REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE
UNIVERSITE ABDERRAHMANE MIRA DE BEJAÏA

FACULTE DES SCIENCES EXACTES
DEPARTEMENT D'INFORMATIQUE

MEMOIRE DE FIN DE CYCLE
EN VUE D'OBTENTION DU DIPLOME DE MASTER RECHERCHE EN INFORMATIQUE
OPTION : INTELLIGENCE ARTIFICIELLE

Thème

Apprentissage fédéré pour la détection d'intrusion (reconnaissance faciale)

Présenté par :

Ikhenache Arab

Soutenu devant le jury composé de :

Présidente	Mme. Khoulalene Nadjet	M.C.B	U. A. MIRA BEJAÏA
Encadrante	Mme. Aloui Soraya	M.C.B	U. A. MIRA BEJAÏA
Co-encadrant	M. Amroun Kamal	Professeur	U. A. MIRA BEJAÏA
Examinateur	M. Ouzeggane Redouane	M.A.A	U. A. MIRA BEJAÏA

Promotion 2023-2024.

Remerciement

Tout d'abord, je remercie Dieu, Tout-Puissant, pour m’avoir accordé la force, la patience et la persévérance nécessaires pour mener à bien ce travail.

Je remercie chaleureusement mon encadreur, Mme. Aloui, pour son encadrement, ses précieux conseils et sa disponibilité tout au long de ce projet. Je suis également très reconnaissant envers mon co-encadreur, M. Amourn, pour son soutien constant et ses orientations éclairées.

Je remercie également les membres du jury, Mme. Khoulalen et M. Ouzegane, pour leurs lectures attentives de mon mémoire et pour l'honneur qu'ils me font en participant au jugement de ce travail.

J’adresse par la suite mes sincères remerciements à tous les professeurs, intervenants et toutes les personnes qui ont guidé mes réflexions et répondu à mes questions durant mes recherches. Leur soutien et leur expertise ont été d'une aide précieuse tout au long de ce parcours.

À tous, je vous exprime ma gratitude et vous adresse mes plus sincères remerciements.

DIDICACE

Aucune dédicace ne saurait exprimer mon respect, mon amour éternel et ma considération pour les sacrifices que vous avez consentis pour mon instruction et mon bien-être. Votre présence, votre écoute, votre confiance en moi et votre soutien constant m'assurent des bases solides me permettant de persévérer et de me surpasser. J'espère que votre bénédiction m'accompagnera toujours. À mes familles paternelles et maternelles.

À mes amis, qui m'ont accompagné et soutenu tout au long de ce travail.

Table des matières

TABLE DES FIGURES

TABLE DES TABLEAUX

Liste des abréviations

- ADS : Anomaly Detection Systems
- AFL : Asynchronous Federated Learning
- AI : Artificial Intelligence
- ANFIS : Systèmes d'inférence neuro-flous adaptatifs (Adaptive Neuro-Fuzzy Inference Systems)
- BNN : Binarized Neural Networks
- BVP : Impulsion de volume sanguin (Blood Volume Pulse)
- CNN : Convolution Neural Networks
- CPU : Unité centrale de traitement
- DAD : Deep Anomaly Detection
- DDoS: Distributed Denial of Service
- DL : Deep Learning
- DNN : Deep Neural Network
- DRL : Deep Reinforcement Learning
- ECG : Électrocardiographie (Electrocardiography)
- EDA : Activité électrodermale (Electrodermal Activity)
- EMG : Électromyographie (Electromyography)
- ENN : Encrypted Neural Network
- FL : Federated Learning
- FR : Reconnaissance faciale (Facial Recognition)
- GAN : Generative Adversarial Network
- GPU : Unité de traitement graphique
- GRU : Gated Recurrent Unit
- HIDS : Host Intrusion Detection Systems
- HRV : Variabilité de la fréquence cardiaque (Heart Rate Variability)
- IDS : Intrusion Detection Systems
- IIoT : Industrial Internet of Things
- IoT : Internet des objets
- LSTM : Long Short Term Memory
- ML : Machine Learning
- MLP : Multi-Layer Perceptron
- MITM : Man in the Middle
- NIDS : Network Intrusion Detection Systems
- **N-mode SVD :** N-mode Singular Value Decomposition
- **PCA :** Principal Components Analysis
- **QoS** : Quality of Service
- **ReLU :** Rectified Linear Unit

- **RSP :** Respiration (Respiration)
- **SVM :** Machines à vecteurs de support (Support Vector Machines)
- SKT : Température cutanée (Skin Temperature)
- SR : Reconnaissance vocale (Speech Recognition)
- STIN : Satellite-Terrestrial Integrated Networks
- SVD : Singular Value Decomposition
- VPN : Virtual Private Network
- WCN : Wireless Communication Network
- WSN : Wireless Sensor Network

I. Introduction général

L'Apprentissage Fédéré est une approche novatrice en matière d'apprentissage machine qui permet de former des modèles de manière collaborative tout en préservant la confidentialité des données. Cette méthode révolutionnaire ouvre de nouvelles perspectives pour le développement de solutions intelligentes dans divers domaines, de la santé à la sécurité en passant par les applications mobiles. En effet, en permettant aux appareils de collaborer sans partager leurs données brutes, l'Apprentissage Fédéré offre la possibilité de tirer parti de vastes ensembles de données distribuées sans compromettre la vie privée des utilisateurs.

Chapitre 1: Définition et Fonctionnement de l'Apprentissage Fédéré

Dans ce premier chapitre, nous explorerons en détail les fondements de l'Apprentissage Fédéré, en mettant en lumière son fonctionnement, ses avantages et ses applications potentielles. Nous examinerons également les principaux concepts et technologies sous-jacents qui permettent la mise en œuvre de cette approche collaborative.

Chapitre 2: Reconnaissance Faciale et détection d’intrusion

Le deuxième chapitre sera consacré à la reconnaissance faciale, une application majeure de l'Apprentissage Fédéré. Nous discuterons des principes de base de la reconnaissance faciale, des algorithmes et des outils de programmation utilisés pour développer des systèmes de reconnaissance faciale performants et sécurisés. En parallèle, nous aborderons également la détection d'intrusion, essentielle pour protéger les réseaux informatiques contre les accès non autorisés et les attaques malveillantes. Nous examinerons les méthodes de détection d'intrusion, les défis rencontrés et les technologies employées pour développer des systèmes plus efficaces et sécurisés. Ce chapitre explorera en détail les concepts, les techniques et les outils liés à la reconnaissance faciale et à la détection d'intrusion, soulignant leur importance dans le domaine de la sécurité informatique.

Chapitre 3: État de l'Art de l'Apprentissage Fédéré pour les Systèmes d'Intrusion

Dans ce chapitre, nous passerons en revue les avancées récentes dans le domaine de l'Apprentissage Fédéré appliqué à la détection d'intrusion. Nous examinerons les différentes approches, les défis techniques et les solutions proposées pour améliorer la sécurité des systèmes informatiques grâce à cette méthode d'apprentissage collaborative.

Chapitre 4: Implémentation de Modèle pour la Reconnaissance Faciale

Le dernier chapitre de ce mémoire se concentrera sur l'implémentation d'un modèle de reconnaissance faciale en utilisant l'Apprentissage Fédéré. Nous détaillerons les différentes étapes de prétraitement des données, la création du modèle CNN mobilenetv2, et l'évaluation des performances du modèle pour la reconnaissance faciale. Les résultats prometteurs obtenus ouvriront la voie à de futures avancées dans le domaine de la sécurité et de la surveillance basées sur la technologie de reconnaissance faciale.

Je vais offrir un aperçu approfondi de l'Apprentissage Fédéré, de la reconnaissance faciale et de leur application combinée pour la sécurité des systèmes informatiques. Il met en lumière les opportunités, les défis et les perspectives d'avenir de cette approche révolutionnaire qui promet de transformer la manière dont nous concevons et utilisons les technologies intelligentes.

Problématique

Comment l'apprentissage fédéré peut-il être optimisé pour améliorer la détection d'intrusion et la reconnaissance faciale tout en garantissant la confidentialité et la sécurité des données distribuées, et quelles sont les principales barrières techniques et réglementaires à surmonter pour son implémentation à grande échelle ?

Cette problématique explore les tensions entre la nécessité de modèles performants et la protection des données personnelles, en cherchant à identifier les solutions techniques et les cadres réglementaires nécessaires pour réaliser cet équilibre.

II. : Apprentissage fédère

Chapitre 1 : Apprentissage fédéré.

1.1 Introduction

L'apprentissage fédéré révolutionne la machine Learning en décentralisant l'entraînement des modèles, préservant ainsi la confidentialité des données. Contrairement aux méthodes traditionnelles, qui centralisent les données sur un serveur unique, cette approche permet aux appareils de collaborer tout en maintenant leurs données localement. Cela réduit les risques de compromission des données sensibles et renforce la sécurité des informations.

1.2 Définition et principe de base

Définition : est une méthode décentralisée d'apprentissage automatique où plusieurs dispositifs ou serveurs collaborent pour former un modèle de machine learning, en conservant leurs données d'entraînement localement. Cela permet de créer des modèles robustes tout en préservant la confidentialité et la sécurité des données. . **[2]**

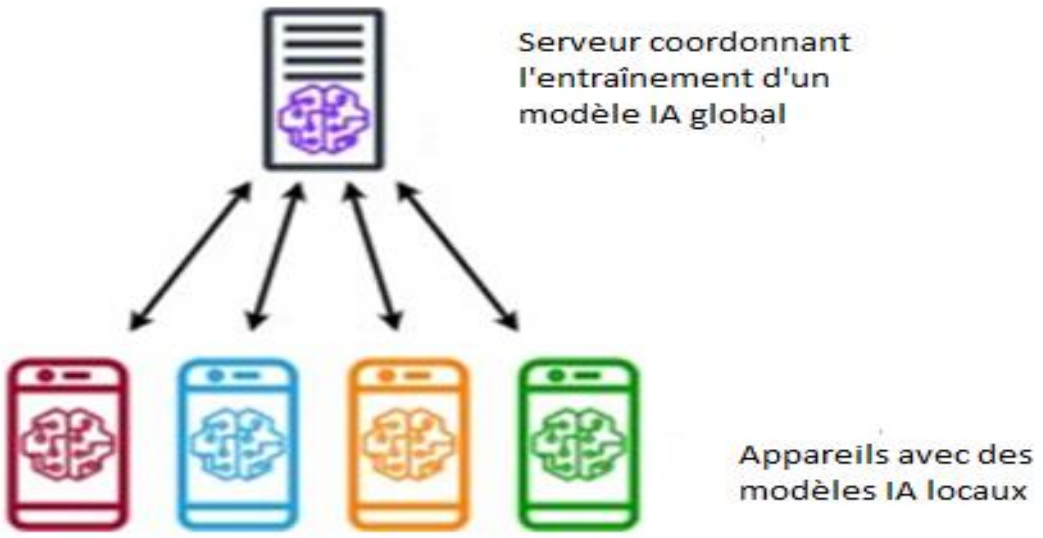

Figure 0-1: 1apprentissage fédéré ***[1].***

L'apprentissage fédéré, introduit par Google en 2016, vise à entraîner des modèles de machine Learning sur un réseau de périphériques décentralisés (comme les smartphones) ou des serveurs locaux. Chaque appareil entraîne un modèle localement avec ses propres données, puis seulement les paramètres (gradients) du modèle sont partagés avec un serveur central. Ce serveur agrège ces paramètres pour mettre à jour le modèle global, sans jamais accéder directement aux données brutes des appareils. **[2]**

1.3 Les principales étapes de l'apprentissage fédéré

L'apprentissage fédéré réinvente le développement des modèles d'IA en permettant à plusieurs appareils de contribuer à un modèle global tout en préservant la confidentialité des données. Le processus débute par la sélection d'appareils distants, suivie de la distribution d'un modèle initial pour un entraînement local sécurisé. Les résultats sont agrégés pour former un modèle global amélioré, favorisant une collaboration efficace tout en respectant la vie privée des utilisateurs.

