UNIVERSITÉ LARBI TÉBESSI, TÉBESSA

Faculté des Sciences Exactes et Sciences de la Nature et de la Vie

Département des Mathématiques et Informatique

Laboratoire des Mathématiques, Informatique et Systèmes (LAMIS)

THÈSE

En vue de l'obtention du diplôme de

Doctorat 3ème Cycle L.M.D

Discipline : Informatique

Spécialité : Réseaux de Systèmes Intelligents

Présentée et soutenue par

Abdelhakim ZEROUAL

Titre :

Une approche basée sur des techniques biométriques pour la sécurité dans l'environnement du Mobile Cloud Computing

Devant le jury ci-dessous :

M. Hakim Bendjenna	Prof.	Université Larbi Tébessi, Tebessa	Président
M. Mohamed Ridda Laour	Prof.	Université Larbi Tébessi, Tebessa	Examinateur
M. Chaker Mezioud	Prof.	Université Abdelhamid Mehri, Constantine	Examinateur
M. Ahmed Ahmim	MCA	Université Mohamed-Cherif Messaadia, Souk Ahras	Examinateur
M. Mohamed Amroune	Prof.	Université Larbi Tébessi, Tebessa	Encadreur
M. Makhlouf Derdour	Prof.	Université Larbi Ben M'Hidi, Oum El Bouaghi	Co-encadreur

Le 13/07/2022

ملخص

في الوقت الحاضر ، يستخدم المجتمع بشكل متزايد الأجهزة المحمولة الذكية ، ويتم تحديد استخدامها من خلال ملف تعريف المستخدمين في مجموعة متنوعة من القطاعات ، بما في ذلك الشبكات الاجتماعية ، والصحة الإلكترونية ، والألعاب ، والتجارة الإلكترونية ، والتعليم الإلكتروني ، وتخزين البيانات ، وما إلى ذلك. يحتاج المستخدمون إلى أجهزة محمولة قوية بشكل متزايد نتيجة لتطوير تطبيقات الهاتف المحمول ، حيث يحتاجون إلى موارد أكثر قوة.

يعد تطوير الأجهزة المحمولة لتلبية احتياجات المستخدم أمرًا مكلفًا ولا يستطيع الجميع تحمله. أدى ظهور تقنية الحوسبة السحابية المتنقلة (MCC) ، وهي مزيج من تقنيتين (الحوسبة المتنقلة والحوسبة السحابية) ، إلى حل العديد من المشكلات ، بما في ذلك تنفيذ الأعمال الشاقة من قبل المستخدمين الذين لديهم إمكانية الوصول إلى السحابة بدلاً من استخدام جهاز محمول . يتم تخزين البيانات في السحابة ، مما يلغي الحاجة إلى التخزين المحلي على الأجهزة المحمولة. على الرغم من مزاياها ، إلا أن الاستخدام المتزايد لهذه التكنولوجيا جلب معها مشكلات جديدة مثل تفريغ العمل والأمان وخصوصية بيانات المستخدم.

يركز بحثنا في هذه الرسالة على المصادقة في بيئة السحابة المتنقلة. لحماية دخول مستخدمي الأجهزة المحمولة إلى السحابة ، يوصى باستخدام طريقة مصادقة الوجه تعتمد على التعلم العميق في ظل البيانات المشفرة. أولاً ، الاقتراح هو معالجة صور الوجه باستخدام طريقة النمط الثلاثي المحلي (LTP) ، مما أدى إلى ارتفاع معدل التعرف. من ناحية أخرى ، فإن استخدام شعاع الميزات من نموذج تم تدريبه بالفعل من أجل المصادقة. يتم تشفير هذا الأخير باستخدام التشفير المتماثل جزئيًا (PHE) بدلاً من التشفير المتجانس بالكامل (FHE) الذي يتطلب الكثير من الموارد. التشفير المتماثل جزئيًا هو الخيار الأفضل لإجراء التشفير وفك التشفير باستخدام الجهاز المحمول. نظرًا لأن شعاع الميزات مشفر لا يمكن للسحابة رؤية محتوى شعاع الميزات أثناء مرحلة المطابقة في السحابة ، ولكن يمكنها إجراء عمليات حسابية. إنها خاصية لتماثل الشكل لحساب المسافة الإقليدية بين أشعة الميزات.

