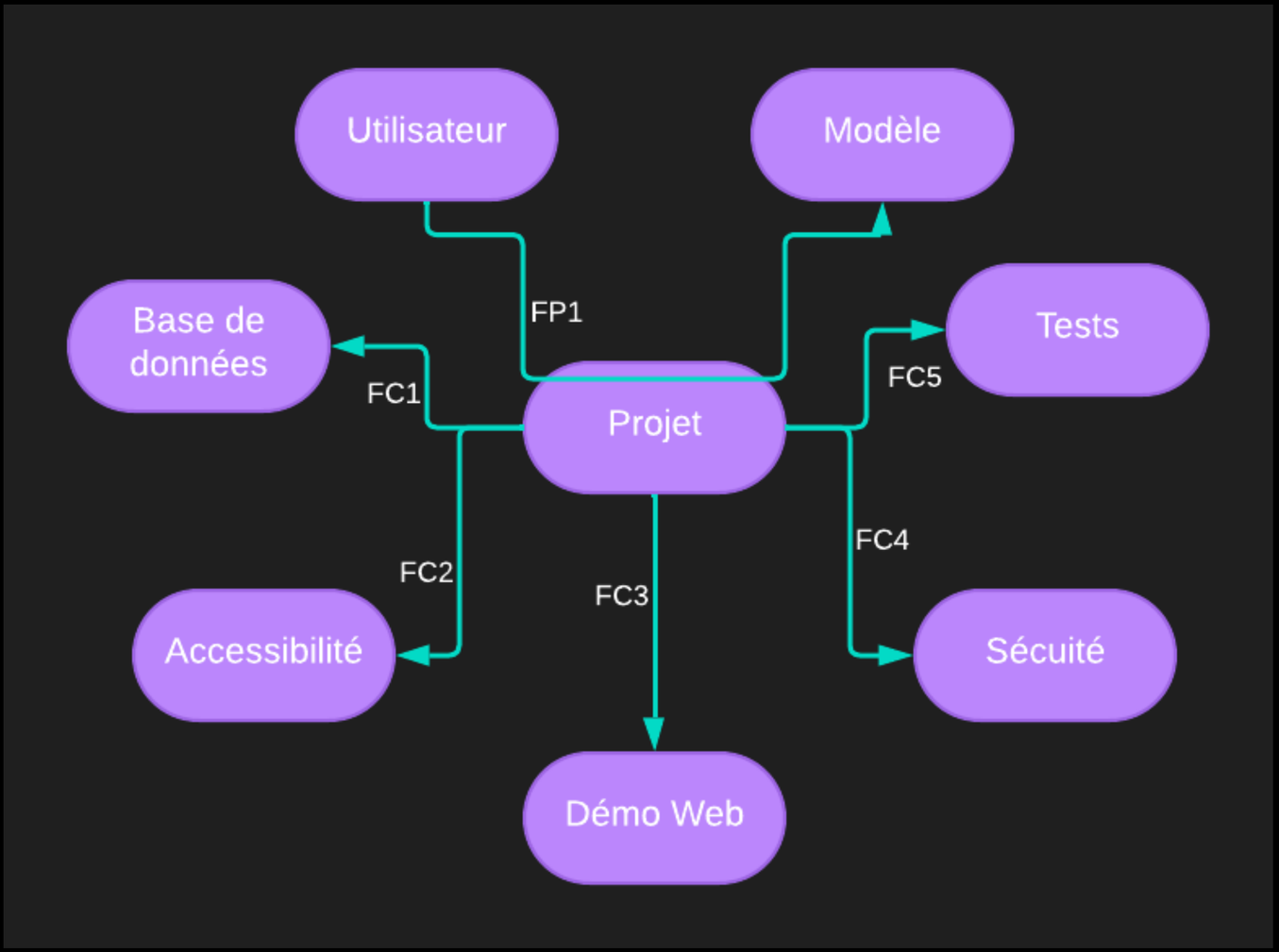
Comment

- Réalisation d'un état de l'art scientifique
- Implémenter et/ou utiliser un algorithme de chiffrement homomorphique, entraîner un modèle sur une base de données chiffrées
- Créer une base de donnée avec des photos d'animaux chiffrées
- Produire un site web de démo.