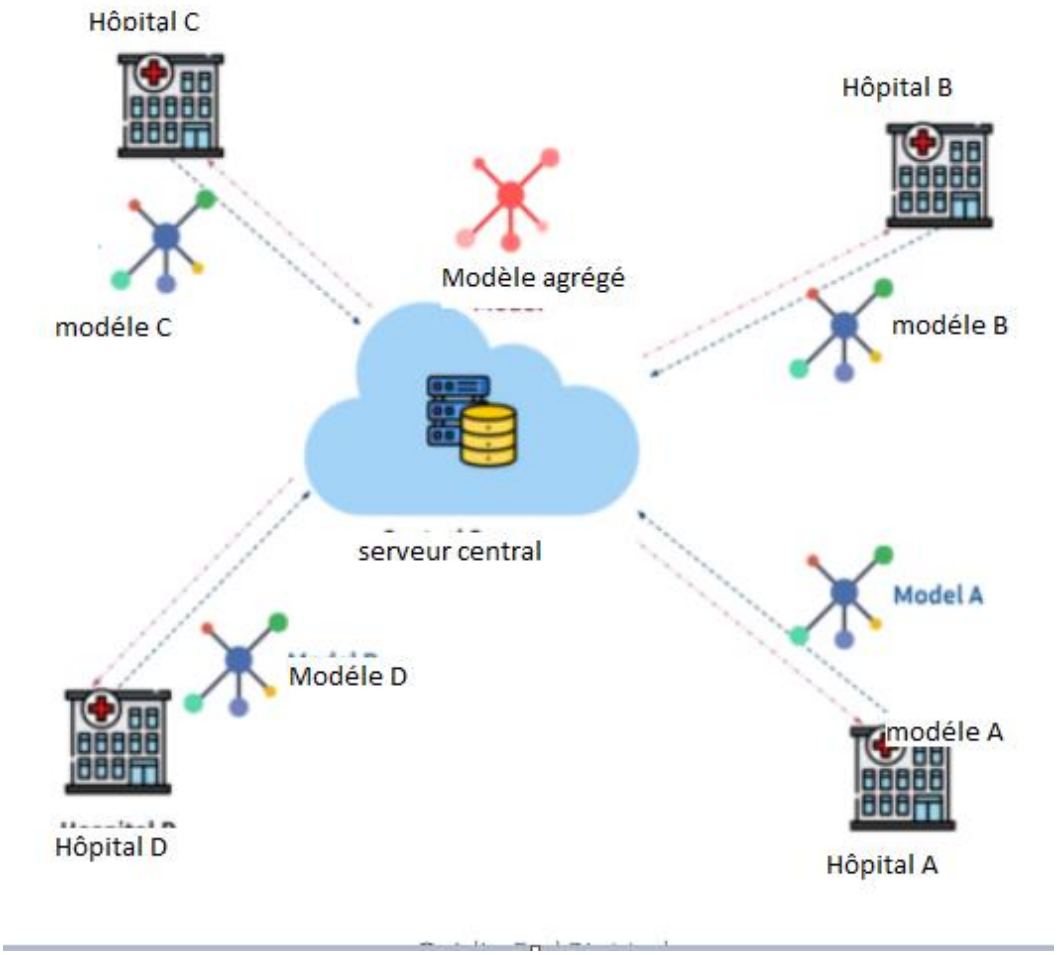

Figure 0-2: architecture générale de system fédéré ***[3].***

1.3.1 Initialisation

Description : Cette première étape consiste à initialiser un modèle global, souvent un modèle de machine learning comme un réseau de neurones. Le modèle est créé par le serveur central ou par un point central de coordination.

Processus : Un modèle initial, non entraîné ou pré-entraîné, est préparé.

Ce modèle global est ensuite envoyé aux appareils participants, tels que des smartphones, des ordinateurs ou des serveurs locaux.

1.3.2 Entraînement Local

Description : Chaque appareil participant reçoit le modèle global pour lancer l'entraîne sur ses propres données locales.

Processus : Les appareils utilisent leurs données locales pour entraîner le modèle pendant un certain nombre d'itérations ou pour une période de temps définie.

Chaque appareil effectue la rétro propagation pour ajuster les poids du modèle en fonction de ses données locales.

Cet entraînement est fait localement, de sorte que les données ne quittent jamais l'appareil.

1.3.3 Mise à Jour et Agrégation

Description : Après l'entraînement local, les appareils mettent à jour le modèle en envoyant les gradients (ou les poids ajustés) au serveur central.

Processus : Les gradients ou les poids ajustés sont chiffrés pour des raisons de sécurité, puis envoyés au serveur central.

Le serveur central reçoit ces mises à jour de plusieurs appareils.

Le serveur central agrège ces mises à jour, généralement en calculant une moyenne pondérée des poids ou des gradients reçus.

Cette agrégation permet de mettre à jour le modèle global en tenant compte des ajustements apportés par tous les appareils participants.

1.3.4 Distribution

Description : Le modèle global mis à jour est ensuite redistribué aux appareilsparticipants pour une nouvelle itération d'entraînement.

Processus : Le modèle global mis à jour est envoyé à tous les appareils participants.

Les appareils reçoivent le modèle mis à jour et commencent une nouvelle phase d'entraînement local avec leurs données.

Ce cycle d'entraînement local, de mise à jour et d'agrégation se répète jusqu'à ce que le modèle atteigne un niveau de performance satisfaisant ou qu'un certain nombre d'itérations soit complété. **[4]**

1.4 Avantages de l'Apprentissage Fédéré

Confidentialité et Sécurité : Les données restent sur les appareils locaux,minimisant ainsi le risque de violation de la vie privée et des fuites de données.

Efficacité en Bande Passante : Seuls les paramètres du modèle (plutôt queles données brutes) sont échangés, ce qui réduit la consommation de bande passante.

Personnalisation : Les modèles peuvent être personnalisés pour des groupesspécifiques d'utilisateurs ou des appareils sans nécessiter un accès aux données globales.

1.5 Défis et Limites

- Communication et Latence : Le processus d'échange fréquent des paramètres du modèle peut entraîner des délais et nécessite une bonnegestion de la bande passante.
- Hétérogénéité des Données : Les données peuvent varier considérablement entre les appareils, elle se réfère à la variation des données ce qui peut entraîner des défis dans la convergence du modèle global.
- Limitations Algorithmiques : Les algorithmes traditionnels peuvent ne pas être directement applicables à l'apprentissage fédéré en raison de contraintes de communication et de confidentialité. **[5]**

1.6 Applications de l'Apprentissage Fédéré

Figure 0-3 : application de l'apprentissage fédéré ***[6].***

- **Santé** : Apprentissage fédéré est utilisé pour entraîner des modèles sur des données médicales réparties dans différents hôpitaux, aidant à préserver laconfidentialité des patients.
- T**echnologie Mobile** : Les smartphones utilisent l'apprentissage fédéré pour améliorer des fonctionnalités comme la saisie prédictive ou la reconnaissance vocale sans envoyer les données des utilisateurs aux serveurs centraux.
- **Industrie Financière** : Les banques utilisent l'apprentissage fédéré pour développer des modèles de détection de fraude sans partager les données sensibles des clients entre les institutions. **[6]**

1.7 Études de Cas

1.7.1 Google Keyboard (Gboard)

Chapitre 1 : Apprentissage fédéré.

Figure 0-4 : logo de Google keyboard. [7]

Google a appliqué l'apprentissage fédéré pour améliorer le clavier Gboard, permettant aux utilisateurs de bénéficier de meilleures suggestions de saisie prédictive sans compromettre leur confidentialité. Les modèles sont entraînés sur les appareils des utilisateurs en utilisant les données locales, puis les mises à jour des modèles sont agrégées de manière sécurisée pour améliorer le modèle global. Cette approche innovante garantit que les informations personnelles des utilisateurs restent sur leurs appareils tout en permettant à Google d'améliorer continuellement la précision et la pertinence des prédictions de texte fournies par Gboard. Cela montre comment l'apprentissage fédéré peut être appliqué de manière pratique pour offrir des services de haute qualité tout en respectant rigoureusement la confidentialité des données des utilisateurs. **[7]**

1.7.2 Initiative OpenMined

Figure 0-5: logo de openmined. ***[7]***

OpenMined est une communauté open-source dédiée au développement d'outils et de frameworks pour l'apprentissage fédéré et la confidentialité différentielle. Leur mission est de rendre l'apprentissage automatique et l'analyse des données plus accessibles tout en préservant la confidentialité des données personnelles. En favorisant la collaboration ouverte et la transparence, OpenMined vise à créer des solutions technologiques innovantes qui permettent aux individus et aux organisations de bénéficier des avantages de l'intelligence artificielle sans compromettre la sécurité des informations sensibles. [7]

1.8 Techniques Avancées en Apprentissage Fédéré

- Confidentialité Différentielle : Ajout de bruit aux mises à jour du modèle pour garantir qu'aucune donnée individuelle ne peut être reconstruite à partir des gradients agrégés.
- Cryptographie Homomorphe : permet de réaliser des calculs sur des données chiffrées sans avoir besoin de les déchiffrer, assurant ainsi que les informations sensibles ne sont jamais exposées.
- Moyennage Fédéré (Federated Averaging) : Une technique populaire d'agrégation oùles mises à jour locales des modèles sont moyennées pour obtenir la mise à jour globale. **[8]**

1.9 Conclusion

L'utilisation de l'apprentissage fédéré transforme l'entraînement et la mise en œuvre des modèles de machine Learning en offrant un processus décentralisé qui garantit la confidentialité des données. Cela offre de nouvelles opportunités dans des domaines où la préservation de la vie privée est essentielle, même si des obstacles techniques et logistiques doivent être surmontés afin d'exploiter pleinement son potentiel. Le deuxième chapitre examine de manière approfondie deux domaines essentiels : la reconnaissance faciale, comprenant les méthodes de vérification des visages et les problèmes de confidentialité liés à la diversité des images, et la détection d'intrusion, mettant en évidence les techniques pour repérer les activités. Malveillantes dans le trafic réseau.

III. : Reconnaissance faciale et détection d’intrusion

1.10Introduction

L'évolution rapide des technologiques dans divers domaine, notamment dans le domaine de reconnaissance faciale qui est devenu comme une biométrie pour chaque personne et la détection d'intrusion pour surveiller, détecter et prévenir les accès non autorisé aux systèmes et réseaux, Ce chapitre explore les concepts, techniques, et applications de ces deux technologies, ainsi que les défis associés à leur mise en œuvre.

1.11La Reconnaissance Faciale

Définition :

La reconnaissance faciale est une technologie biométrique utilisée pour identifier, authentifier et vérifier l'identité d'une personne en analysant et en comparant ses caractéristiques faciales uniques, telles que la forme du visage, les proportions, les contours et les motifs distinctifs. **[25]**

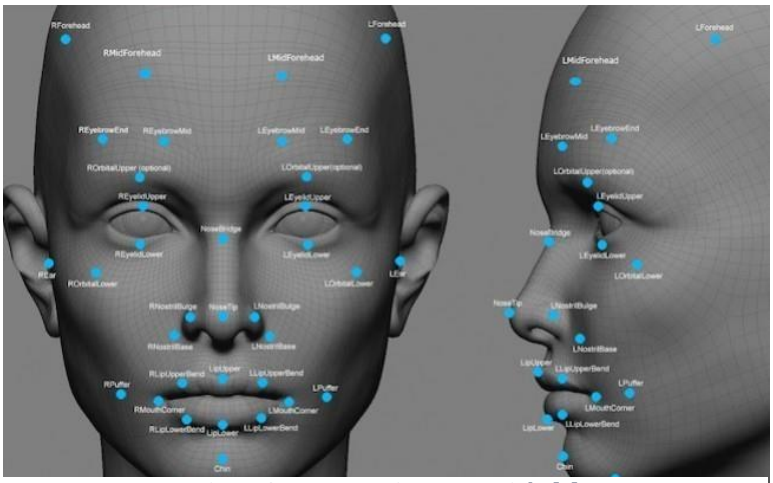

*Figure 0-1: Reconnaissance Faciale **[9]***

La reconnaissance faciale utilise les caractéristiques uniques du visage pour identifier et authentifier les individus de manière automatisée. Cette technologie joue un rôle croissant dans divers domaines grâce aux progrès de l'intelligence artificielle.

1.11.1 Principe de Fonctionnement

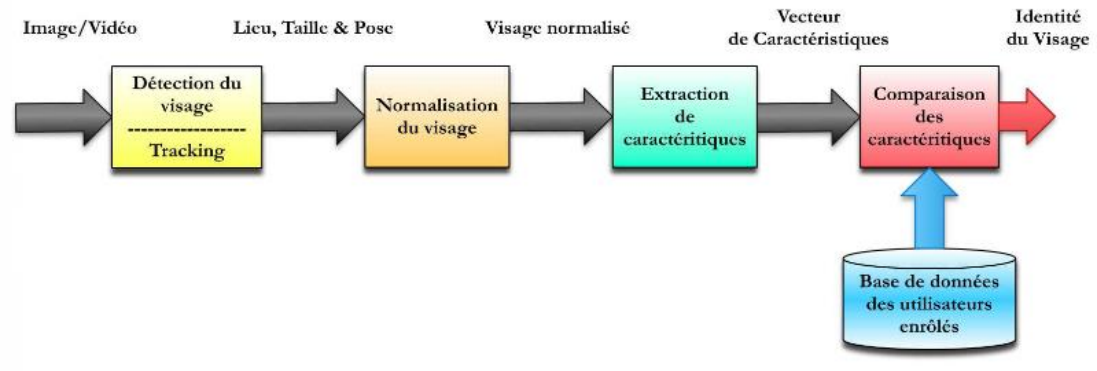

Figure 0-2 les technique principale de la reconnaissance faciale. [10]

L'illustration présente les différentes étapes d'un dispositif de reconnaissance faciale. Nous vous présentons une explication de chaque principe illustré :

- Image/Vidéo : L'opération débute par l'acquisition d'une photographie ou d'une vidéo avec des visages.
- Aperçu du visage : L'objectif de cette étape est de repérer et de suivre les visages présents dans l'image ou la vidéo. Des algorithmes sont employés afin de repérer les zones où se trouvent les visages.
- détection : Une fois que les visages ont été détectés, les données concernant leur position, leur taille et leur orientation sont établies.
- Régulation du visage : On normalise les visages détectés afin de garantir leur taille uniforme et leur orientation correcte. Cela peut nécessiter des procédures telles que l'ajustement et la réadaptation des visages.

- Extraction de propriétés : consiste à identifier les caractéristiques uniques du visage, comme la forme et les points clés, pour permettre l'identification automatisée des individus. Ce processus utilise des techniques avancées de traitement d'images pour garantir précision et fiabilité.

- Analyse des traits : Les traits extraits sont comparés à ceux stockés dans une base de données afin de déterminer ou confirmer l'identité des visages.

