

Reconnaissance Clavier

Soutenance Finale

Elèves : Abdelmalek BELGHOMARI – Mohamed Abderrahmane BEDDA –
Haykel SRIHA – Cedric WILLAUME – Winnie KAMTCHUENG

Encadrants : Christophe ROSENBERGER – Tanguy GERNOT



L'École des Ingénieurs Scientifiques

1. Introduction
2. Méthodologie de développement
3. Conception
4. Conclusion

Objectifs :

- Reconnaissance du contenu tapé au clavier à l'aide d'un enregistrement audio
- Identification de l'utilisateur grâce à l'analyse des émissions sonores du clavier
- Livrer une démonstration web de la reconnaissance de touches et de personnes

Contexte :

- Répond à des nécessités liées à la cybercriminalité
- Aide des services de sécurité à l'accès aux données sensibles
- Surveillance de l'activité d'utilisateurs
- Fournit une authentification biométrique
- Prévention contre de futures attaques biométriques

1. Etat de l'art

Paper	Year	Principle	Accuracy(percentage)
A Practical Deep Learning-Based Acoustic Side Channel attack on keyboards	2023	CoAtNet	93%
Analyse de la dynamique de frappe au clavier sonore pour l'identification, le profilage et l'extraction du texte saisi	2022	SVM/MFCC	96%
Don't skype & type	2017	MFCC	91%
Don't skype & type	2017	LF	100%
Reconnaissance de saisie sur clavier par analyse acoustique	2011	Intercorrelation/DFT	99%
Keyboard Acoustic Emanations Revisited	2009	MFCC/HMM	87% without any noise
Keyboard Acoustic Emanations: An Evaluation of strong passwords and typing styles	Unknown	Tim-Frq	82.69%