Pourquoi

- Permettre aux entreprises ou aux services publiques de bénéficier d'un modèle de prédiction sans que celles-ci n'aient à partager des données sensibles ou confidentielles (par exemple un hôpital)
- Détecter des données sensibles sans y accéder directement

Diagramme pieuvre



FP1 : L'utilisateur doit pouvoir fournir des données chiffrées (sécurisées, voire confidentielles) et le modèle doit fournir une prédiction elle-même chiffrée que l'utilisateur peut déchiffrer.

FC1 : Le modèle doit s'entrainer à reconnaitre et prédire sur des données chiffrées (chiffrement homomorphique).

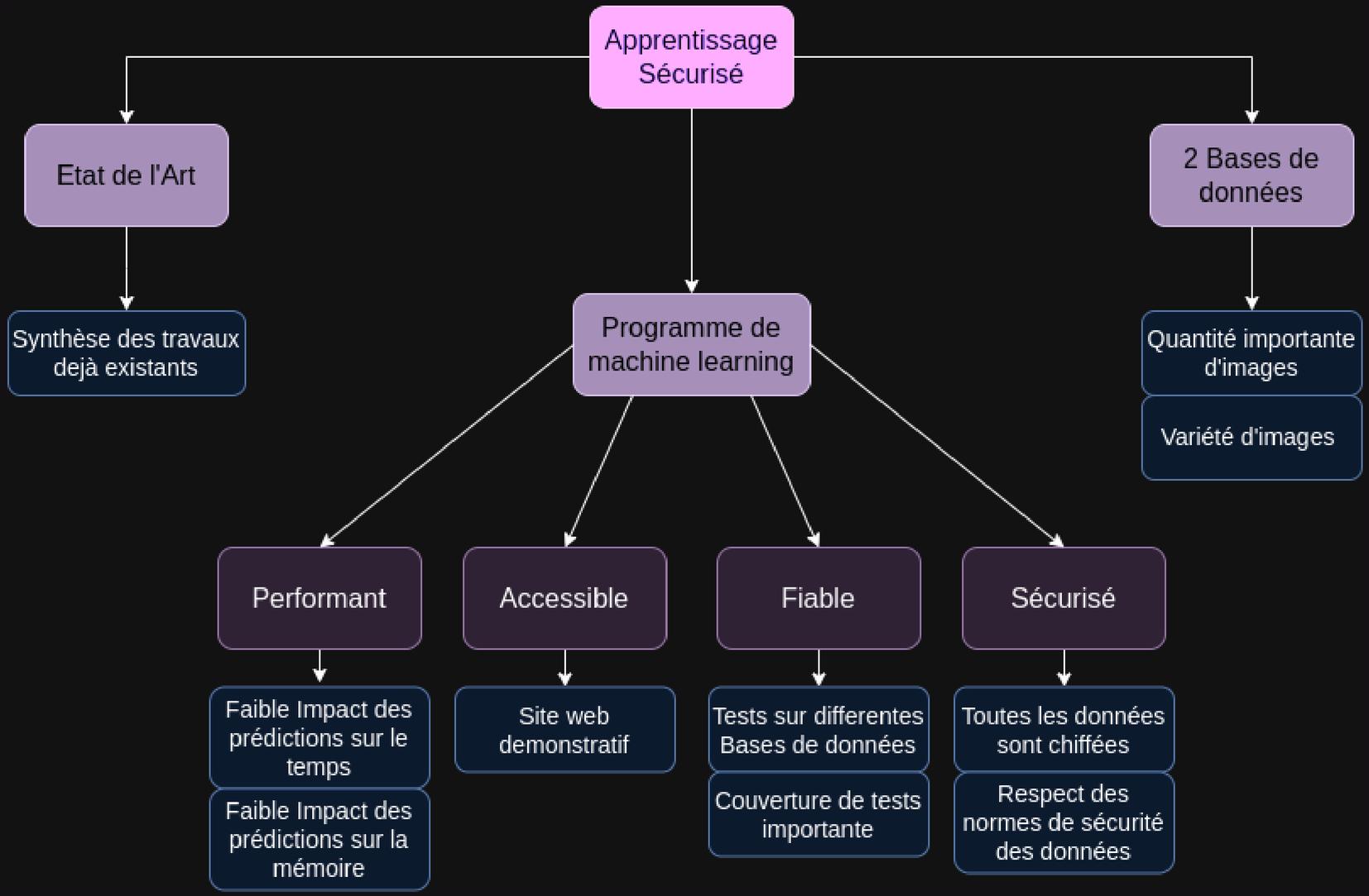
FC2 : L'utilisation doit être simple et intuitive, éventuellement fournir à l'utilisateur un moyen de chiffrer les données avec une clé privée, qu'il pourra utiliser par la suite pour déchiffrer le résultat fournit par le modèle.