تم تقييم هذا العمل باستخدام خمس قواعد بيانات للوجه ، والنتائج المحققة ، سواء كان معدل التعرف أو وقت التنفيذ ، مرضية عند مقارنتها بالأعمال الموجودة.

الكلمات المفتاحية

الحوسبة السحابية، الحوسبة السحابية المتنقلة، القياسات الحيوية، التعلم العميق، مصادقة التعرف، التشفير متماثل الشكل.

Résumé

De nos jours, les gens utilisent de plus en plus des appareils mobiles puissants et intelligents, et leur utilisation est déterminée par le et le type des utilisateurs dans plusieurs secteurs, notamment les réseaux sociaux, la santé, les jeux vidéo, Le commerce électronique ou e-commerce, l'apprentissage en ligne, le stockage des données, etc… de ce fait, les utilisateurs ont besoin d'appareils mobiles de plus en plus puissants en raison du développement des applications mobiles, car ils nécessitent des ressources puissantes.

Le développement des appareils mobiles pour satisfaire les besoins des utilisateurs est couteux et n'est pas accessible à tout le monde. L'apparition de la technologie Mobile Cloud Computing qui est une combinaison de deux technologies (Mobile Computing et Cloud Computing) a résolu certains problèmes tels que l'exécution des tâches lourdes par les utilisateurs ayant accès au cloud plutôt que l'utilisation d'un appareil mobile. Le stockage de données se fait dans le cloud, éliminant ainsi le besoin de les stocker en local sur les appareils mobiles. Malgré ses avantages, l'utilisation accrue de cette technologie a entrainé d'autres défis tels que le déchargement des tâches, la sécurité et la confidentialité des données des utilisateurs.

Dans cette thèse, L'objectif de notre recherche porte sur l'authentification dans l'environnement du Mobile Cloud. Pour protéger l'accès des utilisateurs de mobiles ou qu'on nomme communément les « mobinautes » au cloud, une méthode d'authentification faciale basée sur le l'apprentissage profond sous des données chiffrées a été préconisée.

Dans un premier lieu, il est suggéré d'appliquer la méthode LTP pour traiter les images faciales, ce qui nous a menés à un taux de reconnaissance élevé, d'une part et d'autre part l'utilisation de vecteur de caractéristiques issu du modèle déjà formé pour l'authentification. Ce dernier est chiffré en utilisant le chiffrement partiellement homomorphe (PHE) au lieu de l'utilisation du chiffrement complètement homomorphe (FHE) qui nécessite des ressources puissantes, c'est le choix idéal pour que le processus de chiffrement et le déchiffrement soit exécuté au niveau du mobile en toute fluidité. Lors de la phase de correspondance dans le cloud entre le vecteur chiffré et le vecteur stocké dans le cloud, ce dernier ne peut pas avoir le contenu du vecteur de caractéristiques car il est chiffré, mais il peut faire des opérations arithmétiques c'est une propriété de l'homomorphisme pour calculer la distance euclidienne entre ses vecteurs pour la correspondance.

Ce travail est évalué à partir de cinq bases de données faciales, les résultats obtenus que ce soit le taux de reconnaissance ou le temps d'exécution sont satisfaisants comparativement aux autres travaux précédents.

Mots clés

Cloud computing, mobile cloud computing, biométrie, apprentissage profond, authentification, chiffrement homomorphe.

Abstract

Nowadays, society is increasingly using smart mobile devices, and their use is determined by the profile of users in a variety of sectors, including social networks, e-health, gaming, e-commerce, e-learning, data storage, and so on. Users require increasingly powerful mobile devices as a result of the development of mobile applications, as they require more powerful resources.