Figure 1 : Tableau de comparaison de différents modèles de reconnaissance sonore

Méthodologie de développement

2. Agilité du Projet : Novembre à Janvier

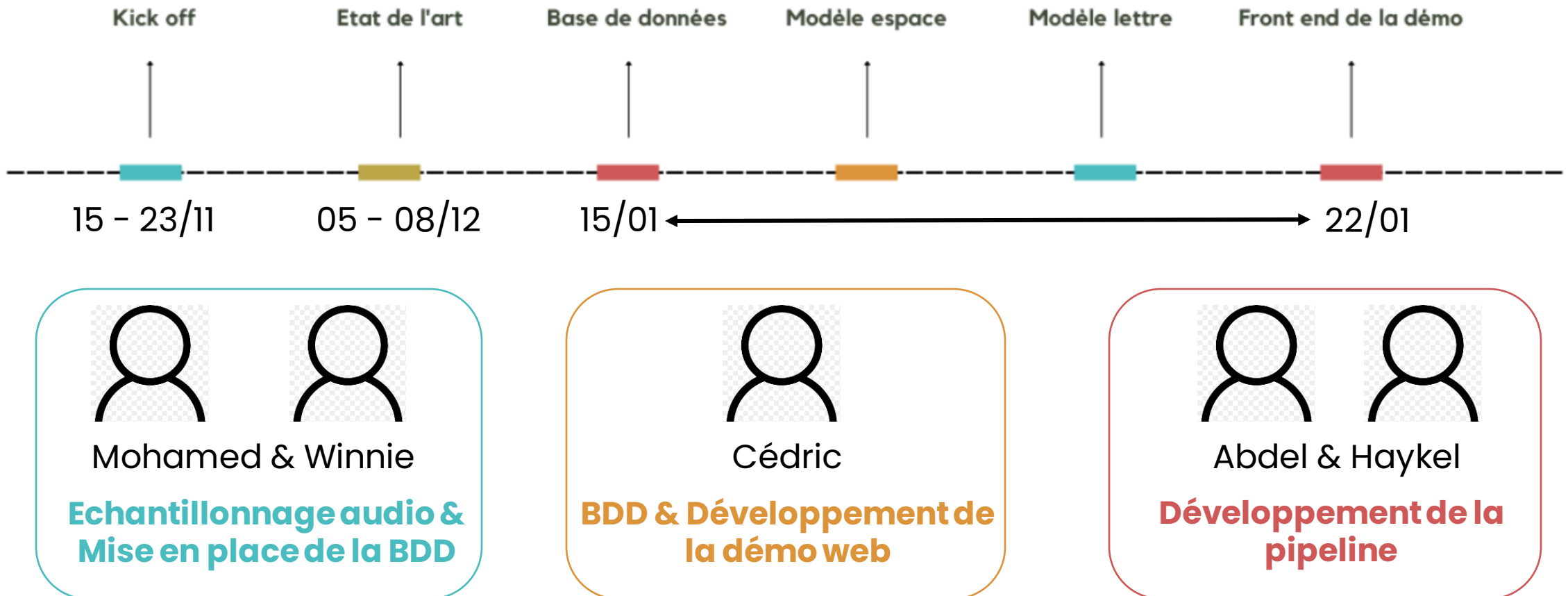


Figure 2 : Organisation Agile du projet

Méthodologie de développement

3. Agilité du Projet: Février à Avril

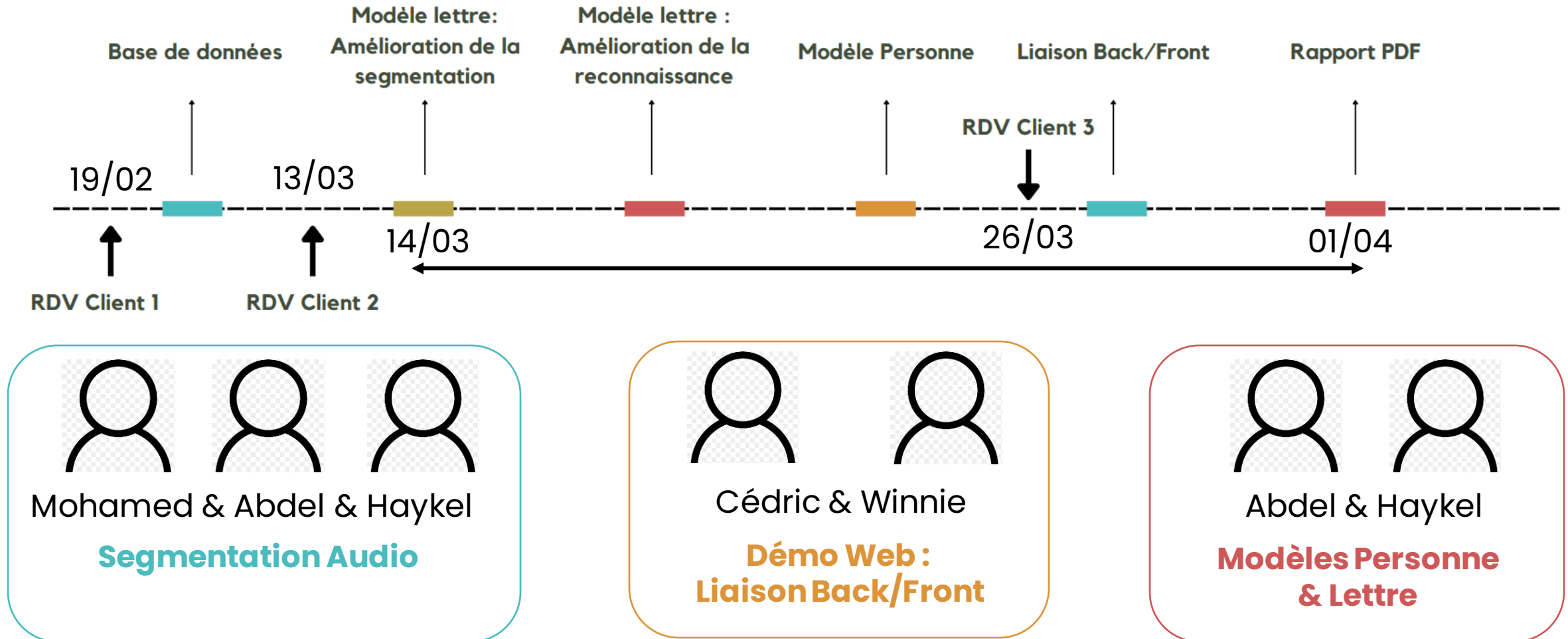










Figure 3 : Organisation Agile du projet après Mi-Parcours

4. Outils utilisés

- Partage de code : 
- Canal de discussion du groupe :  
- Edition & Partage de documents :    
- Contact avec les tuteurs/clients : 

1. Base de données



Matériels utilisés :