FC3 : Présence d'un site web de démonstration, qui montrera les performances de notre modèle en illustrant le plus possible le processus (chiffrement, prédiction, entrée/sortie, déchiffrement, etc.).

FC4 : Le modèle ne doit pas avoir accès à la clé de déchiffrement, il traite et renvoie uniquement des données chiffrées.

FC5 : Le modèle sera testé sur une base de donnée différente de celle sur laquelle il apprend pour réduire l'erreur de prédiction.

Livrables du projet

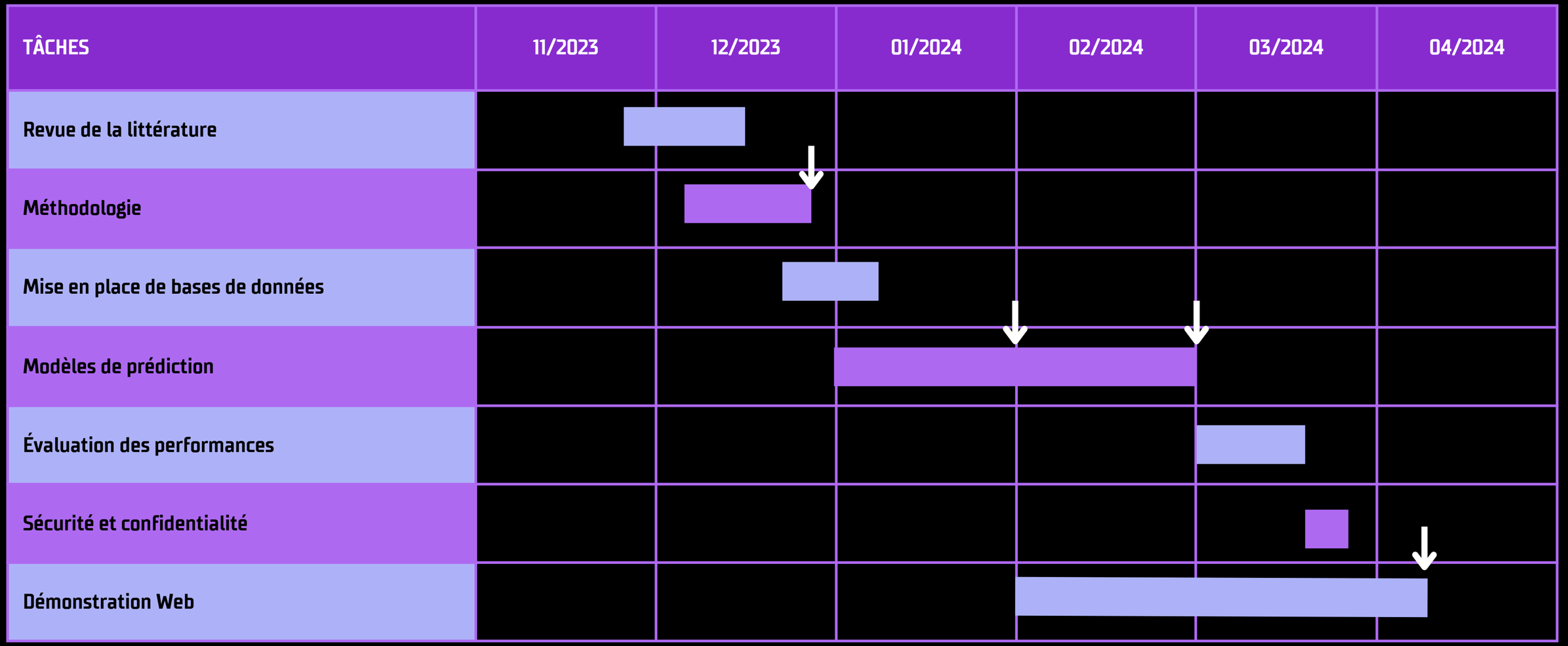


Tâches du projet

Apprentissage sur données confidentielles

Revue de la littérature	• Synthèse des travaux de recherche antérieurs sur l'apprentissage sur des données confidentielles • Analyse des approches existantes pour la protection de la vie privée dans le contexte de l'apprentissage statistique • Identification des principales méthodes utilisées pour réaliser des tâches de prédiction à partir de données protégées • Réalisation d'un état de l'art scientifique
Méthodologie	• Recherche détaillée des méthodes et des techniques utilisées pour assurer la confidentialité des données • Réflexion sur les protocoles de formation des modèles d'apprentissage à mettre en place
Mise en place de bases de données	• Description de deux bases de données, une base de donnée d'entrainement et une qui permettra de valider le modèle en mettant l'accent sur leur nature sensible et la manière dont ils ont été traités pour préserver la confidentialité
Modèles de prédiction	• Présentation des modèles de prédiction utilisés dans le cadre du projet • Développement et/ou test sur l'architecture des modèles et les algorithmes d'apprentissage utilisés
Évaluation des performances	• Résultats des expérimentations sur la prédiction à partir de données protégées • Analyse de l'impact sur la performance, incluant la précision des prédictions et le temps de calcul
Sécurité et confidentialité	• Mesures mises en place pour garantir la sécurité des modèles et des données • Analyse des vulnérabilités potentielles et des contre-mesures adoptées
Démonstration Web	• Réalisation d'une démo Web du programme de machine learning réalisé

Planification: Diagramme de Gantt



↓ : JALON

Ressources humaines