Developing mobile devices to satisfy user needs is costly and not everyone can afford it. The appearance of Mobile Cloud Computing (MCC) technology, which is a hybrid of two technologies (Mobile Computing and Cloud Computing), has solved several issues, including the execution of heavy work by users with access to the cloud rather than utilising a mobile device. Data is stored in the cloud, eliminating the need for local storage on mobile devices. Despite its advantages, the increased use of this technology has brought with it new issues such as work offloading, security, and user data privacy.

The focus of our research in this thesis is on authentication in the Mobile Cloud environment. To protect mobile users' access to the cloud, a facial authentication method based on deep learning under encrypted data was recommended. First, the suggestion is to process face images using the LTP approach, which led to a high recognition rate. The use of feature vectors from a model that has already been trained for authentication, on the other hand. The latter is encrypted using Partially Homomorphic Encryption (PHE) rather than Fully Homomorphic Encryption (FHE) which requires a lot of resources. PHE is the best option for the encryption and decryption procedure using mobile device. Because the feature vector is encrypted, the cloud cannot see the content of the feature vector during the matching phase in the cloud, but it can perform arithmetic operations. It is a property of the homomorphism to calculate the Euclidean distance between its vectors for correspondence.

This work is assessed using five facial databases, and the results achieved, whether the recognition rate or execution time, are satisfactory when compared to the previous work.

Keywords

Cloud computing, mobile cloud computing, biometrics, deep learning, authentication, homomorphic encryption.

Remerciements

Au début, je tiens à dire merci à mon directeur de thèse, le professeur Mohamed AMROUNE, qui m'a bien guidé et soutenu tout au long du travail de recherche, de l'état de l'art à la recherche des ***résultats****. Ses immenses connaissances, sa motivation et sa patience m'ont donné plus de puissance et d'esprit pour exceller dans la rédaction de recherche. Mener l'étude académique sur un sujet aussi difficile ne pouvait pas être aussi simple que comme il l'a fait pour moi. Il est mon mentor et un meilleur conseiller pour mes études de doctorat au-delà de l'imagination. Je tiens aussi à remercier mon Co-directeur de thèse, le Professeur Makhlouf DERDOUR, pour ses conseils, sa motivation, son support et ses commentaires ainsi que son soutien et ses encouragements.*

Un remerciement spécial au Professeur Issam MALKI pour son chaleureux accueil et son soutien durant mon stage au Royaume-Uni, son aide de rédaction de l'article.

J'ai également le plaisir de remercier le Professeur Mohamed Ridda LAOUAR et le Professeur Hakim BENDJENNA, qui ont facilité mon accès au Laboratoire de Recherche (LAMIS) de l'université de Tébessa et m'ont donné l'opportunité de faire partie de leur équipe. Il ne m'aurait pas été possible de mener cette recherche sans leur précieux soutien. Ils comptent tous vraiment beaucoup pour moi.

Je n'oublierai pas d'exprimer ma gratitude au Professeur Abdallah MERAOUMIA, pour son encouragement et ses suggestions judicieuses. Il a joué un rôle majeur dans le perfectionnement de mes compétences en rédaction de recherche. Ses conseils sans fin sont difficiles à oublier tout au long de ma vie.

Je tiens aussi à remercier MESRS (ministère de l'Enseignement Supérieur et de la Recherche Scientifique, Algérie) qui ont financé mon stage à l'étranger au Royaume-Uni pour la finalisation de ma thèse de Doctorat.

Un grand merci à mes amis, le docteur Atef BENTAHAR, docteur Ayoub YAHIAOUI et docteur Abderrazak KHEDIRI pour leurs support, motivation et leur aide et le fait qu'ils aient été toujours présents et disponibles.

En fin de compte, je suis reconnaissant à mes parents, frères et sœurs, amis et connaissances qui se sont souvenus de moi dans leurs prières pour le succès ultime. Je me considère comme rien sans eux. Ils m'ont donné suffisamment de soutien moral, d'encouragement et de motivation pour atteindre mes objectifs. Je tiens à remercier mes deux frères ANIS et AYMENE pour leurs accompagnements en route à l'université.

Mes deux lignes de vie (parents) m'ont toujours soutenu moralement et financièrement pour que je ne m'occupe que des études et de l'atteinte de mon objectif sans aucun obstacle sur le chemin.