- Micro & Clavier Huawei Matebook

Contenu de la base de données :

- 2 datasets de 50 fichiers audios de phrases
- 4 datasets audios de 30 audios de phrases
- 3 datasets audios de 27 lettres (avec espace)

Protocole suivi :

- Enregistrement sur le Matebook avec la démo web
- Touche tapée une par une, sans dactylographier : pour modèle touche
- Vitesse de tape normale pour le modèle personne.
- Sans aucun bruit ambiant

Conception

2. Chaîne opérationnelle : Reconnaissance de lettres

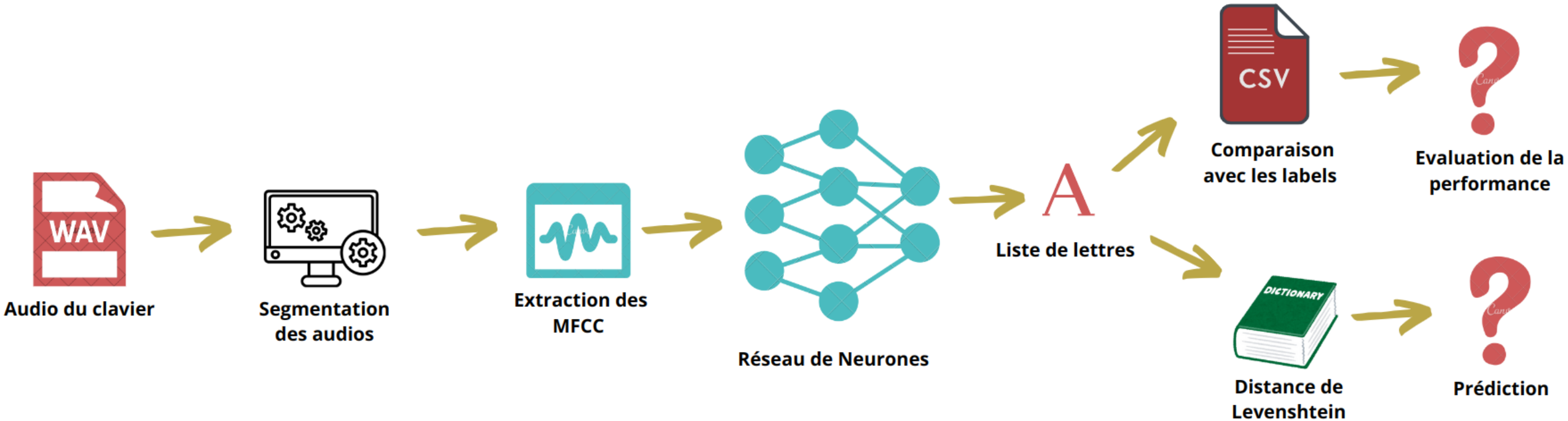