- Liste des utilisateurs inscrits: Les vecteurs de caractéristiques des utilisateurs enregistrés sont stockés dans la base de données. C'est en utilisant cette base de données qui sont comparées les nouveaux vecteurs de caractéristiques afin de procéder à la reconnaissance.

- Identification du Visage: consiste à déterminer l'identité d'une personne en comparant ses caractéristiques faciales extraites avec celles d'une base de données. Lorsqu'une correspondance est trouvée, l'identité associée est validée, permettant ainsi une identification précise et automatisée à travers le système de reconnaissance faciale.

Les systèmes de reconnaissance faciale utilisent cette séquence d'étapes dans différentes applications, allant de la sécurité à la gestion des identités et des accès. **[11]**

1.11.2 Techniques et Algorithmes

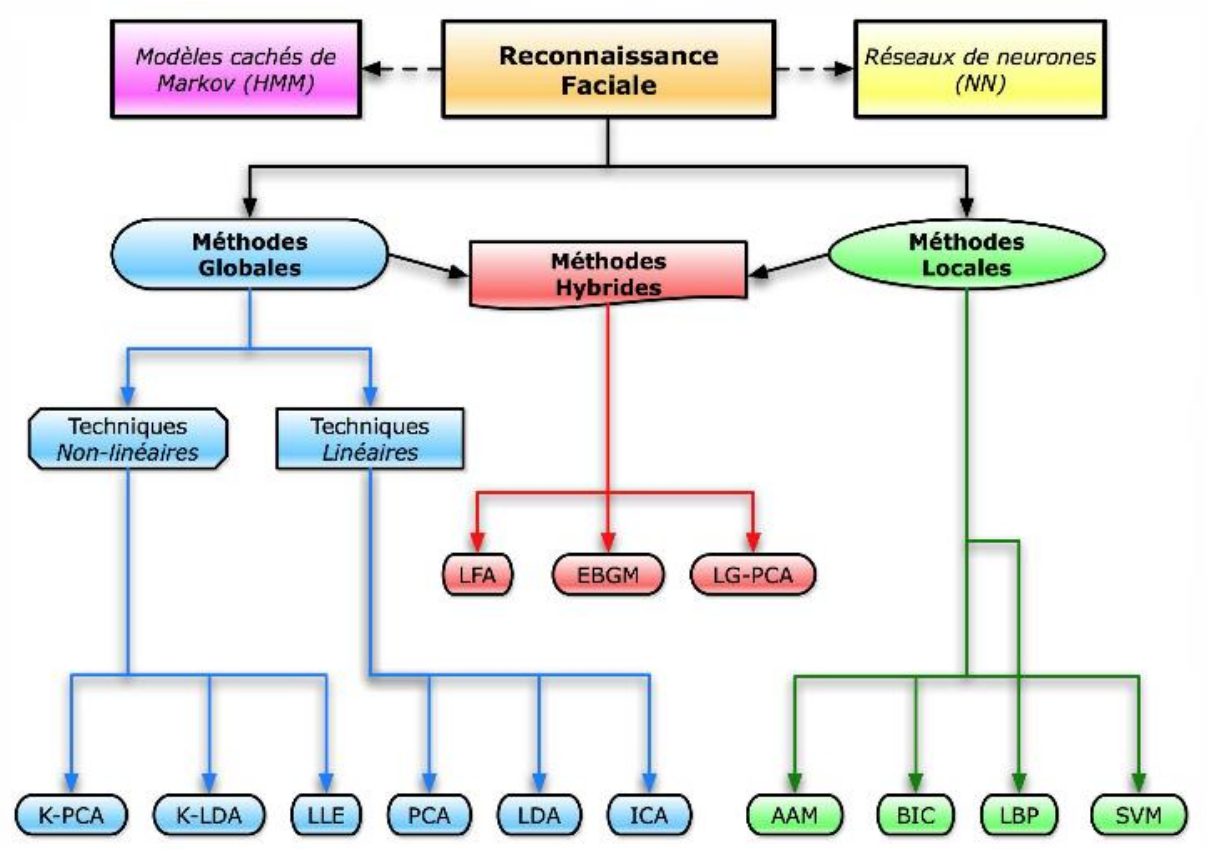

Figure 0-3: classification des algorithmes principaux de reconnaissance faciale. ***[12]***

On peut classer les algorithmes de reconnaissance faciale en différentes catégories :

Méthodes Cachées de Markov (HMM)

- -HMM (Hidden Markov Models) : Modèles probabilistes qui représentent des processus ayant des états cachés. Utilisés pour modéliser les variations temporelles et séquentielles des caractéristiques faciales. Réseaux de Neurones (NN)
- NN (Neural Networks) : Modèles d'apprentissage profond qui simulent le fonctionnement du cerveau humain pour identifier et reconnaître des motifs complexes dans les images faciales.
  Méthodes Globales

Techniques Non-linéaires

- K-PCA (Kernel Principal Component Analysis) : Extension de l'analyse en composantes principales (PCA) qui utilise des fonctions noyaux pour capturer des relations non linéaires dans les données faciales.
- K-LDA (Kernel Linear Discriminant Analysis) : Variante de l'analyse discriminante linéaire (LDA) qui applique des fonctions noyaux pour améliorer la séparation des classes dans un espace de caractéristiques non linéaire.
- -LLE (Locally Linear Embedding) : Méthode de réduction de la dimensionnalité qui préserve les relations de voisinage local pour mieux représenter les structures non linéaires des visages.
  Techniques Linéaires
- PCA (Principal Component Analysis) : Technique de réduction de la dimensionnalité qui identifie les axes de variation maximale dans les données faciales pour une représentation plus compacte.
- LDA (Linear Discriminant Analysis) : Méthode de classification qui projette les données dans un espace où les classes sont mieux séparées, maximisant ainsi la variance entre les classes et minimisant la variance intra-classe.
- -ICA (Independent Component Analysis)** : Technique qui sépare les données en composants statistiquement indépendants, souvent utilisée pour extraire des caractéristiques significatives des visages.

Méthodes Hybrides

- LFA (Local Feature Analysis) : Méthode qui analyse des caractéristiques locales du visage, telles que les yeux, le nez, et la bouche, pour une reconnaissance plus précise.
- EBGM (Elastic Bunch Graph Matching) : Technique qui utilise des graphes de caractéristiques locales et des graphes élastiques pour matcher et reconnaître les visages malgré les variations d'expression et de pose.
- -LG-PCA (Local Gabor PCA) : Combinaison de filtres de Gabor, qui capturent des informations locales de texture, avec PCA pour une analyse plus robuste des caractéristiques faciales.

Méthodes Locales

- AAM (Active Appearance Model) : Modèle qui combine la forme géométrique et la texture pour ajuster un modèle de visage à une image faciale et en extraire des caractéristiques.
- BIC (Bayesian Intrapersonal/Interpersonal Classifier) : Classificateur bayésien qui sépare les variations intrapersonnelles (différences au sein de la même personne) des variations interpersonnelles (différences entre différentes personnes).
- LBP (Local Binary Pattern) : Descripteur de texture qui transforme les motifs locaux d'une image en histogrammes binaires, utilisé pour capturer des informations de texture fines des visages.
- SVM (Support Vector Machine) : Algorithme de classification supervisée qui trouve l'hyperplan optimal pour séparer les différentes classes de données, souvent utilisé pour la reconnaissance faciale.
-
- Ces explications fournissent un aperçu des principales techniques et méthodes utilisées dans le domaine de la reconnaissance faciale, en mettant en évidence leur approche et leur application spécifiques.. **[13]**

1.11.3 Applications

- **Sécurité et surveillance** : Utilisée dans les systèmes de vidéo surveillance pour identifier les criminels et prévenir les intrusions.
- **Contrôle d'accès** : Utilisée dans les systèmes de contrôle d'accès auxbâtiments et appareils.
- **Commerce et marketing** : Utilisée pour analyser le comportement des clients et personnaliser les offres. **[14]**

1.11.4 Défis

- **Précision et préjugés :** Les algorithmes peuvent comporter des préjugés en fonction du genre, de l'âge et de l'origine ethnique.

- **Préserver la vie privée :** Il est essentiel de se préoccuper des questions de vie privée et d'éthique.

- Les variations de luminosité, les angles de vue et les expressions faciales peuvent

influencer la précision en fonction des conditions environnementales. **[14]**

1.12La Détection d'Intrusion

1.12.1 Principe de Fonctionnement

*Figure 0-4 : intrusion [**15**]*

La détection d'intrusion implique la surveillance des systèmes et des réseaux pour détecter des activités suspectes et potentiellement malveillantes. Les IDS peuvent être classés en deux catégories principales :

- **Basés sur les signatures**: Ils détectent les intrusions en comparant l'activité réseau à des signatures d'attaques connues, des modèles spécifiques de trafic ou de comportement associés à des tentatives d'intrusion précédemment identifiées.
- **Basés sur les anomalies**: Détectent les intrusions en identifiant des déviations par rapport au comportement normal du système. **[16]**

1.12.2 Techniques et Algorithmes

Il est crucial de détecter les intrusions en utilisant des méthodes de signature et d'anomalie, qui sont indispensables pour assurer la sécurité des réseaux. La combinaison de ces méthodes renforce la prévention des cyberattaques, même si leur gestion est complexe, et est adaptée pour faire face aux nouvelles menaces. **[16]**

- **Analyse des logs :** Surveillance des journaux d'événements pour détecter des activités anormales.
- **Détection par signature** : Utilisation de bases de données de signatures d'attaques pour identifier des menaces connues.
- **Détection par anomalies** : Utilisation de l'apprentissage automatique pour modéliser le comportement normal du système

1.12.3 Applications

• La sécurité des réseaux vise à préserver les réseaux d'entreprise des intrusions et des attaques.
• Gestion de la sécurité des systèmes : Vérification des systèmes d'exploitation et des applications afin de repérer les comportements dérangeants.
• Internet des objets (IoT) : Contrôle des dispositifs IoT afin de prévenir les attaques. **[17]**

1.12.4 Défis

• Les IDS peuvent émettre des alertes pour des activités légitimes, ce qui entraîne la création de faux positifs.
• La complexité des attaques : Les attaquants mettent en œuvre des méthodes de plus en plus avancées afin d'éviter la détection.
• Les IDS doivent avoir la capacité de traiter de grandes quantités de données en temps réel sans compromettre les performances du système. **[18]**

1.13Conclusion

La reconnaissance faciale et la détection d'intrusion jouent un rôle essentiel dans la protection des systèmes et des réseaux. Même si ces technologies font face à des défis importants, elles profitent de progrès constants en matière d'algorithmes et de techniques, ce qui permet d'offrir des applications innovantes et performantes. En ce qui concerne le prochain chapitre qui est l'état de l'art, il est primordial de prendre en compte les avancées récentes et les études en cours pour améliorer la précision, la résistance et la sécurité de ces systèmes. Il est également essentiel de prendre en compte les aspects éthiques et de protection de la vie privée, en particulier en ce qui concerne la collecte et l'exploitation des données biométriques et des données sur les comportements réseau.

IV. : État de l'Art de l'Apprentissage Fédéré pour les Systèmes d'Intrusion.

1.14Introduction

Le apprentissage fédère est une approche de l'apprentissage machine qui permet d'entraîner des modèles de manière collaborative sans que les données ne quittent les appareils des utilisateurs. Cette technique présente un intérêt particulier dans le domaine dela détection d'intrusions et de la reconnaissance faciale, où la confidentialité des données est cruciale. L'apprentissage fédère pour Intrusion Détection System et le apprentissage fédère pour la reconnaissance faciale se distinguent par leur capacité à exploiter les informations locales des appareils tout en préservant la vie privée des utilisateurs, Dans ce chapitre, nous allons explorer les concepts clés et les recherches en apprentissage fédéré et la reconnaissance faciale, en mettant l'accent sur les techniques d'apprentissage fédéré dans la détection d'intrusion et les réseaux neuronaux avancés. Nous examinerons les algorithmes, les défis, et les solutions proposés, ainsi que les applications pratiques et études de cas pertinentes, notamment les approches décentralisées pour préserver la confidentialité des données.

1.15Travaux connexes

Omar Abdel Waheb, Azzam Mourad, Hadi Otrok et Tarik Taleb :

Dans cet article, les auteures dans **[19]** ont proposé une étude de classification à plusieurs niveaux, critères intéressants et orientations futures offre une analyse approfondie de l'apprentissage automatique fédéré, mettant en évidence les défis actuels, les approches de pointe et les orientations futures. Dans ce domaine innovant. Un schéma de classification en trois niveaux a été élaboré afin de classer la littérature existante sur l'apprentissage machine fédéré, en mettant en évidence les critères potentiels pour la recherche à venir. Ils mettent en évidence l'importance de préserver la confidentialité des utilisateurs, la nature non autonome et non uniforme des données, ainsi que les risques potentiels pour le processus d'apprentissage distribué. L'objectif de cet articleest de fournir des instructions précises et des conseils pour concevoir des solutions d'apprentissage machine fédérée plus performantes et sécurisées, afin d'orienter les chercheurs et les professionnels dans ce domaine en plein essor.