Table de matière

ملخص *1*

RESUME *2*

ABSTRACT *4*

REMERCIEMENTS *5*

TABLE DE MATIERE *6*

LISTE DES FIGURES *8*

LISTE DES TABLEAUX *11*

INTRODUCTION GENERALE *12*

MOTIVATION 12
PROBLEMATIQUE 13
OBJECTIFS 13
METHODOLOGIE 13
ORGANISATION DE LA THESE 14

CHAPITRE 1 - MOBILE CLOUD COMPUTING *15*

1.1 INTRODUCTION 15
1.2 MOBILE COMPUTING 16
1.3 CLOUD COMPUTING 18
1.3.1 Les modèles de services de cloud computing 18
1.3.2 Les caractéristiques de cloud computing 19
1.4 MOBILE CLOUD COMPUTING 20
1.4.1 Les modèles de Mobile Cloud Computing 22
1.4.2 Les caractéristiques du Mobile Cloud Computing 24
1.4.3 Les Avantages du Mobile Cloud Computing 25
1.4.4 Les systèmes et applications de mobiles cloud computing 26
1.4.5 Les Problèmes de sécurité dans le Mobile Cloud Computing 27
1.5 CONCLUSION 39

CHAPITRE 2 - LES APPROCHES BASEES SUR LES MODALITES BIOMETRIQUES POUR L'AUTHENTIFICATION *40*

2.1 INTRODUCTION 40
2.2 LES SYSTEMES BIOMETRIQUES 40
2.2.1 Le système d'identification par empreinte digitale 41
2.2.2 Le système d'identification faciale 41
2.2.3 Le système d'identification de l'iris 42
2.2.4 Le système d'identification d'empreinte de paume 43

2.3 L'APPRENTISSAGE AUTOMATIQUE 44
2.3.1 Paradigmes et méthodes d'apprentissage automatique 46
2.4 LES RESEAUX DE NEURONES ARTIFICIELS (ANN) 53
2.4.1 Les réseaux de neurones feedforward 53
2.4.2 Backpropagation 55
2.4.3 Les réseaux de neurones convolutifs 56
2.4.4 Les composants essentiels d'un réseau de neurone 62
2.5 LES TECHNIQUES D'APPRENTISSAGE EN PROFONDEUR POUR LES SYSTEMES BIOMETRIQUES 67
2.6 CONCLUSION 68

CHAPITRE 3 - LES SYSTEMES BIOMETRIQUES ET L'APPRENTISSAGE AUTOMATIQUE 69

3.1 INTRODUCTION 69
3.2 LES TRAVAUX CONNEXES 69
3.3 LES CONTRIBUTIONS PROPOSEES 73
3.3.1 Modèle d'authentification profond dans le MCC 73
3.3.2 Utilisation de la méthode ajustement fin pour une authentification approfondie dans le Mobile Cloud Computing basée sur le système Tensorflow Lite 78
3.3.3 Modèle d'apprentissage profond légé pour améliorer l'authentification dans le Mobile Cloud Computing 80
3.4 CONCLUSION 92

CHAPITRE 4 - EXPERIMENTATION ET DISCUSSION 94

4.1 INTRODUCTION 94
4.2 MATERIELS ET LOGICIELS UTILISES 94
4.3 LES BASE DE DONNEES 94
4.4 LES RESULTATS OBTENUS 97
4.4.1 L'évaluation de la solution 1 97
4.4.2 L'évaluation de la solution 2 98
4.4.3 L'évaluation de la solution 3 101
4.5 DISCUSSION 105
4.6 CONCLUSION 107

CONCLUSION GENERALE ET PERSPECTIVES 108

PERSPECTIVES 109

PRODUCTION SCIENTIFIQUE 110

ACTIVITES SCIENTIFIQUES 111

BIBLIOGRAPHIE 112

LISTE DES ABREVIATIONS 127

Liste des figures

Figure 1.1 L'origine de MCC (De, 2016). 16

Figure 1.2 Les différents niveaux du service et les services offerts par le cloud (De, 2016). 18