Figure 4 : Fonctionnement du réseau de neurones modèle lettre

2. Chaîne opérationnelle : Reconnaissance de personnes

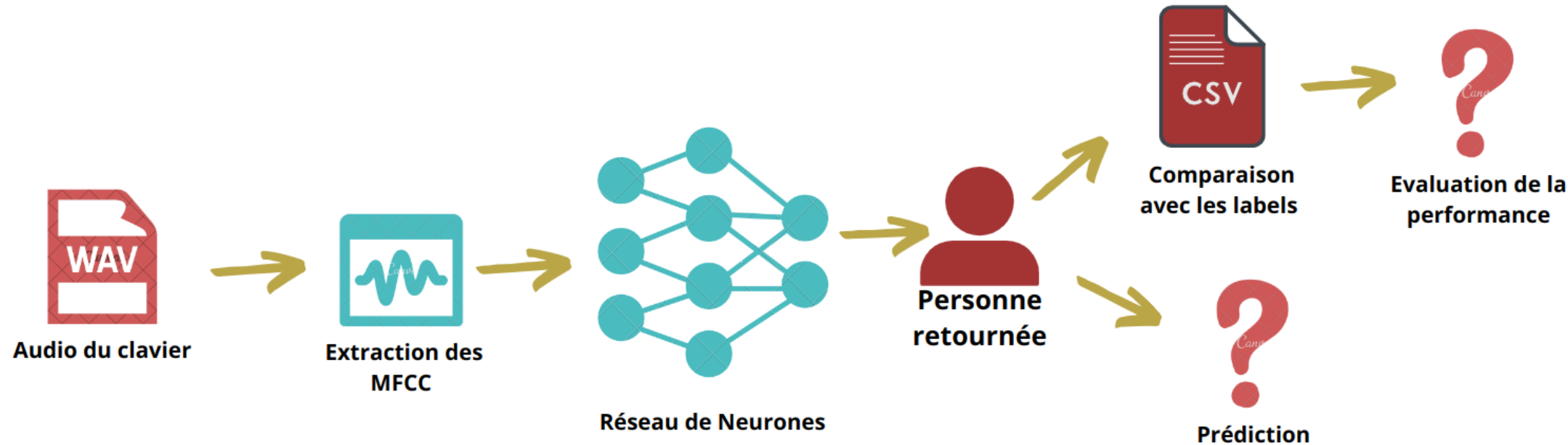


Figure 5 : Fonctionnement du réseau de neurones modèle personne

Conception

2.1. Echantillonnage des audios : Modèle Lettre

Objectif :

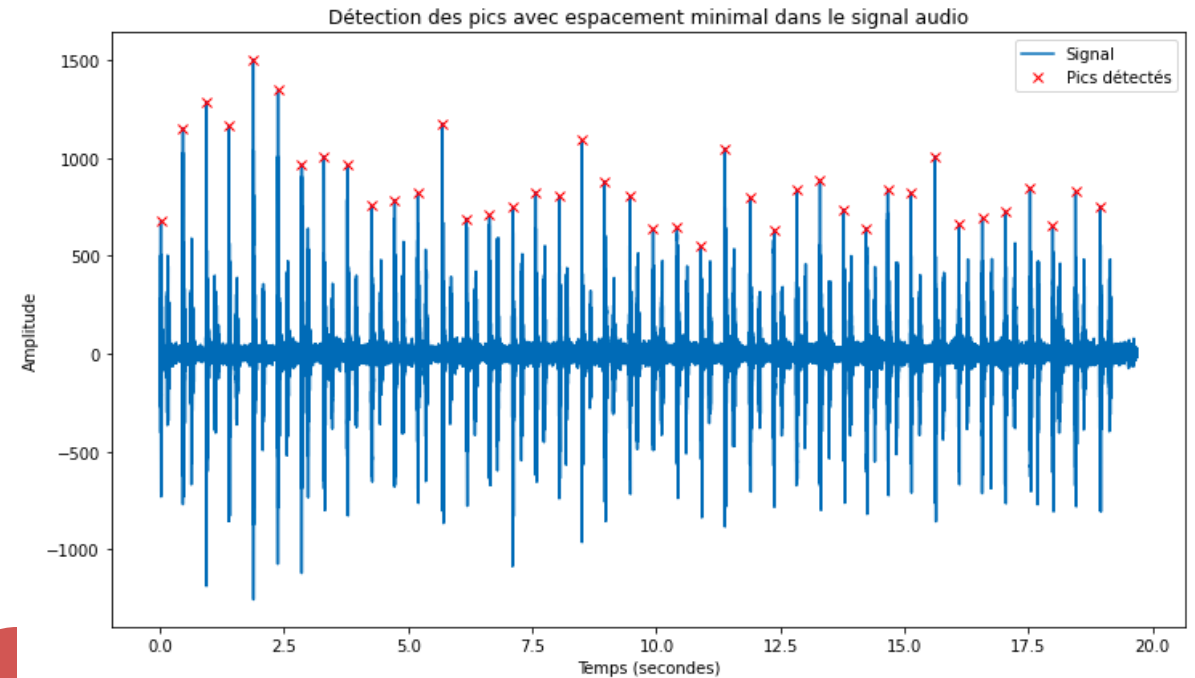
- Extraction sonore touche par touche

Outils utilisés:

- Bibliothèque python: scipy.signal
- Fichiers audios de la base de données

Méthode suivie :

- Détection de pics du signal
- Extraction des données MFCC du signal



2.2. MFCC

Objectif :