Tâche	Compétence requise	Niveau de compétence	Volume de Travail (7 heures/semaine)	Période de Disponibilité
Effecuter un état de l'art scientifique	• Compréhension d'article scientifique et choix intelligent des sources et documents utilisés	Ingénieur	15 homme-semaines	Dès le début du projet
Développement du modèle d'apprentissage	• Compréhension des principes de l'IA et de l'apprentissage automatique, • Compétences en programmation	Ingénieur, Junior	32 homme-semaines	Lorsque l'état de l'art est fini
Evaluation des perfomances	• Tester un modèle	Ingénieur, Junior	9 homme-semaines	À la fin du développement du modèle
Optimisation des Performances	• Ajuster un modèle, • Optimiser	Ingénieur, Junior	4 homme-semaines	Après les tests de précision
Démonstration Web	• Développement web • Interface utilisateur	Ingénieur, Junior	21 homme-semaines	À la fin de l'optimisation des performances

Budget

TÂCHES	TEMPS
Revu de la littérature	3 semaines
Méthodologie	3 semaines
Mise en place de bases de données	2 semaines
Modèles de prédiction	2 mois

TÂCHES	TEMPS
Evaluation des performances	2/3 semaines
Sécurité et confidentialité	2 semaines
Démonstration Web	1 mois
Total	5 mois

Analyse des risques

Nature du risque	Impact sur le projet	Mesure de prévention ou de réduction	Coût
Changement des Exigences Client	Risque de délais et de modifications importantes	Engagement du client à figer les exigences à une date précise	-
Indisponibilité d'une Ressource Clé	Risque de retards	Plan de contingence avec une liste de remplaçants possibles	-
Non réalisation du modèle d'apprentissage automatique	Risque de retard dans la livraison du projet	Contrôle régulier durant le développement du modèle	Réunions supplémentaires avec les tuteurs
Défaillance Matérielle ou Logicielle	Risque de perturbation du développement	Utilisation de matériel fiable, sauvegardes régulières des données	Coût additionnel pour le matériel de secours
Mésentente de l'équipe	Risque de perturbation dans l'avancé du projet	Communication régulière entre tous les membres	Temps dédié à la bonne cohésion de groupe
Non-Fin du Projet à Temps	Risque de délais grave dans la livraison du produit final	Planification réaliste, suivi régulier des jalons	Coût additionnel pour des heures supplémentaires si nécessaire

ENSI CAEN

Merci de votre attention