Thien Duc Nguyen, Samuel Marchal, Markus Miettinen ,HosseinFereidooni ,N. Asokan et Ahmad-Reza Sadeghi :

Dans L'article, les auteures dans **[20]** ont présente un système innovant pour détecter les appareils IoT compromis. Les auteurs ont développé un système fédéré de détection d'anomalies auto-apprenant pour l'IoT, un système distribué auto-apprenantbasé sur des modèles de détection d'anomalies spécifiques aux types d'appareils IoT. En utilisant une approche unique de représentation des paquets réseau comme des symboles, le système est capable de détecter efficacement les comportements anormaux des appareils IoT sans nécessiter d'intervention humaine ni de données étiquetées. Une caractéristique clé de un système fédéré de détection d'anomalies auto-apprenant pour l'IoT est son utilisation de l'apprentissage fédéré pour agréger les profils de détection d'anomalies, ce qui permet une détectionprécise des attaques tout en réduisant les fausses alarmes. Les expériences menéesavec plus de 30 appareils IoT ont démontré que D¨I O T est rapide et efficace, avec un taux de détection élevé de 95,6 % et aucune fausse alarme signalée. En résumé, cet article propose une approche prometteuse pour renforcer la sécurité des appareils IoT en utilisant des techniques d'apprentissage automatique et d'analysedes anomalies spécifiques aux types d'appareils.

Ilhan Firat Kilincer, Fatih Ertam et Abdulkadir Sengur :

Dans ce l’article, Kilincer et ses collègues proposent dans **[21]** une étude approfondie des méthodes d'apprentissage automatique pour détecter les intrusions en cyber sécurité. Les chercheurs évaluent les résultats de diverses méthodes en se basant sur des échantillons de données spécifiques et examinent les atouts et les points faibles de chaque approche. L'objectif de leur étude est de fournir des données précieuses afind'améliorer la détection des intrusions et de renforcer la sécurité des systèmes logiciels.

Sawsan Abdul Rahman, Hanine Tout, Chamseddine Talhi et AzzamMourad :

Dans cet article, les auteurs dans **[22]** ont proposé une approche face à la croissance des cyberattaques visant les appareils IoT, l'approche centralisée traditionnelle présente des limites en termes de scalabilité et de protection des données. Le schéma proposé permet aux appareils IoT de collaborer et de partager des connaissances tout en garantissant laconfidentialité des données et en améliorant la précision de la détection.

L'apprentissage fédéré maintient la confidentialité des données en effectuant l'entraînement et l'inférence des modèles de détection localement. L'article met en avant les avantages d'une approche décentralisée pour la détection d'intrusions dans les appareils IoT, en soulignant la nécessité de calculs décentralisés dans un environnement où les données sont largement réparties. Une évaluation approfondieest réalisée en utilisant le jeu de données NSL-KDD pour comparer l'efficacité du partage et de l'agrégation des modèles dans un contexte d'apprentissage fédéré par rapport aux approches centralisées et d'apprentissage sur appareil.

M. Alex O. Vasilescu et Demetri Terzopoulos :

Les auteurs ont proposé dans **[23]** une approche novatrice utilisant l'algèbre multilinéaire pour l'analyse des images faciales en vue d'améliorer les taux de reconnaissance faciale. Les auteurs appliquent cette méthode, appelée TensorFaces, pour obtenir une représentation plus efficace des ensembles d'images faciales en séparant les différents facteurs tels que les géométries faciales, les expressions, les poses de têteet les conditions d'éclairage. Comparé aux méthodes traditionnelles telles que les eigenfaces, TensorFaces offre des taux de reconnaissance faciale améliorés. Cette approche prometteuse ouvre de nouvelles perspectives pour la reconnaissance faciale dans des domaines tels que la biométrie et l'interaction homme-machine.

M. Egger, M. Schels, M. L. Braun, et M. Riegler :

Dans cet article, les auteurs **[24]** ont suggéré d'étudier l'importance de la reconnaissance des émotions dans les interactions entre les individus et les ordinateurs, ainsi que ses applications dans différents secteurs tels que les maisons intelligentes, l'industrie 4.0, la santé personnelle et la réadaptation. Il étudie également diverses approches pour reconnaître les émotions et leur pertinence pour diverses applications. L'article souligne l'importance grandiose de la technologie de reconnaissance des émotions et son potentiel d'amélioration des interactions entre les individus et les ordinateurs dans différents environnements.

1.16Tableau comparatifs

Auteur	Dataset	objectifs	Modelé	Résultat
Omar Abdel Wahab Azzam Mourad Hadi Otrok Tarik Taleb	CIFAR-10 dataset IID dataset	cet article vise à fournir un guide complet pour les chercheurs et lespraticiens intéressés par l'apprentissage machine fédéré, en mettant en avant les défis actuels, les solutions existantes et les pistes de recherche futures dans ce domaine en évolution rapide	Distributed Learning Parallel Learning Ensemble Learning	
Thien Duc Nguyen Samuel Marchal	Activity dataset Deploymentdataset	Présenter D¨I O T, un système pour détecter lesappareils IoT compromis.	Développement de D¨IO T, un système distribué auto-apprenant pour la détection des appareils IoT compromis. Utilisation d'une	D¨I O T a démontré une efficacité élevée avec un taux de détection de 95,6 % et aucune fausse alarme signalée lors de l'évaluation. Le système a montré une rapidité de

Markus Miettinen Hossein Fereidooni N. Asokan Ahmad-Reza Sadeghi	Attack dataset	Utiliser une approche de détection d'anomalies spécifique aux types d'appareils pour une détection précise des attaques sans générer de fausses alarmes. Proposer un modèle d'apprentissag efédéré pour agréger les profils de détection d'anomalies. Réaliser une analyse expérimentale approfondie avec plus de 30 appareils IoT pour démontrer l'efficacité et la rapidité de D¨I OT dans la détection des appareils compromis. Fournir un ensemble de données d'attaque et	approche de détection d'anomalies spécifiqueaux types d'appareils pour profiler les comportements des appareils et détecter les attaques. Représentation des paquets réseau comme des symbolespour permettre l'utilisation d'une technique d'analyse linguistique efficace dans la détection desanomalies. Application d'une approche d'apprentissage fédéré pour agréger les profils de détection d'anomalies pour la détection des intrusions. Réalisation d'une analyse expérimentale approfondie avec plusde 30 appareils IoT pour évaluer la rapidité et l'efficacité de D¨I O T dans la détection des appareils compromis. Collecte de datasets, y compris un dataset d'activité, un dataset de déploiement et un dataset d'attaque, pour évaluer la performance de D¨I OT dans des scénarios	détection,avec un temps moyen de détection de 257 ± 194 ms pour divers scénariosd'attaque. D¨I O T a été capable dedétecter les attaques même à un stade précoce, avant que les attaques ne se propagent. Les résultats ont montréque D¨I O T peut détecter les attaques surles appareils IoT sans générer de faux positifs, ce qui le rend adapté à une utilisation dans des environnements réels. L'utilisation de l'apprentissage fédéré a permis d'améliorer la performance du système en agrégeant les profils de détection d'anomaliesde manière efficace.

		rendre l'implémentation de D¨I O T disponible pour la recherche.	réels.	
Ilhan Firat Kilincer, Fatih Ertam Abdulkadir Sengur		Réaliser une étude comparative desméthodes d'apprentissage automatique pour la détection d'intrusions en cybersécurité. Évaluer les performances des différentes approches en utilisant des jeuxde données spécifiques. Analyser les avantages et leslimites de chaque méthodepour la détection d'intrusions. Fournir des informations précieuses pour améliorer la détection des intrusions et renforcer la sécurité des	Lightweight, Usable Convolution NeuralNetworks (CNN) (LUCID) pour la détection DDoS . Apprentissage par imitation combiné à l'apprentissage fédérépour une meilleure sécurité et protection contre les attaques d'ingénierie inverse . Utilisation d'algorithmes d'apprentissage automatique tels que les arbres de décisionboostés par gradient et les machines à vecteurs de support pour la détection d'intrusion . Techniques de contrôle de structure variable intelligent combinées à des réseaux neuronaux artificiels pour estimer et compenser les attaques initiées	Le système D¨IOT a démontré une précision de 95,6% dans la détection des anomalies en moyenne en 257 ms, ce qui le rend adapté auxappareils IoT à faible consommation d'énergie et aux réseaux de capteurs qui dépendent de la vitesse de l'IDS. Le système a également montré des taux de fausses alarmes exceptionnellement bas dans des scénarios en temps réel.

		systèmes informatiques.	dansle lien avant des systèmes cyber-physiques non linéaires.	
Sawsa nAbdul Rahma n Hanine Tout Chamseddin eTalhi Azzam Mourad.	NSL-KDD dataset	Présenter un schéma d'apprentissage fédéré pour la détection d'intrusions dansl'Internet des objets (IoT). Évaluer l'efficacitéde ce schéma en comparaison avec des approches centralisées et d'apprentissag esur appareil. Mettre en avant l'importance de préserver la confidentialité desdonnées générées par les appareils IoT tout en réduisant la surcharge de communication. Explorer comment l'apprentissage fédéré peut garantir des performances comparables à l'approche centralisée tout en assurant la confidentialité desdonnées.	Entraînement et inférence des modèlesde détection localement sur les appareils IoT pour préserver la confidentialité desdonnées. Communication desmises à jour des modèles avec un serveur distant pour agréger les informations et partager un modèle amélioré avec les appareils participants. Utilisation du jeu de données NSL-KDD pour évaluer l'efficacitédu schéma proposé en comparaison avec des approches centraliséeset d'apprentissage sur appareil. Réalisation d'une analyse empirique des résultats expérimentaux pour mettre en évidence la robustesse et les avantages du modèle de détection basé sur l'apprentissage fédéré	Une efficacité démontréedu schéma proposé par rapport aux approches centralisées et d'apprentissage sur appareil. Une préservation de la confidentialité des données générées par lesappareils IoT tout en maintenant des performances proches del'approche centralisée. Des performances comparables à l'approchecentralisée et une amélioration par rapport aux modèles distribués non agrégés entraînés sur les appareils. Des résultats expérimentaux montrant une précision élevée et une robustesse du modèle de détection basé sur l'apprentissage fédéré, avec des performances proches de l'approche centralisée.

M. Alex O. Vasilescu et Demetri Terzopoulos	base de données d'images faciales de Weizmann.	Proposer une approche basée sur l'algèbre multilinéaire pour l'analyse et la représentation des ensembles d'images faciales. Développer une méthode, appelée TensorFaces, quipermet de séparer et de représenter de manière efficaceles différents facteurs influençant la formation des images faciales, tels que les expressions, les poses de tête, lesconditions d'éclairage. Comparer les performances de TensorFaces avecles méthodes traditionnelles telles que les eigenfaces pour la reconnaissance faciale. Explorer les applications potentielles de cette approche	Utilisation de l'algèbre multilinéaire pour représenter les ensembles d'images faciales sous forme detenseurs. Application de l'algorithme "N-mode SVD" (Singular Value Decomposition) comme une extension multilinéaire de la SVD matricielle pour décomposer les tenseurs d'images faciales et séparer les différents facteurs influençant la formation des images. Développement de l'approche TensorFacesqui exploite cette représentation multilinéaire pour améliorer les taux de reconnaissance faciale par rapport aux méthodes traditionnelles comme les eigenfaces. Comparaison des performances de TensorFaces avec les approches basées sur PCA (Principal Components Analysis) pour évaluer son efficacité dans des scénarios impliquant des variations de points de vue et d'éclairage.	Expérience de reconnaissanc e : Entraînement : 23 personnes, 3 points de vue, 4 éclairages Test : 23 personnes,2 points de vue, 4 éclairages Taux de reconnaissance avec PCA : 61% Taux de reconnaissance avecTensorFaces : 80% Expérience de reconnaissanc e : Entraînement : 23 personnes, 5 points de vue, 3 éclairages

		dans des domaines tels que la biométrie,la surveillance, l'interaction homme-machine.		
M. Egger, M. Schels, M. L. Braun,et M. Riegler.		Fournir un aperçu des méthodes de reconnaissance des émotions. Comparer l'applicabilité de ces méthodes ense basant sur desétudes existantes. Permettre aux praticiens, chercheurs et ingénieurs de trouver un système le plusadapté à certaines applications.	Electroencéphalographie (EEG) : Utilisée pour déterminer les émotionsavec une grande précision, mais nécessiteun environnement clinique en raison de sa configuration chronophage et de sa sensibilité au bruit. Reconnaissance faciale (FR) : Outil puissant pourla reconnaissance des émotions sans contact physique avec le patient,utilisant une webcam connectée à une unité informatique. Autres paramètres physiologiques : Les	Précision de classification de 89.29 % pour différencier la tristesse etle bonheur en analysant le SKT . Utilisation de l'EMG pour mesurer la tension musculaire liée au stress mental et la corrélation avec l'augmentation de la valence . Système proposé en 2010pour reconnaître les émotions basé sur la réponse galvanique de la peau (GSR) et l'EMG, liantle GSR à l'excitation et l'EMG à la valence des Sujets.

Tableau 0-1: tableau comparatif

1.17Discutions sur les travaux

Les recherches exposent la rapidité de l'évolution et l'importance de l'apprentissage fédéré pour préserver la confidentialité des données et améliorer l'efficacité des modèles d'enseignement. Les diverses méthodes et les résultats obtenus mettent en évidence les difficultés actuelles, comme la protection de la vie privée et l'amélioration de la précision des modèles, tout en proposant des perspectives prometteuses pour la recherche à venir.

Ces recherches mettent également en évidence l'utilisation de l'apprentissage fédéré dans différents domaines, tels que le cyber sécurité et la reconnaissance faciale, en mettant en évidence comment cette technologie peut répondre aux besoins spécifiques de chaque domaine tout en offrant des avantages importants en matière, De sécurité et de détection.