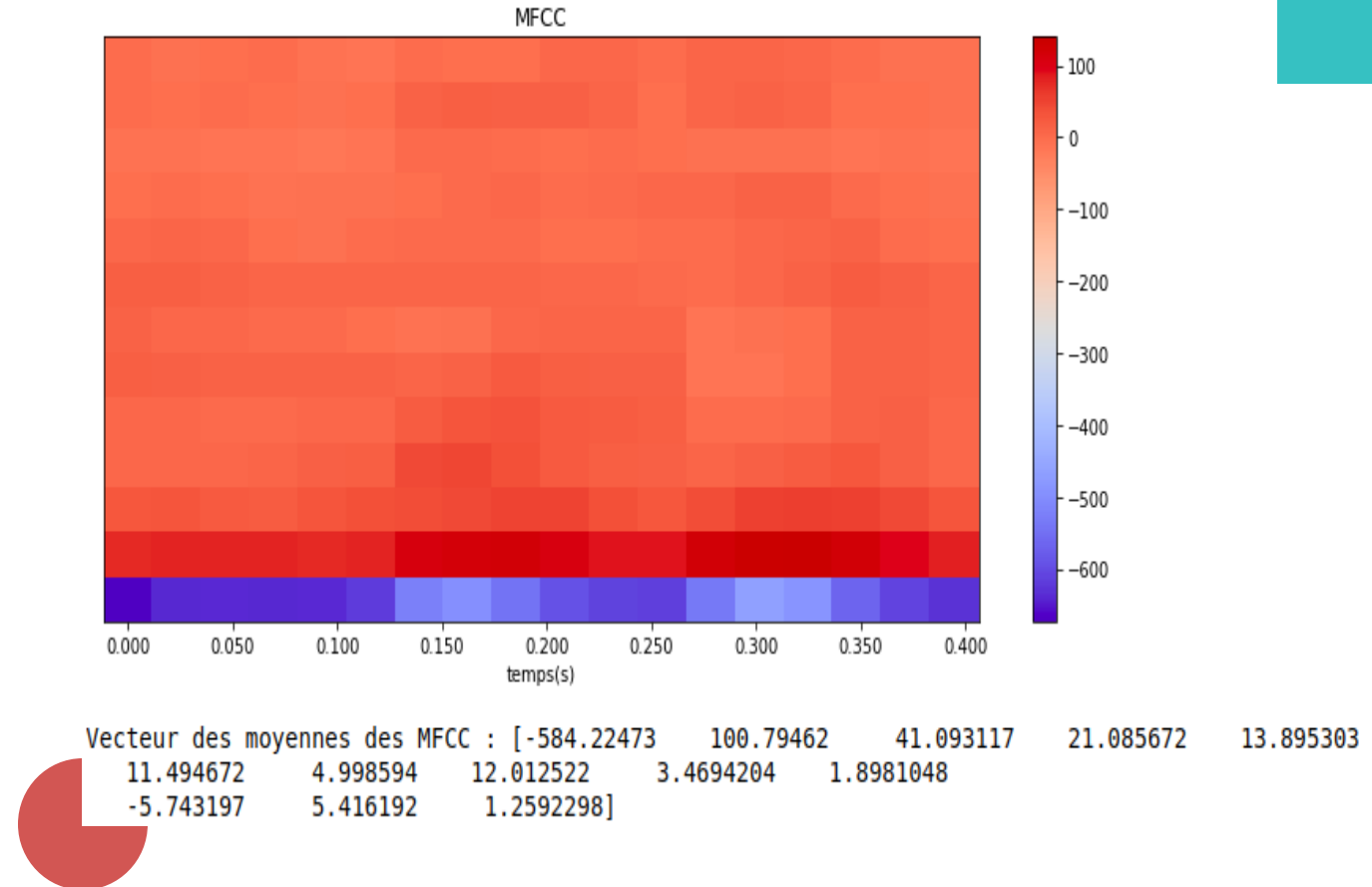
- Caractériser une touche avec les coefficients MFCC

Outils utilisés:

- Base de données de segments d'audios
- librosa, numpy
- pandas, csv

Méthode suivie :

- Extraction des données MFCC du signal
- Moyenner chaque coefficient sur l'ensemble des trames



2.2. MFCC

Méthode d'extraction des MFCC pour la reconnaissance de personne :

- Segmenter un fichier audio en plusieurs parties de même taille
- Extraire un nombre fixe de MFCC pour chaque segment

=> combien de segments et de MFCC par segments faut-il pour avoir une performance optimale ?