Figure 1.3 L'architecture générale de MCC (Donald and Arockiam, 2014). 21

Figure 1.4 Modèle de Cloudlet (Ali, 2020). 24

Figure 1.5 Les principales caractéristiques du Mobile Cloud Computing (Yu and Leung, 2015). 24

Figure 1.6 L'architecture de WallDroid (Kilinc et al., 2012). 30

Figure 1.7 Exemple simple de processus d'authentification. 30

Figure 1.8 L'architecture d'authentification (Chow et al., 2010). 31

Figure 1.9 Le flux de données de SeDiCi 2.0 pour l'authentification (De, 2016). 32

Figure 1.10 Le schéma d'authentification biométrique basé sur le cryptage (Zhao et al., 2013). 33

Figure 1.11 L'architecture de stockage sécurisé des données dans le cloud (De, 2016). 35

Figure 2.1 Les différents termes couramment utilisés dans l'IA (Roche, 2020). 45

Figure 2.2 Les types d'apprentissage automatique (Roche, 2020). 47

Figure 2.3 Le processus de ML actif en ligne. (Roche, 2020). 50

Figure 2.4 Réseau de neurones feedforward (Ojha et al., 2017). 54

Figure 2.5 (a) La couche bleu de l'image en couleurs vraies du chiffre quatre. (b) Aplatissement de la couche dans un seul tableau alignant une colonne après l'autre (Roche, 2020). 57

Figure 2.6 (a) Les données originales de l'image du chiffre quatre. (b) Les dimensions horizontales réduites des données d'image (Roche, 2020). 58

Figure 2.7 (a) & (b) Affichent les données d'image après le traitement par le facteur de sous-échantillonnage (Roche, 2020). 59

Figure 2.8 (a) L'image originale du chiffre quatre. (b) L'image avec le facteur de sous-échantillonnage horizontale et verticale (Roche, 2020). 60

Figure 2.9 L'architecture général du Réseau de Neurones Convolutifs (Roche, 2020). 61

Figure 2.10 Le processus de Max-pooling (Roche, 2020). 61

Figure 2.11 Binary Step. 63

Figure 2.12 Bipolar. 63

Figure 2.13 Sigmoid. 63

Figure 2.14 ReLu. 63

Figure 2.15 Les fonctions de perte de régression, perte de classification binaire, perte de classification multi-classes et leurs sous-divisions. 66

Figure 3.1 Contributions proposées. 73

Figure 3.2 Architecture proposée pour cette approche. 75

Figure 3.3 L'architecture de DeepCNN proposé (Zeroual et al., 2018). 76

Figure 3.4 L'organigramme de Tensorflow Lite (Zeroual et al., 2019). 78

Figure 3.5 L'encodage LTP pour un bloc de 3x3 (Zeroual et al., 2021). 81

Figure 3.6 L'architecture de l'approche proposée. 84

Figure 3.7 Le système d'authentification proposé. 84

Figure 3.8 L'architecture de réseau de neurones convolutifs proposée (Zeroual et al., 2021). 85

Figure 3.9 L'extraction de caractéristiques (Zeroual et al., 2021). 88

Figure 3.10 Le diagramme séquentiel de la phase d'enregistrement. 90

Figure 3.11 Le diagramme séquentiel de la phase d'authentification. 91

Figure 4.1 Echantillons de la base de données ORL (Zeroual et al., 2021). 95

Figure 4.2 Echantillons de la base de données Yale (Zeroual et al., 2021). 95

Figure 4.3 Echantillons de la base de données Extended Yale (Zeroual et al., 2021). 96

Figure 4.4 Echantillons de la base de données Georgia Tech (Zeroual et al., 2021). 96

Figure 4.5 Echantillons de la base de données FEI (Zeroual et al., 2021). 96

Figure 4.6 (a) La métrique précision du DeepCNN. (b) Loss du DeepCNN (Zeroual et al., 2018). 97

Figure 4.7 Les performances de la classification (Zeroual et al., 2018). 98

Figure 4.8 (a) La précision de VggNet avec une seule couche non gelée. (b) Loss de VggNet avec une seule couche non gelée (Zeroual et al., 2019). 99