1.18Point fort et critique :

Wahab, O. A., Mourad, A., Otrok, H., & Taleb, T. (2021):

- **Points forts :** Classification multi-niveaux, critères désirables et orientations futures, offrant une vue d'ensemble complète de l'apprentissage machine fédéré.
- **Critiques :** Peut nécessiter des mises à jour régulières pour suivre l'évolution rapide du domaine.

Thien Duc Nguyen, Samuel Marchal, Markus Miettinen, Hossein Fereidooni, N. Asokan, et Ahmad-Reza Sadeghi :

- **Points forts :** Approche innovante pour la détection d'intrusions IoT, spécifique aux types d'appareils, offrant une détection précise.
- **Critiques :** Peut nécessiter des tests supplémentaires pour valider l'efficacité dans divers scénarios.

Ilhan Firat Kilincer, Fatih Ertam et Abdulkadir Sengur :

- **Points forts :** Aborde les concepts, défis et orientations futures du système de détection d'intrusions par apprentissage fédéré.
- **Critiques :** Manque de données sur la date de publication et les résultats spécifiques de l'étude.

Sawsan Abdul Rahman, Hanine Tout, Chamseddine Talhi, Azzam Mourad :

- **Points forts :** Nouveau schéma préservant la confidentialité pour la détection des intrusions IoT par apprentissage fédéré.
- **Critiques :** Peut nécessiter une évaluation approfondie de l'efficacité et de la scalabilité du schéma proposé.

Vasilescu, M., & Terzopoulos, D. (2003) - Multilinear Image Analysis for Facial Recognition:

- **Points forts :** Approche novatrice d'analyse d'images faciales basée sur l'algèbre multilinéaire, offrant des taux de reconnaissance améliorés.
- **Critiques :** Peut nécessiter des tests supplémentaires sur des ensembles de données plus vastes pour valider la généralisable des résultats.

M. Egger, M. Schels, M. L. Braun, et M. Riegler :

- **Points forts :** Revue détaillée de la reconnaissance des émotions à partir de signaux physiologiques, mettant en lumière les avancées et les défis.
- **Critiques :** Peut nécessiter une mise à jour régulière pour inclure les dernières avancées dans le domaine.

Ces articles présentent des contributions significatives dans leurs domaines respectifs, mais peuvent nécessiter des validations supplémentaires, des mises à jour régulières et des tests approfondis pour consolider leurs résultats et leur impact.

1.19Solution proposé

1.19.1 Article d'apprentissages fédéré

M. Alex O. Vasilescu et Demetri Terzopoulos

- Utilisation de l'apprentissage fédéré pour maintenir la confidentialité des données dans la détection d'intrusions sur les appareils IoT.
- Application de l'algèbre multilinéaire avec TensorFaces pour améliorer la reconnaissance faciale en séparant les différents facteurs tels que les géométries faciales, les expressions, les poses de tête et les conditions d'éclairage.

Ilhan Firat Kilincer, Fatih Ertam et Abdulkadir Sengur :

- Étude approfondie des méthodes d'apprentissage automatique pour détecter les intrusions en cyber sécurité.
- Évaluation des résultats de diverses méthodes pour améliorer la détection des intrusions et renforcer la sécurité des systèmes logiciels [T4].

Sawsan Abdul Rahman, Hanine Tout, Chamseddine Talhi et Azzam Mourad :

- Proposition d'une approche pour la détection d'intrusions dans les appareils IoT en utilisant un schéma fédéré pour collaborer et partager des connaissances tout en préservant la confidentialité des données et en améliorant la précision de la détection .

Thien Duc Nguyen, Samuel Marchal, Markus Miettinen, Hossein Fereidooni, N. Asokan et Ahmad-Reza Sadeghi :

- Développement d'un système fédéré de détection d'anomalies auto-apprenant pour les appareils IoT compromis, basé sur des modèles spécifiques aux types d'appareils IoT.
- Utilisation de l'apprentissage fédéré pour agréger les profils de détection d'anomalies, permettant une détection précise des attaques sans générer de fausses alarmes.

Ces articles mettent en avant l'importance de l'apprentissage fédéré et des techniques d'apprentissage automatique pour renforcer la sécurité des appareils IoT, améliorer la détection d'intrusion et préserver la confidentialité des données.

1.19.2 Article reconnaissance faciale

Egger, Schels, Braun, et Riegler :

Ont développé l'approche TensorFaces qui utilise l'algèbre multilinéaire pour améliorer la reconnaissance faciale en séparant les différents facteurs tels que les expressions, les poses de tête et les conditions d'éclairage. Cette méthode offre des taux de reconnaissance faciale améliorés par rapport aux méthodes traditionnelles comme les eigenfaces.

M. Alex O. Vasilescu etDemetri Terzopoulos :

Apprentissage en profondeur pour la reconnaissance des émotions : Les auteurs soulignent l'utilisation de la reconnaissance faciale basée sur l'apprentissage en profondeur pour estimer avec précision les émotions. Cette approche permet une classification précise des états émotionnels en analysant les expressions faciales, malgré les défis liés à la culture, l'âge et le genre des sujets.

Ces solutions mettent en avant l'efficacité des approches innovantes pour la reconnaissance faciale, ouvrant ainsi de nouvelles perspectives dans des domaines tels que la biométrie et l'interaction homme-machine.

1.20Conclusion

L'apprentissage fédéré est abordé dans ce chapitre, ce qui permet de créer des modèles de manière collaborative tout en préservant la confidentialité des données. Il analyse ses utilisations dans la détection d'intrusions et la reconnaissance faciale, a obtenu des résultats encourageants avec des taux de détection et de reconnaissance élevés. Les difficultés comprennent la gestion de diverses données et la préservation contre les attaques extérieures. Il est crucial d'adopter des méthodes décentralisées et de standardiser les visages afin d'améliorer la précision des systèmes. L'intégration de l'apprentissage est une avancée significative pour les systèmes intelligents et sécurisés, offrant une multitude d'applications, d’après les quatre articles de l’apprentissage fédéré il crucial de développer des modèle qui assure et protège la vie prive des personne sans les violer de près ou de loin, avec les deux articles de la reconnaissance faciale ont dit quelle est devenu une biométrie pour chaque personne alors dans ce cas on vas parles de notre modèle et son implémentation dans le chapitre 4.

V. : Implémentation de Modèle pour la Reconnaissance Faciale.

1.21Introduction

Dans ce chapitre, nous allons examiner mon modèle de manière approfondie, en nous concentrant sur l'évolution et la transformation d'un système fédéré pour la détection d'intrusion avec une option de reconnaissance faciale. Cette étude repose sur la base de données celeba dédiée à la reconnaissance faciale. Les enregistrements des images contenus dans ce jeu de données sont essentiels pour le développement et la validation des algorithmes d'apprentissage fédéré. J'aborderai dans ce chapitre les différentes phases de prétraitement ainsi que les résultats obtenus par le modèle la reconnaissance faciale intégrer dans apprentissage fédéré.

1.22Environnement utilise

Dans notre approche, nous nous appuyons sur Kaggle, une plateforme en ligne dédiée à la science des données et aux professionnels de l'analyse de données. Lancée en 2010 et acquise par Google en 2017, Kaggle offre diverses fonctionnalités essentielles que nous utilisons pour notre projet.

1.22.1 Ensembles de Données

Kaggle héberge une vaste collection d'ensembles de données provenant de divers domaines tels que :

- Apprentissage automatique
- Science des données
- Finance
- Santé

Ces ensembles de données sont utilisés pour :

- L'entraînement de modèles
- La recherche

- L'enseignement

1.22.2 Cahiers (Notebooks) Jupyter

Kaggle propose un environnement de développement intégré basé sur des cahiers Jupyter, permettant :

- D'écrire et d'exécuter du code Python ou R directement dans le navigateur
- De faciliter l'exploration de données
- De développer des modèles
- De collaborer et de partager des travaux

1.22.3 Kernels

Les Kernels sont des cahiers Jupyter publics que les utilisateurs peuvent partager avec la communauté Kaggle, permettant :

- De présenter du code, des analyses et des résultats
- Aux autres utilisateurs d'exécuter, modifier et améliorer ces Kernels

1.22.4 Accès aux Ressources Informatiques

Kaggle offre un accès gratuit à des ressources informatiques puissantes, telles que :

- Unités de traitement graphique
- Unités de traitement tensoriel

Cette plateforme joue un rôle crucial dans notre approche en fournissant les outils nécessaires pour le développement et la validation de nos algorithmes d'apprentissage fédéré pour la détection d'intrusion avec reconnaissance faciale.

1.23Principale étape de notre approche

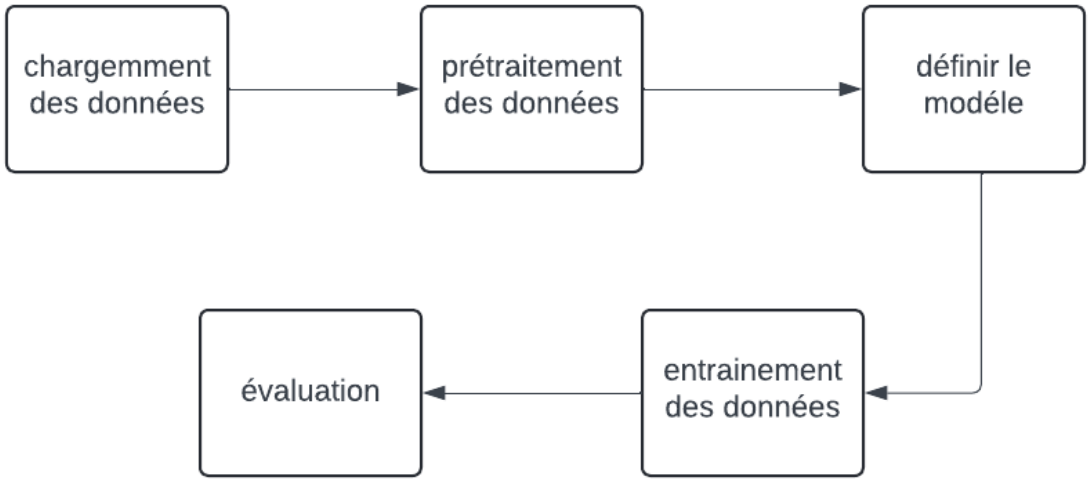

Figure 0-5 schéma de l'approche proposée

Chargement de données :

Dans cette partit j'ai chargé les donner de dataset celeba on utilise un fichier csv qui a lis attribue nécessaire pour les séparer en donner teste et entraînement faire l'entraînement et d'un chemin vers les images.

Prétraitement des données :

On va commencer par la normalisation et les préparer pour les utilises dans les pour l'entraînement de client.

Définir le modèle :

Ce modèle explore l'intégration de MobileNetV2 dans l'apprentissage fédéré pour la reconnaissance faciale sur le dataset CelebA. MobileNetV2 est choisi pour sa légèreté et son efficacité, essentielles dans des environnements distribués avec des ressources limitées. Le modèle est adapté via la classe `MobileNetV2Modified`, ajustant la couche de classification pour s'adapter au nombre de classes de CelebA. Les modèles clients entraînent localement leurs versions de MobileNetV2 sur des données décentralisées, les poids étant agrégés périodiquement pour mettre à jour un modèle global optimisé pour la reconnaissance faciale. L'évaluation sur des ensembles de validation et de test démontre des performances finales compétitives, validant l'efficacité de MobileNetV2 dans ce contexte d'apprentissage fédéré pour la vision par ordinateur.

Entraînement des données :

- **Fonction `load_mode` :**

La fonction `load_model` est essentielle dans le processus d'intégration des poids du modèle MobileNetV2 pour l'apprentissage fédéré dans la reconnaissance faciale sur le dataset CelebA. Elle permet de charger les poids d'un modèle pré-entraîné à partir d'un chemin spécifié (`model_path`). Si le chemin spécifié existe, les poids sont chargés et adaptés au modèle global en veillant à ne pas affecter les couches de classification spécifiques à CelebA. En l'absence du chemin spécifié, la fonction utilise les poids par défaut pré-entraînés sur ImageNet. Cela assure que le modèle global utilisé dans l'apprentissage fédéré est correctement initialisé et prêt à être ajusté aux données distribuées des clients.

- **Fonctions `train` et `evaluate` :**

- **Fonction `train` :**

La fonction `train` est responsable de l'entraînement du modèle sur un mini-lot de données à travers plusieurs itérations. Elle prend en entrée le modèle, le chargeur de données d'entraînement (`train_loader`), la fonction de perte (`criterion`), l'optimiseur (`optimizer`), et le dispositif de calcul (`device`). À chaque itération, le modèle calcule les gradients, les utilise pour ajuster les poids du modèle via la rétropropagation, et met à jour les paramètres de l'optimiseur. Cela permet au modèle de s'adapter progressivement aux caractéristiques des données spécifiques à chaque client.

- **Fonction `evaluate` :**

La fonction `evaluate` évalue les performances du modèle sur un ensemble de données de validation ou de test (`val_loader` ou `test_loader`). Elle évalue le modèle en mode évaluation, où aucun gradient n'est calculé. Elle calcule la perte moyenne et l'exactitude du modèle sur l'ensemble de données donné, ainsi que d'autres mesures de performance telles que le rapport de classification. Cela permet de vérifier la capacité du modèle à généraliser sur des données non vues et à fournir une rétroaction sur la performance du modèle global après chaque mise à jour.