nombre de
segments choisi

20

nombre de
mfccs choisi

20

Nombre de MFCCs	5	10	15	20	25	30	35	40	45	50
Nombre de Segments										
5	0.750000	0.750000	0.750000	0.833333	0.833333	0.833333	0.833333	0.916667	0.916667	0.833333
10	0.833333	0.833333	0.916667	0.833333	0.916667	0.833333	0.833333	0.916667	0.916667	0.916667
15	0.916667	0.916667	0.916667	0.916667	0.916667	0.916667	0.916667	0.916667	0.916667	0.916667
20	1.000000	1.000000	1.000000	1.000000	1.000000	1.000000	1.000000	1.000000	1.000000	0.916667
25	1.000000	1.000000	0.916667	0.916667	0.916667	1.000000	0.916667	0.833333	1.000000	
30	0.916667	0.916667	0.916667	0.916667	0.916667	1.000000	0.916667	0.916667	0.916667	0.916667
35	0.916667	0.916667	0.916667	0.916667	0.916667	0.916667	0.916667	0.916667	0.833333	0.916667
40	0.916667	0.916667	0.916667	0.916667	0.916667	0.916667	0.916667	0.916667	0.916667	0.916667
45	0.916667	0.916667	0.916667	0.916667	0.916667	0.916667	0.916667	0.916667	0.916667	0.916667
50	0.916667	0.916667	0.916667	0.916667	0.916667	0.916667	0.916667	0.916667	0.916667	0.916667

Evaluations du modèle en fonction du nombre de segment et de MFCC extraits

Conception

2.3. Apprentissage

Objectif :

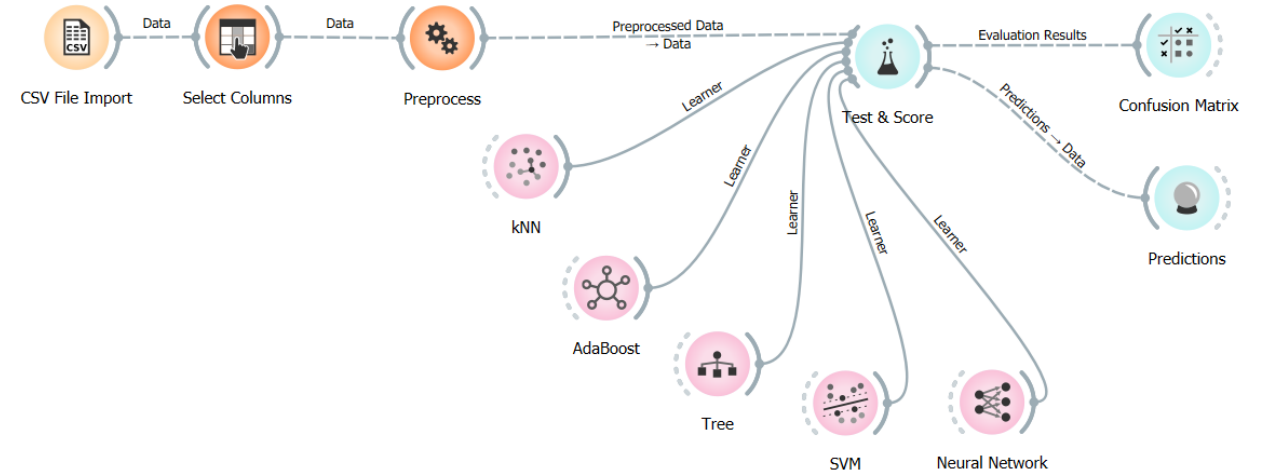
- Déterminer la meilleure méthode de classification

Outils utilisés:

- Orange

Méthode suivie :

- Entrée de données MFCC dans le workflow via un CSV
- Calcul de la meilleure méthode d'apprentissage



Model	AUC	CA	F1	Prec	Recall	MCC
kNN	0.934	0.701	0.703	0.710	0.701	0.689
AdaBoost	0.704	0.431	0.433	0.436	0.431	0.407
Tree	0.736	0.410	0.407	0.407	0.410	0.386
SVM	0.973	0.707	0.705	0.710	0.707	0.695
Neural Network	0.976	0.736	0.736	0.737	0.736	0.726

Conception

2.4. Conception du modèle

Objectif :