Figure 4.9 (a) La précision de VggNet avec deux couches non gelées. (b) Loss de VggNet avec deux couches non gelées (Zeroual et al., 2019). 100

Figure 4.10 (a) La précision de VggNet avec trois couches non gelées. (b) Loss de VggNet avec trois couches non gelées (Zeroual et al., 2019). 100

Figure 4.11 (a) La précision de VggNet avec quatre couches non gelées. (b) Loss de VggNet avec quatre couches non gelées (Zeroual et al., 2019). 101

Figure 4.12 Précision, loss, précision de validation et loss de validation à l'aide de LTP-DeepCNN : (a) base de données ORL, (b) base de données Yale, (c) base de données Yale étendue, (d) base de données Georgie Tech, (e) base de données FEI (Zeroual et al., 2021). 103

Liste des tableaux

Tableau 1.1 La comparaison de différents systèmes de sécurité des données _____38

Tableau 3.1 L'analyse des avantages et des inconvénients des travaux existants. _____72

Tableau 4.1 La relation entre couches, précision et temps d'exécution. _____101

Tableau 4.2 Les metriques pour différents ensembles de données utilisant DeepCNN et LTP-DeepCNN._____102

Tableau 4.3 Coûts techniques (Temps et Mémoire). _____104

Tableau 4.4 Le taux de reconnaissance sous des données chiffrées. _____104

Tableau 4.5 La comparaison entre nos travaux. _____105

Tableau 4.6 Les précisions de la classification sur différentes bases de données avec CLTP, CLBP et LTP-DeepCNN. _____106

Tableau 4.7 La comparaison entre l'approche proposée et les travaux connexes. _____106

Introduction générale

Mobile Cloud Computing (MCC) est une solution architecturale qui intègre la puissance de calcul des appareils mobiles tels que les smartphones et les tablettes avec des ressources basées sur le cloud. Les appareils mobiles de MCC peuvent compléter les ressources de plusieurs comptes basés sur le cloud à distance plutôt que localement en raison des augmentations de calcul. La combinaison se traduit par un nouveau type d'expérience informatique mobile qui est fluide sur n'importe quel appareil ou lors du passage d'un appareil à l'autre.

Aujourd'hui, dans la vie quotidienne, la plupart des gens utilise leurs appareils mobiles pour certains besoins tels que les réseaux sociaux, la santé, les jeux, le stockage dans le cloud, ou pour consulter les courriels, exécuter des taches lourdes, etc...

Motivation

La sécurité dans le MCC devient une tâche importante et complexe, cela est due à l'augmentation des utilisateurs qui utilisent les appareils mobiles. Une partie de la société évite d'utiliser la technologie MCC du fait de leurs craintes concernant leurs données. Cette crainte a motivé les chercheurs de travailler dans cet axe pour satisfaire les besoins des utilisateurs. Il y a de nombreux travaux qui ont été déjà réalisés, spécialement l'authentification des utilisateurs que ce soit avec les méthodes classiques ou biométriques.

Les solutions biométriques s'avèrent les mieux adaptées car la plupart des appareils mobiles sont des appareils intelligents qui contiennent des appareils photos, des capteurs d'empreintes digitale, des capteurs gyroscopes, etc… parmi les avantages de la solution biométrique, l'identité biométrique ne peut pas être oubliée, elle est facile à gérer et difficile à pirater. Mais il faut que le système proposé soit robuste en termes de reconnaissance et de temps d'exécution et doit d'autre part préserver les données des utilisateurs.

Cela nous a motivés de proposer une approche d'authentification basée sur l'apprentissage profond en utilisant la reconnaissance faciale sous des données chiffrées en utilisant le chiffrement partiellement homomorphe qui peut être exécuté dans les appareils mobiles parce que les ressources de ces appareils sont limitées.