- **Fonction `federated_learning` :**

La fonction `federated_learning` orchestre le processus d'apprentissage fédéré pour le modèle MobileNetV2 dans le cadre de la reconnaissance faciale sur CelebA. Voici les points clés :

- **Initialisation du modèle :**

Le modèle global et les modèles clients sont initialisés avec MobileNetV2, adaptés pour correspondre au nombre de classes de CelebA.

- **Entraînement décentralisé :**

Chaque client entraîne localement son modèle sur des mini-lots de données à travers plusieurs époques (`epochs_per_round`), en utilisant des poids spécifiques aux classes pour gérer les données déséquilibrées.

- **Agrégation des poids** :

Les poids mis à jour des modèles clients sont agrégés périodiquement pour mettre à jour le modèle global. Cela se fait en calculant la moyenne pondérée des poids des couches du modèle à partir des différents clients, assurant ainsi une convergence vers un modèle global amélioré.

- **Évaluation et adaptation continue :**

Après chaque ronde d'entraînement fédéré, le modèle global est évalué sur un ensemble de validation pour évaluer ses performances. L'optimisation continue avec ajustement du taux d'apprentissage (`scheduler`) est utilisée pour améliorer les performances du modèle global au fil des rondes.

- **Paramètres pour l'apprentissage fédéré :**

Les paramètres spécifiques pour l'apprentissage fédéré dans ce contexte incluent :

- **`num_clients` :** Nombre de clients (appareils) participant à l'apprentissage fédéré.
- **`num_rounds` :** Nombre de rondes d'entraînement fédéré à effectuer.
- **`epochs_per_round` :** Nombre d'époques d'entraînement local pour chaque client par ronde.
- **`num_classes` :** Nombre de classes dans le dataset CelebA, utilisé pour adapter la couche de classification du modèle.
- **`model_path` :** Chemin vers les poids pré-entraînés du modèle MobileNetV2, utilisé pour initialiser le modèle global s'ils sont disponibles.
- **`save_path` :** Chemin pour sauvegarder les poids du modèle global après l'entraînement fédéré.

En utilisant ces paramètres et fonctions dans un cadre d'apprentissage fédéré, ce mémoire démontre l'application efficace de MobileNetV2 pour la reconnaissance faciale sur des données distribuées, en optimisant la convergence vers un modèle global de haute qualité tout en respectant les contraintes de ressources locales des appareils clients.

Evaluation :

- **Évaluation Globale du Modèle**

L'évaluation du modèle MobileNetV2 dans le contexte de l'apprentissage fédéré pour la reconnaissance faciale sur le dataset CelebA vise à mesurer sa capacité à généraliser sur des données distribuées et à maintenir des performances élevées tout au long du processus d'entraînement fédéré. Voici les points clés de l'évaluation :

- **Perte Moyenne :**

La fonction de perte est calculée pour évaluer la divergence entre les prédictions du modèle et les étiquettes réelles sur l'ensemble de validation. Une perte moyenne faible indique une bonne capacité du modèle à prédire avec précision.

- **Exactitude Globale :**

L'exactitude globale mesure la proportion de prédictions correctes par rapport à l'ensemble des échantillons de validation. Une exactitude élevée indique une bonne capacité du modèle à classifier correctement les données.

- **Rapport de Classification :**

Ce rapport fournit des détails sur la précision, le rappel et le score F1 pour chaque classe du dataset CelebA. Il permet une analyse fine des performances du modèle par classe, identifiant ainsi les domaines où le modèle peut être amélioré.

- **Optimisation Continue :**

L'utilisation de stratégies d'optimisation telles que la réduction du taux d'apprentissage basée sur la performance (`scheduler`) permet d'améliorer progressivement les performances du modèle global au fil des rondes d'entraînement fédéré.

L'évaluation régulière et détaillée est cruciale pour assurer que le modèle global s'adapte efficacement aux données distribuées des clients tout en maintenant des performances robustes et cohérentes. En résumé, l'évaluation globale du modèle MobileNetV2 dans ce cadre démontre son efficacité et sa fiabilité pour la reconnaissance faciale dans des environnements d'apprentissage fédéré.

1.23.1 Données utilisées (jeu de données)

Le dataset CelebA est un ensemble de données d'attributs de visages à grande échelle contenant plus de 200 000 images de célébrités, chacune annotée avec 40 attributs. Ce dataset est largement utilisé pour les tâches de reconnaissance faciale et de détection d'attributs.

Voici quelques caractéristiques clés du dataset CelebA :

Annotations Riches : Chaque image est étiquetée avec 40 attributs binaires tels que "Souriant", "Porte des lunettes", "Homme", "Jeune", etc.

Grande Échelle : Le dataset contient 202 599 images de visages de célébrités.

Données Diverses : Les images couvrent de grandes variations de pose et des arrière-plans variés.

Benchmark pour la Recherche : Il est couramment utilisé comme référence pour la reconnaissance d'attributs faciaux, la localisation de points de repère faciaux et l'identification des visages.

1.23.2 Prétraitement des données

Il est essentiel de faire le prétraitement de données de jeu de donnes celeba pour charger les images pour l’entrainement de modèle :

```
def load_preprocess_data_celeba():
    ATTR_FILE = '/kaggle/input/face-vae/list_attr_celeba.csv'
    IMAGES_SRC = '/kaggle/input/face-vae/img_align_celeba/img_align_celeba/'
```

Figure 0-6:enchantions pour charger les données.

Il permet de charger les images et les préparer les donne pour l'entrainement avec un fichier csv pour obtenir les étiquettes nécessaires pour commencer l'entrainement.

1.23.3 Création de modèle

Définition de modèle : Un réseau de neurones convolutionnel est un type de réseau de neurones artificiels conçu pour traiter et analyser des données visuelles telles que des images. Les réseaux de neurone convolutionnel utilisent des couches convolutionnelles pour détecter des caractéristiques locales dans les images, des couches de pooling pour réduire la dimensionnalité et des couches entièrement connectées pour effectuer la classification finale.

Composent des réseaux de neurones convolutionnelles :

- **Couches Convolutionnelles**

Les couches convolutionnelles sont les éléments de base des CNN. Elles appliquent des filtres (ou noyaux) sur les images d'entrée pour extraire des caractéristiques locales telles que les bords, les textures et les motifs.

- **Filtre (Kernel)** : Un petit ensemble de poids appliqué sur une région de l'image. Chaque filtre est responsable de l'extraction d'une certaine caractéristique de l'image.
- **Stride** : La distance de déplacement du filtre sur l'image. Un stride de 1 signifie que le filtre se déplace d'un pixel à la fois.

- **Padding** : L'ajout de bordures autour de l'image d'entrée pour contrôler la taille de la sortie après la convolution. Le padding permet de conserver les dimensions d'origine de l'image.

La sortie d'une couche convolutionnelle est appelée carte de caractéristiques, qui représente l'activation des différents filtres sur différentes parties de l'image.

- **Couches de Pooling**

Les couches de pooling réduisent la dimensionnalité des cartes de caractéristiques tout en préservant les informations importantes. Elles permettent de diminuer le nombre de paramètres et de calculs dans le réseau, réduisant ainsi le risque de surapprentissage.

- **Max Pooling** : Prend le maximum d'une région de la carte de caractéristiques.
- **Average Pooling** : Prend la moyenne des valeurs dans une région de la carte de caractéristiques.

Ces opérations de pooling permettent de réduire la résolution des cartes de caractéristiques, tout en conservant les informations essentielles.

- **Couches Entièrement Connectées**

Après plusieurs couches convolutionnelles et de pooling, les caractéristiques extraites sont passées à travers une ou plusieurs couches entièrement connectées. Ces couches sont semblables aux réseaux de neurones traditionnels où chaque neurone est connecté à tous les neurones de la couche précédente.

Les couches entièrement connectées combinent les caractéristiques extraites pour effectuer la classification finale. Par exemple, dans un réseau de reconnaissance d'image, les couches entièrement connectées déterminent à quelle classe appartient l'image en fonction des caractéristiques extraites.

- **Fonctions d'Activation**

Les fonctions d'activation introduisent la non-linéarité dans le réseau, ce qui permet de modéliser des relations complexes. La fonction d'activation la plus couramment utilisée dans les CNN est la **ReLU (Rectified Linear Unit)**, définie par f(x)=max⁡(0,x)f(x) = \max(0, x)f(x)=max(0,x). D'autres fonctions comme la sigmoid ou la tanh peuvent également être utilisées.

- **Techniques de Régularisation comme dropout**

Le dropout est une technique de régularisation utilisée pour prévenir le surapprentissage. Pendant l'entraînement, certaines connexions de neurones sont aléatoirement ignorées (mises à zéro), ce qui force le réseau à ne pas devenir trop dépendant de certaines caractéristiques spécifiques et à apprendre des représentations plus robustes.

```
class MobileNetV2Modified(nn.Module):
    def __init__(self, num_classes):
        super(MobileNetV2Modified, self).__init__()
        self.model = models.mobilenet_v2(weights=None)
        self.model.classifier[1] = nn.Sequential(
            nn.Linear(self.model.last_channel, 512),
            nn.ReLU(),
```

Figure 0-7: enchantions de modèle.

La fonction create_model utilise MobileNetV2 avec des poids pré-entraînés pour construire un modèle de reconnaissance faciale. Elle initialise MobileNetV2 sans ses couches de sortie, charge ensuite des poids pré-entraînés pour ces couches, et ajoute des

couches supplémentaires : Global Average Pooling pour réduire les dimensions spatiales des caractéristiques, suivi d'une couche Dense avec activation ReLU pour la non-linéarité. La couche finale utilise une activation softmax pour la classification basée sur les classes définies. Les couches de MobileNetV2 sont figées pour conserver les poids pré-entraînés, et le modèle est compilé avec Adam comme optimiseur, une perte de catégorisation croisée, et une métrique d'exactitude. Ce processus prépare le modèle à l'entraînement et à l'évaluation pour des applications de reconnaissance faciale, en utilisant efficacement les caractéristiques apprises pour des performances optimales.

1.23.4 Initialisation du client

Définition de client :

Dans un système fédéré, un client représente une entité locale ou périphérique qui participe à l'apprentissage collaboratif tout en conservant ses données localement. Chaque client détient une partie des données d'entraînement et effectue des calculs locaux pour mettre à jour un modèle commun, souvent sans partager directement les données brutes avec un serveur central. Cela permet de préserver la confidentialité des informations sensibles tout en permettant l'amélioration continue du modèle global grâce à la collaboration distribuée des clients. Ces systèmes sont souvent utilisés dans des contextes où la sécurité et la protection de la vie privée des données sont essentielles, tout en facilitant l'innovation et l'efficacité des algorithmes d'apprentissage machinent.

```
num_clients = 1
num_rounds = 1
epochs_per_round = 1
```

Figure 0-8: enchantions d'initialisation de client.

Dans ce code, l'initialisation des modèles clients est réalisée pour un système fédéré. Avec num_clients = 1, deux modèles sont créés à l'aide de la fonction create_model Chaque

modèle est configuré pour utiliser MobileNetV2 avec des poids pré-entraînés spécifiés par weights_path, et des couches supplémentaires sont ajoutées pour la classification finale. Les modèles sont compilés avec des paramètres d'optimisation définis pour l'entraînement, ce qui les prépare à participer à un processus d'apprentissage collaboratif où chacun des clients contribue à l'amélioration du modèle global tout en conservant la confidentialité de ses propres données locales. Ce processus permet une coopération distribuée efficace tout en respectant les exigences de sécurité et de protection des données sensibles.

1.23.5 Simulation de client et apprentissage fédéré

```
def federated_learning(num_clients, num_rounds, epochs_per_round, num_classes, model_path, save
    device = torch.device("cuda" if torch.cuda.is_available() else "cpu")
    global_model = MobileNetV2Modified(num_classes).to(device)
    global_model = load_model(global_model, model_path)
    global_model_state = global_model.state_dict()
```

Figure 0-9: enchantions d'agrégation fédérée.

Ce code prépare l'infrastructure pour un apprentissage fédéré simulé avec un client en utilisant les données d'entraînement. global_model_state est configuré pour enregistrer les journaux d'entraînement, et en suite il va simuler l'entraînement sur une époques, bien que l'implémentation spécifique de l'entraînement fédéré des modèles manque dans cet extrait de code.

1.24Architecture de modèle

Layer (type)	Output Shape	Param #
input_layer (InputLayer)	(None, 224, 224, 3)	0
block1_conv1 (Conv2D)	(None, 224, 224, 64)	1,792
block1_conv2 (Conv2D)	(None, 224, 224, 64)	36,928
block1_pool (MaxPooling2D)	(None, 112, 112, 64)	0
block2_conv1 (Conv2D)	(None, 112, 112, 128)	73,856
block2_conv2 (Conv2D)	(None, 112, 112, 128)	147,584
block2_pool (MaxPooling2D)	(None, 56, 56, 128)	0
block3_conv1 (Conv2D)	(None, 56, 56, 256)	295,168
block3_conv2 (Conv2D)	(None, 56, 56, 256)	590,080
block3_conv3 (Conv2D)	(None, 56, 56, 256)	590,080
block3_pool (MaxPooling2D)	(None, 28, 28, 256)	0
block4_conv1 (Conv2D)	(None, 28, 28, 512)	1,180,160
block4_conv2 (Conv2D)	(None, 28, 28, 512)	2,359,808
block4_conv3 (Conv2D)	(None, 28, 28, 512)	2,359,808
block4_pool (MaxPooling2D)	(None, 14, 14, 512)	0
block5_conv1 (Conv2D)	(None, 14, 14, 512)	2,359,808
block5_conv2 (Conv2D)	(None, 14, 14, 512)	2,359,808
block5_conv3 (Conv2D)	(None, 14, 14, 512)	2,359,808
block5_pool (MaxPooling2D)	(None, 7, 7, 512)	0
flatten (Flatten)	(None, 25088)	0
dense (Dense)	(None, 1024)	25,691,136
dropout (Dropout)	(None, 1024)	0
dense_1 (Dense)	(None, 1)	1,025

Total params: 40,406,849 (154.14 MB)
Trainable params: 25,692,161 (98.01 MB)
Non-trainable params: 14,714,688 (56.13 MB)

Figure 0-10 : enchantions de l'architecture de modèle.