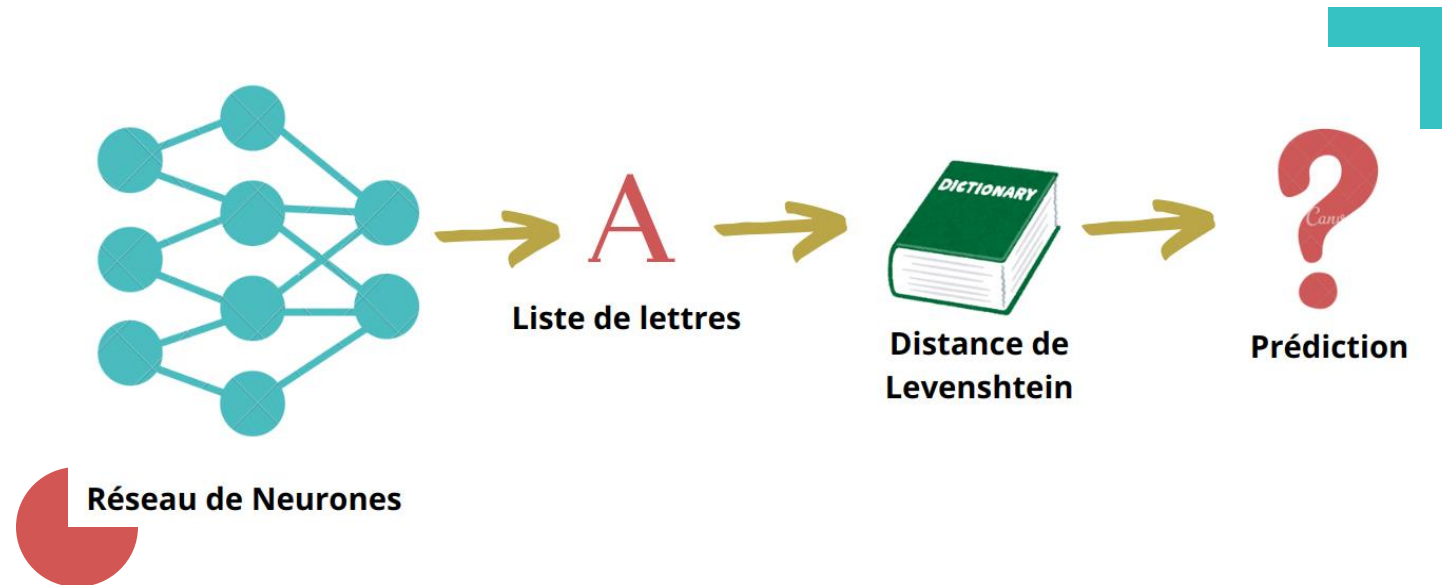
- Implémentaion d'un réseau de neurones
- Affinage des prédictions avec Levenshtein

Outils Utilisés :

- MLPClassifier de scikit learn
- Joblib
- StandardScaler
- NLTK, dictionnaire français de 20,000 mots

Méthode suivie :

- Normalisation des données
- Implémentation du réseau de neurones
- Calcul de la distance de Levenshtein



Conception

3. Démo Web

Objectif :

- Tester le produit sur n'importe quel ordinateur
- Partage simple du modèle

Outils utilisés :

- HTML, CSS, JavaScript, PHP

Fonctionnalité :

- Enregistrement lors de la saisie
- Traitement de l'enregistrement
- Affichage des prédictions de touches et de la personne



Conclusion

1. Travail réalisé

- Réalisation du kick-off
- Développement des modèles
- Démo web

2. Difficultés rencontrées

- Base de données
- Mauvaise performance du modèle lettre
- Manque de coordination entre les équipes

3. Perspectives

- Meilleures bases de données
- Réduire les contraintes
- Renseignements auprès de spécialistes

Rapport De Projet



MERCI !

Bibliographie

Animation de la démo web :

- <https://github.com/kaizhelam/Hacking-Matrix-Rain-Effect>

Documents de l'état de l'art :

- [Don't skype & type: Acoustic Eavesdropping in Voice-Over-IP](#)
- [Keyboard Acoustic Emanations Revisited](#)
- [A Practical Deep Learning-Based Acoustic Side Channel attack on keyboards](#)
- [Analyse de la dynamique de frappe au clavier sonore pour l'identification, le profilage et l'extraction du texte saisi](#)
- [Reconnaissance de saisie sur clavier par analyse acoustique](#)
- [Keyboard Acoustic Emanations: An Evaluation of strong passwords and typing styles](#)