Problématique

Les ressources de dispositifs mobiles ne se sont pas développées de manière à gérer efficacement le stockage local, le transfert et le traitement de données massives. A cet effet, l'utilisation du cloud pour résoudre ce genre de problème a créé un nouvel élan de recherche connu sous le nom du Mobile Cloud Computing (MCC). Cependant, cette utilisation dépend grandement de la sécurité et de la protection des données personnelles et privées, car les utilisateurs deviennent de plus actifs sur le net.

A cet effet, assurer la sécurité dans l'environnement du MCC est obligatoire et se considère comme une tâche difficile. La biométrie se présente comme une alternative qui peut être très efficace pour prendre en charge la sécurité dans l'environnement du MCC.

La solution biométrique pour l'authentification a besoin de ressources puissantes spécialement si le travail est basé sur l'apprentissage profond. Comme les ressources des appareils mobiles sont restreintes, on va devoir chercher une solution efficace, légère et robuste pour sécuriser le système d'authentification tout en préservant les données confidentielles des utilisateurs.

Objectifs

L'objectif de cette thèse est de concevoir un système efficace et robuste pour l'authentification dans l'environnent du MCC en tenant compte les ressources limitées des appareils mobiles ce qui rend la tâche plus complexe car comme on le sait, le chiffrement et le déchiffrement en plus de la reconnaissance à base de l'apprentissage profond prend beaucoup du temps et de ressources.

Ce système doit être basé sur l'apprentissage profond afin que la reconnaissance faciale soit précise en tenant compte de la préservation des données confidentielles transmises lors de la phase d'authentification.

Méthodologie

Afin de résoudre les problèmes d'authentification dans l'environnement du MCC et après une étude profonde sur les lacunes ou insuffisances des travaux antérieurs.

Nous proposons :

Au niveau cloud :

- L'entrainement du modèle à base de réseaux de neurones convolutifs,
- Le modèle généré est converti en un modèle compatible pour les utilisateurs mobiles à des fins d'extraction des caractéristiques de l'utilisateur.

Au niveau mobile :

- Utiliser le modèle converti pour extraire le vecteur de caractéristique qui caractérise l'image du visage de l'utilisateur,
- Chiffrement du vecteur de caractéristique avec le chiffrement partiellement homomorphe pour la comparaison et l'authentification.

Organisation de la thèse

Après une introduction qui décrit l'environnement du Mobile Cloud Computing, les défis de sécurité qui nous a motivés à soulever une problématique afin de cerner les objectifs à atteindre ainsi qu'une méthodologie qui explique brièvement la solution proposée.

Cette thèse est composée de quatre chapitres qui sont :

Chapitre 1 : dans ce chapitre on parlera de l'environnement du Mobile Cloud Computing ainsi que les défis de sécurité dans cet environnement avec quelques travaux connexes.

Chapitre 2 : ce chapitre traitera les modalités biométriques et leurs approches et leur utilisation dans l'authentification.

Chapitre 3 : les travaux réalisés dans le contexte d'utilisation ou l'intégration de la biométrie spécialement l'apprentissage profond dans l'environnement du Mobile Cloud Computing pour l'authentification, ainsi que notre solution proposée.

Chapitre 4 : ce chapitre sera consacré à l'expérimentation et l'analyse des résultats obtenus suivies par une étude comparative pour la validation du travail réalisé.

Cette thèse est achevée par une conclusion générale et des perspectives présentant une synthèse des travaux proposés avec des entrevoir aux futurs.

Chapitre 1 - Mobile Cloud Computing

1.1 Introduction

Le Mobile Cloud (MC) est devenu un nouveau sujet de recherche ces dernières années en raison des progrès rapides des réseaux et de la technologie mobile. Dans le passé, les ordinateurs étaient utilisés pour le calcul. Des sondages menés récemment montrent que la majorité du public est plus disposée et capable d'utiliser des appareils mobiles tels que des téléphones portables et des tablettes, ainsi que des assistants numériques personnels (PDA), que des ordinateurs de bureau.

La base actuelle d'utilisateurs de smartphones a, selon des données récentes, déjà dépassé le niveau du milliard. L'informatique à l'aide d'appareils mobiles est ainsi apparue comme un concept plus réalisable que l'approche traditionnelle. Certains inconvénients, notamment un manque de stockage, un manque de puissance de calcul et une durée de vie de la batterie limitée dans les appareils mobiles, continuent d'être des obstacles pour la technologie MC.