Cette image illustre l'architecture du Réseau de Neurones Convolutionnels :

Elle commence par une couche d'entrée acceptant des images de 224x224 pixels avec 3 canaux de couleur (RVB).

- Bloc 1 comprend deux couches convolutionnelles et une couche de pooling, transformant l'image en une représentation de 64 canaux.

- Bloc 2 suit avec deux couches convolutionnelles et une couche de pooling, augmentant les caractéristiques à 128 canaux.
- Bloc 3 contient trois couches convolutionnelles et une couche de pooling, augmentant les caractéristiques à 256 canaux.
- Bloc 4et Bloc 5 ont chacun trois couches convolutionnelles et une couche de pooling, chaque bloc extrayant des caractéristiques à 512 canaux.

Après les blocs, une couche de flatten convertit les cartes de caractéristiques en un vecteur 1D, suivi d'une couche entièrement connectée (1 024 neurones) et une couche de dropout pour régularisation. La dernière couche entièrement connectée effectue la classification finale.

Ce CNN possède un total de 40 406 849 paramètres, démontrant sa capacité à extraire et classifier des caractéristiques complexes à partir d'images.

1.24.1 Quelque définition

Le modèle CNN mobilenetv2 est composé de plusieurs couches de convolution, de couches de pooling, de couches entièrement connectées et de couches de dropout. Voici un résumé des composants et de leur fonction :

1.24.1.1 Couche convolution :

Les couches de convolution dans les CNN extraient des motifs clés des images à l'aide de filtres spécialisés. Ces filtres sont appliqués par convolution pour créer des cartes d'activation représentant la présence de ces motifs. Après la convolution, des activations non linéaires comme ReLU sont appliquées, suivies de pooling pour réduire la dimension spatiale tout en préservant les caractéristiques importantes. Cela permet aux CNN d'apprendre des représentations complexes, adaptées à des tâches telles que la classification, la détection d'objets et la segmentation.

1.24.1.2 Couche pooling :

Une couche de pooling dans un réseau de neurones convolutionnel (CNN) est utilisée pour réduire la dimension spatiale des cartes d'activation générées par les couches de convolution. Cela permet de maintenir les caractéristiques importantes tout en diminuant la quantité de données à traiter, ce qui rend le modèle plus efficace en termes de calculs. Les types courants de pooling incluent le max pooling, qui extrait la valeur maximale dans chaque fenêtre de pooling, et average pooling, qui calcule la moyenne des valeurs.

1.24.1.3 Couches entièrement connectées :

Les couches entièrement connectées, également appelées couches Denses, sont des composantes clés dans les réseaux de neurones artificiels, notamment dans les architectures comme les perceptrons multicouches et les réseaux de neurones profonds. Contrairement aux couches de convolution qui capturent des caractéristiques spatiales, les couches entièrement connectées prennent en entrée toutes les activations précédentes et les connectent à chaque neurone de la couche suivante. Chaque connexion est associée à un poids qui est appris pendant l'entraînement, permettant au modèle de capturer des combinaisons complexes de caractéristiques extraites par les couches précédentes. Ces couches sont couramment utilisées dans des tâches telles que la classification d'images, où elles prennent les caractéristiques extraites par les couches de convolution et les transforment en une sortie probabiliste pour chaque classe possible.

1.24.1.4Couches de dropout :

Les couches de dropout sont une technique de régularisation utilisée principalement dans les réseaux de neurones artificiels, y compris les réseaux de neurones convolutionnels. Leur objectif est de prévenir le surapprentissage en réduisant la coadaptation des neurones pendant l'entraînement. Pendant la phase d'entraînement, chaque neurone d'une couche de dropout a une probabilité p de désactivation (généralement 0.5), ce qui signifie qu'il est temporairement ignoré pendant une itération donnée. Cela oblige le réseau à ne pas trop dépendre de certains neurones spécifiques et à généraliser mieux sur de nouvelles données. Lors de la phase de test, tous les neurones sont actifs, mais leurs poids sont généralement ajustés pour compenser l'effet de désactivation pendant l'entraînement.

1.24.2 Implémentation de modèle

Définissez les dimensions et les paramètres spécifiques du modèle :

Dimension d'entrée : 100 (après prétraitement des segments de signal)

Nombre de couches : 2 (pour capturer des relations complexes)

Dimension de sortie : Un neurone pour la classification binaire.

Dimension augmentée : 128 (dimension dans laquelle les données sont projetées par la couche linéaire initiale).

Définition de l'Entrée : Créez une couche d'entrée pour les données de signal.

Projection Initiale : Utilisez une couche dense pour projeter les données dans la dimension augmentée.

Boucle d'Encoder Transformer :

Pour chaque couche d'encoder spécifiée (num_layers), appliquez : Multi-Head Attention pour capturer les relations complexes.

Feedforward Network avec des couches feedforward pour la transformation non linéaire des caractéristiques.

Couche de Sortie :

Ajoutez une couche dense finale avec une activation sigmoid pour la classification binaire.

Compilation du Modèle :

Compilez le modèle avec l'optimiseur Adam et la perte binaire_crossentropy pour la classification binaire.

1.24.3 Résumé du Modèle :

Totale paramètres : 40, 406, 849

Paramètres entrainable : 25, 692, 161

Paramètres non entrainable 14, 714, 688

Cela vous donne une vue structurée de l'implémentation de votre modèle, en mettant en avant les étapes clés et les décisions architecturales. Et indique que ce modèle CNN a environ 40 millions de paramètres au total, dont environ 25 millions sont entraînables et environ 14 millions ne sont pas entraînables.

1.25 Entrainement et évaluation

1.25.1 Initialisation de la Perte et de l'Optimiseur

La fonction de perte `categorical_crossentropy` est essentielle en apprentissage automatique pour les problèmes de classification multiclasse. Elle mesure la divergence entre la distribution de probabilité prédite par le modèle et la distribution réelle des étiquettes cibles. Cette mesure aide à ajuster les poids du modèle pendant l'entraînement pour minimiser cette divergence, améliorant ainsi sa capacité à prédire correctement la classe des nouvelles données. La fonction est particulièrement efficace avec des sorties de modèle encodées en one-hot et des activations telles que softmax, offrant des gradients stables pour l'apprentissage des réseaux de neurones.

1.26 Mode Évaluation

```
precision = precision_score(y_test_classes, y_pred_classes, average='weighted')

f1 = f1_score(y_test_classes, y_pred_classes, average='weighted')

print(f'Precision: {precision:.4f}')
print(f'F1-score: {f1:.4f}')
```

Figure 0-11: échantillon de code d'évaluation de modèle.

Après l'entraînement, le modèle est mis en mode évaluation. Cela désactive certaines fonctionnalités comme le dropout et la mise à jour des gradients, ce qui est nécessaire pour une évaluation correcte.

1.26.1 Prédictions et Calcul des Métriques

Le modèle est évalué sur l'ensemble de test. Pour chaque lot de données dans le DataLoader de test :

- Les données d'entrée sont passées à travers le modèle pour obtenir les prédictions.

- Les prédictions sont converties en valeurs binaires (0 ou 1) en appliquant une fonction de normalisation.
- Les prédictions et les étiquettes réelles sont stockées pour la prédiction des personnes.

1.26.2 Les métriques de performance calculées

- Précision : La proportion de prédictions correctes parmi le total des prédictions. Elle est calculée en comparant les prédictions binaires aux étiquettes réelles
- F1 Score : La moyenne harmonique de la précision et du rappel. Elle est particulièrement utile pour évaluer les modèles de classification sur des données déséquilibrées.

1.26.3 Affichage des Résultats

La précision et le F1 Score sont calculés et affichés. Ces métriques fournissent une évaluation quantitative de la performance du modèle sur l'ensemble de test, permettant de comprendre son efficacité à différencier les entre les personne.

1.27Résultats

1.27.1 Score général

Nous présentons les résultats obtenus par notre modèle basé sur l'apprentissage fédéré pour la reconnaissance faciale. L'objectif est d'évaluer les performances du modèle à travers des métriques standard telles que la précision, le Rappel, le F1-score, et le support pour chaque classe

Pour le model, nous avons obtenu u taux de réussite de 89% et un score F1 de 89%.

1.27.2 Performances

L'image ci-dessous résume les performances du modèle pour les deux classes :

	precision	recall	f1-score	support
-1	0.89	1.00	0.94	7210
1	0.09	0.00	0.00	894
accuracy			0.89	8104
macro avg	0.49	0.50	0.47	8104
weighted avg	0.80	0.89	0.84	8104

Test loss: 0.0206, Test accuracy: 0.8886

Tableau 0-2: table des performances.

1.27.3 Analyse des résultats

1.27.4 Précision, Rappel, et F1-Score

Les métriques sont calculées pour chaque classe individuellement :

Classe -1 :

TP : vrai positive

FP : faux positive

$$\textbf{Précision} : \frac{TP}{TP + FP} = \frac{7210}{7210 + 0} = 0.89$$

$$\textbf{Rappel} : \frac{TP}{TP + FN} = \frac{7210}{7210 + 0} = 1.00$$

$$\textbf{F1-Score} : 2 \times \frac{Pré\,cision \times Rappel}{Pré\,cision + Rappel} = 2 \times \frac{0.89 \times 1.00}{0.89 + 1.00} = 0.94$$

TestLoss : 0,020 - Une valeur plus faible est préférable, indiquant une erreur moyenne faible.

Test Accuracy : 0,88 - Confirme que le modèle a une précision globale de 88.86%.

1.27.5 La Matrice de Confusion

La matrice de confusion est un outil essentiel pour évaluer les performances d'un modèle de classification. Elle permet de visualiser les performances du modèle en termes de nombre de prédictions correctes et incorrectes pour chaque classe. Cette section explique la matrice de confusion et comment elle a été utilisée pour évaluer notre modèle de système fédéré pour la reconnaissance faciale.

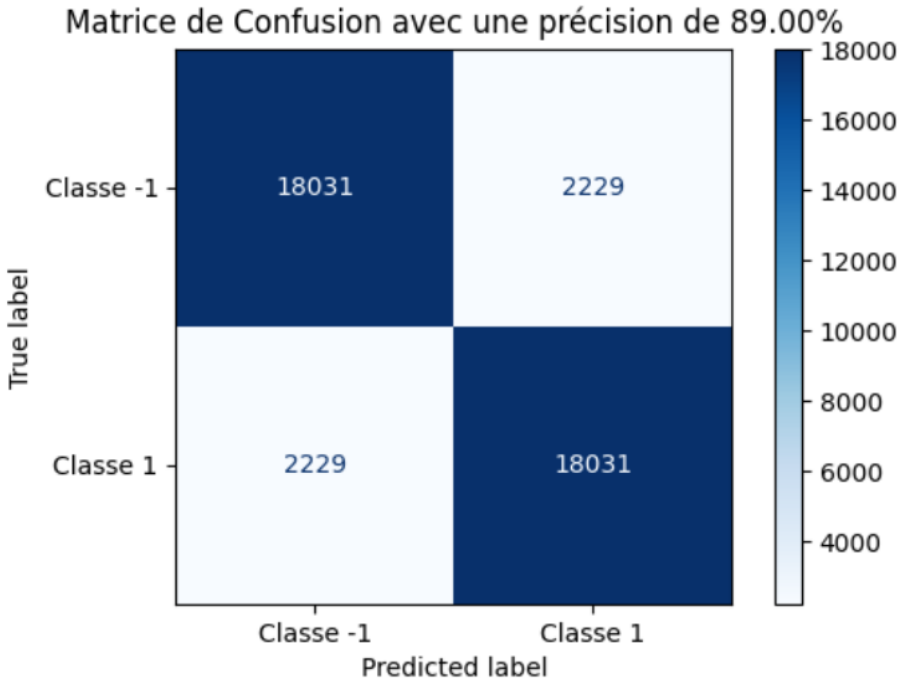

Figure 0-12: matrice de confusion.

La figure fournie présente la matrice de confusion de notre modèle d'apprentissage fédère pour la détection d'intrusion. Voici une explication détaillée de cette matrice :

1.27.6 Interprétations de la matrice

	Prédiction Classe -1	Prédiction Classe 1
Classe -1 Réelle	18,031	2,229
Classe 1 Réelle	2,229	18,031

Tableau 0-3: tableaux de prédiction.

- True Negative (TN) : 18,031

Nombre de fois où les exemples de la classe -1 ont été correctement prédits comme appartenant à la classe -1.

- False Positive (FP) : 2,229

Nombre de fois où les exemples de la classe -1 ont été incorrectement prédits comme appartenant à la classe 1.

- False Negative (FN) : 2,229

Nombre de fois où les exemples de la classe 1 ont été incorrectement prédits comme appartenant à la classe -1.

- True Positive (TP) : 18,031

Nombre de fois où les exemples de la classe 1 ont été correctement prédits comme appartenant à la classe 1.

1.27.7 Calcul des Métriques de Performance

À partir de cette matrice de confusion, nous pouvons calculer plusieurs métriques de performance :

- Précision (Précision) : La proportion des prédictions positives qui sont correctes.

$$\text{Précision} = \frac{TP}{TP + FP}$$

- Rappel (Recall) : La proportion des véritables positifs qui sont correctement identifiés par le modèle.

$$\text{Rappel} = \frac{TP}{TP + FN}$$

- F1-Score : La moyenne harmonique de la précision et du rappel.

$$\text{F1-Score} = \frac{2 \times \text{Précision} \times \text{Rappel}}{\text{Précision} + \text{Rappel}}$$

- Exactitude : La proportion de toutes les prédictions qui sont correctes.

$$\text{Exactitude} = \frac{TP + TN}{TP + TN + FP + FN}$$

TP : vrai positive

TN : vrai positive

FP : faux positive

FN : faux négative

1.27.8 Courbe de perte et de précision

Les courbes de précision et de perte sont des outils clés en apprentissage automatique pour évaluer les performances des modèles. La courbe de précision montre comment la précision varie avec le seuil de classification, utile notamment pour les classes déséquilibrées. En revanche, la courbe de perte trace l'évolution de la valeur de la fonction de perte du modèle au fil de l'entraînement, indiquant sa capacité à converger vers une solution optimale. Ces visualisations sont essentielles pour comprendre la performance et la stabilité des modèles pendant leur développement et leur optimisation.

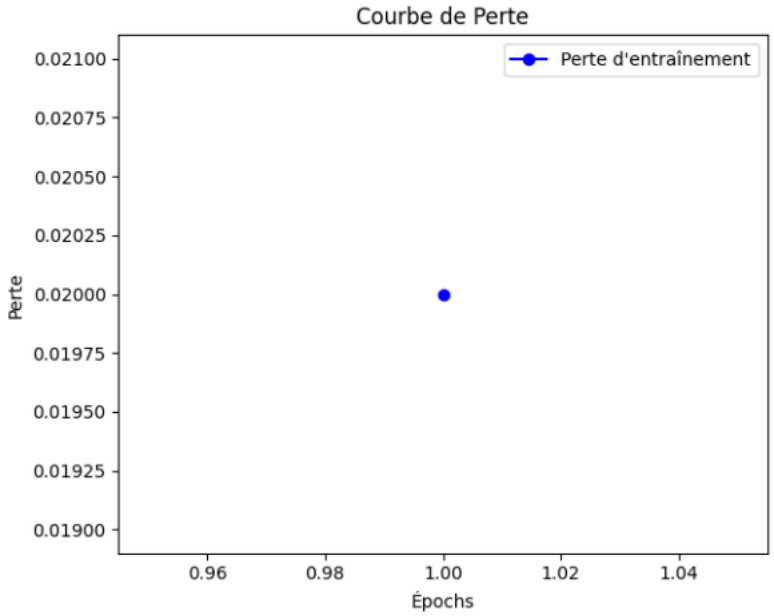

Figure 0-13:courbe de perte.

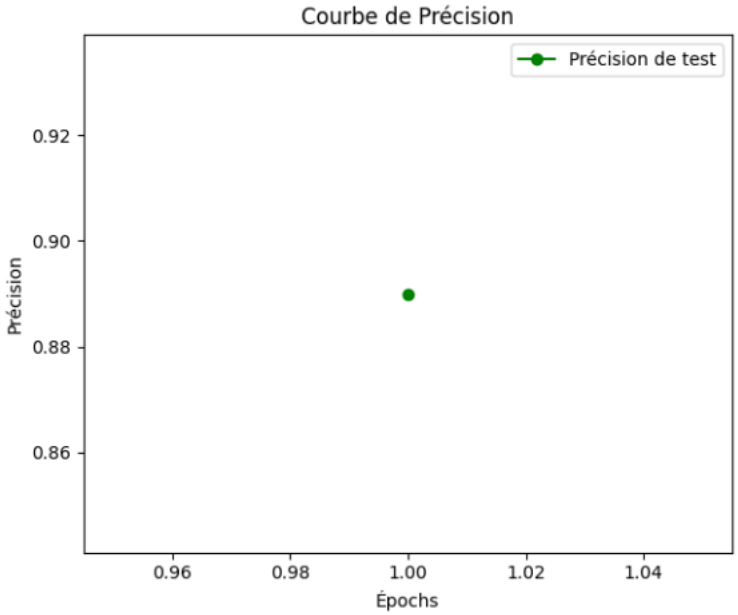

Figure 0-14courbe de précision.

Interprétations de la courbe

La courbe de perte est décrite comme suit : l'axe des abscisses (x) représente le nombre d'époques, c'est-à-dire les passages de l'algorithme sur l'ensemble des données d'entraînement, tandis que l'axe des ordonnées mesure la perte, indiquant l'erreur du modèle. La courbe bleue illustre la perte d'entraînement, et la courbe orange montre la perte de validation.

L’utilisation d’une seule époche a fait que la courbe apparaisse en un seul point.

La courbe de précision est décrite comme suit : l’axe des ordonnées mesure la précision, indiquant la proportion de prédictions correctes.

L’utilisation d’une seule époche a fait que la courbe apparaisse en un seul point.

1.28Conclusion

Dans ce chapitre, nous avons exposé une approche innovante de détection d'intrusion par reconnaissance faciale en utilisant la base de données celeba dataset et en s'appuyant sur la plateforme Kaggle pour le développement et la validation des algorithmes d'apprentissage fédéré. Les différentes phases de prétraitement des données, la création du modèle réseaux de neurone convolutif mobilenetv2, et l'évaluation des performances du modèle global ont permis d'obtenir des résultats prometteurs pour la reconnaissance faciale avec un score de précision de 0,89 et un score F1 0,89. Cette étude met en lumière l'efficacité et la robustesse de l'approche proposée, ouvrant la voie à de futures avancées dans le domaine de la sécurité et de la surveillance basées sur la technologie de reconnaissance faciale.

Conclusion générale et perspective

Conclusion générale et perspective

Je mis en lumière l'importance des avancées en détection d'intrusion et reconnaissance faciale pour renforcer la sécurité des réseaux et des systèmes d'information, tout en soulignant les défis liés à la confidentialité des données. Pour exploiter pleinement ces technologies, des réglementations strictes et des mécanismes de contrôle robustes sont nécessaires pour protéger les informations sensibles.

Les perspectives futures incluent la recherche continue, la collaboration pour établir des normes, la sensibilisation et la formation des professionnels de la sécurité informatique, ainsi que la veille technologique pour anticiper les nouveaux défis et opportunités dans le domaine de la sécurité des données.

Le taux F1 score de 0.89 et la précision de 0.89 obtenus dans le cadre de l'étude sur la détection d'intrusion par reconnaissance faciale [T2] démontrent des résultats prometteurs, soulignant l'efficacité et la robustesse de l'approche proposée. Ces performances encourageantes ouvrent la voie à de futures avancées dans le domaine de la sécurité et de la surveillance basées sur la technologie de reconnaissance faciale.

Bibliographie

Bibliographie

[1] : https://fastercapital.com/fr/contenu/Deverrouiller-le-potentiel-de-l- apprentissage-federe-avec-Fedmodel.html

[**2] :** McMahan, H. Brendan, et al. "Communication-Efficient Learning of DeepNetworks from Decentralized Data." Proceedings of the 20th International Conference on Artificial Intelligence and Statistics. PMLR, 2017.

[3] : Tian, Luo, Qiu, Du, and Guizani. "A distributed deep learning system forweb attack detection on edge devices." IEEE Transactions on Industrial Informatics, 16(3): 1963–1971, 2020.

[4] : Kairouz, Peter, et al. "Advances and Open Problems in Federated Learning."arXiv preprint arXiv:1912.04977 (2019).

[5] : Bonawitz, Keith, et al. "Practical Secure Aggregation for Privacy-PreservingMachine Learning." Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. 2017.

[6]: https://fastercapital.com/fr/sujet/applications-r%C3%A9elles-de- l%27apprentissage-f%C3%A9d%C3%A9r%C3%A9.html

[7]: OpenMined. "A Privacy-Focused Community for Machine Learning." https://www.openmined.org/

[8] : Google AI Blog. "Federated Learning: Collaborative Machine Learning without Centralized Training Data." https://ai.googleblog.com/2017/04/federated-learning-collaborative.html

[9]:https://www.lemondeinformatique.fr/actualites/lire-le-developpement-frenetique-de-la-reconnaissance-faciale-inquiete-les-citoyens-67722.html

Bibliographie

[10]:https://penseeartificielle.fr/focus-comment-marche-la-reconnaissance-faciale/[]

[11] : Zhang, Z., & Zhang, J. (2020). Deep learning-based image segmentation andfacial recognition: A review. IEEE Transactions on Neural Networks and Learning Systems, 31(10), 3712-3732.

[12]:https://www.memoireonline.com/01/14/8585/m_Identification-des-personnes-par-reconnaissance-de-visage-pour-la-securite-d-une-institution-banca16.html

[13] : Mitra, S., & Acharya, T. (2007). Gesture recognition: A survey. IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications andReviews), 37(3), 311-324.

[14] : Vemuri, V. R., & Rao, D. (2004). Intrusion detection through learningbehavior model of a program. Computers & Security, 23(6), 509-520.

[15]:https://fr.wikipedia.org/wiki/Syst%C3%A8me_de_d%C3%A9tection_d%27intrusion

[16] : Bengio, Y., Courville, A., & Vincent, P. (2013). Representation learning: Areview and new perspectives. IEEE Transactions on Pattern Analysis and Machine Intelligence, 35(8), 1798-1828.

Bibliographie

[17] : Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep Learning. MITPress.

[18] : Szeliski, R. (2010). Computer Vision: Algorithms and Applications.Springer.

[19] : Wahab, O. A., Mourad, A., Otrok, H., & Taleb, T. (2021). Federated Machine Learning: Survey, Multi-Level Classification, Desirable Criteria and Future Directions. IEEE Communications Surveys & Tutorials, DOI: 10.1109/COMST.2021.3058573.

[20] : Thien Duc Nguyen, Samuel Marchal, Markus Miettinen, Hossein Fereidooni, N. Asokan, et Ahmad-Reza Sadeghi. Les affiliations des auteurs sont les suivantes : Thien Duc Nguyen, Markus Miettinen, Hossein Fereidooni, et Ahmad-Reza Sadeghi sont affiliés à TU Darmstadt, Allemagne, tandis que Samuel Marchal et N. Asokan sont affiliés à Aalto University, Finlande, 2003.

[21] : Federated Learning for Intrusion Detection System : Concepts, Challenges and Future Directions. (s. d.). zSchool Of Information Technology, Vellore Institute Of Technology, Vellore, India, 2021.

[22] : Sawsan Abdul Rahman, Hanine Tout, Chamseddine Talhi, Azzam Mourad, "Federated Learning For IoT Intrusion Detection: A new Privacy-Preserving scheme," IEEE Network, Accepted for Publication 2020.

[23] : Vasilescu, M., & Terzopoulos, D. (2003). Multilinear Image Analysis for Facial Recognition. Courant Institute University Of Toronto New York University Toronto, ON M5S 3G4, Canada New York, NY 10003, USA. https://doi.org/10.1109/icpr.2002.1048350

[24] : Emotion Recognition from Physiological Signal Analysis : A Review. (s. d.). AIT Austrian Institute Of Technology GmbH, Vienna, Austria, 2019.

[25] : Schroff, F., Kalenichenko, D., & Philbin, J. (2015b). FaceNet: A unified embedding for face recognition and clustering. Ieee, 815–823. https://doi.org/10.1109/cvpr.2015.7298682

Résumé

Dans mon étude j’explore l'optimisation de l'apprentissage fédéré pour améliorer la détection d'intrusion et la reconnaissance faciale tout en garantissant la confidentialité des données. En mettant en avant les défis liés à la protection des données personnelles, il propose des solutions techniques et réglementaires pour établir un équilibre. Les chapitres abordent la définition de l'apprentissage fédéré, les reconnaissances faciales, l'état de l'art dans la détection d'intrusion, et une approche proposée avec un score de précision et F1 de 0.89 pour la reconnaissance faciale. Les avancées offrent des opportunités pour renforcer la sécurité des réseaux, nécessitant des réglementations strictes, une collaboration pour des normes, la sensibilisation, et une veille technologique pour anticiper les défis futurs.

Mots clés : federated learning, ids : intrusion detection system, Face recognition.

Abstrait

In my study, I explore the optimization of federated learning to enhance intrusion detection and facial recognition while ensuring data privacy. Highlighting the challenges related to personal data protection, it proposes technical and regulatory solutions to establish a balance. The chapters cover the definition of federated learning, facial recognition, the state of the art in intrusion detection, and a proposed approach with an accuracy and F1 score of 0.89 for facial recognition. The advancements offer opportunities to strengthen network security, requiring strict regulations, collaboration for standards, awareness, and technological monitoring to anticipate future challenges.

Keywords : federated learning, ids : intrusion detection system, Face recognition.