Le Cloud Computing (CC) peut être une méthode efficace pour surmonter ces obstacles. Le CC est un terme qui fait référence à la combinaison de la virtualisation des ressources et d'un paradigme informatique distribué qui intègre le logiciel en tant que service (SaaS), la plate-forme en tant que service (PaaS) et l'infrastructure en tant que service (IaaS). De nombreux services cloud, tels que Microsoft Azure et Amazon EC2, offrent un stockage et un traitement élastiques et transparents sur une base « à la demande » ou « pay-per-use ». Ainsi, l'union de MC et du CC a abouti à la création d'une nouvelle approche technologique améliorée connue sous le nom de Mobile Cloud Computing (MCC), comme le montre la Figure 1.1. MCC est, en un mot, le CC avec l'ajout d'appareils mobiles en tant que clients légers. Ici, les données des appareils mobiles seront déchargées vers le cloud pour le calcul ou le stockage.

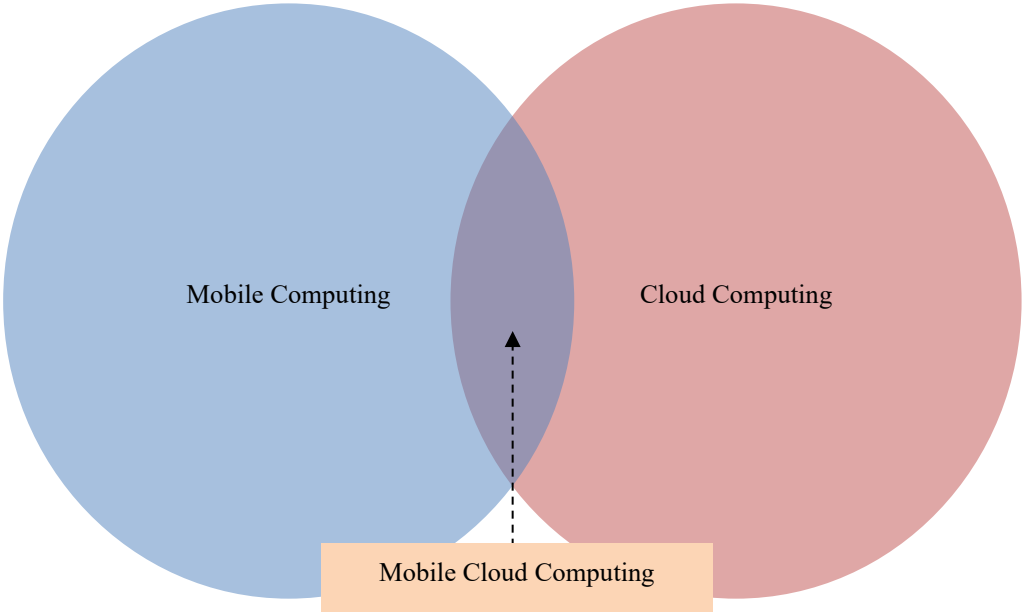

Figure 1.1 L'origine de MCC (De, 2016).

Dans ce chapitre, nous parlerons du cloud computing et de ses caractéristiques, on verra ensuite la technologie Mobile Cloud Computing, ses modèles, les domaines d'application. Enfin, nous discuterons sur les problèmes de sécurité dans le Mobile Cloud Computing.

1.2 Mobile Computing

La mobilité est devenue un terme très courant et joue un rôle de plus en plus important dans l'environnement informatique d'aujourd'hui. Le développement d'appareils mobiles tels que les smartphones, les PDA, les appareils de navigation GPS et les ordinateurs portables, qui sont tous équipés d'une gamme de technologies MC, de mise en réseau et de sécurité, a connu une augmentation fulgurante ces dernières années. De plus, avec les progrès des technologies sans fil telles que WiMax, Ad Hoc Network et WIFI, les utilisateurs peuvent surfer sur Internet beaucoup plus facilement et sans être liés par des câbles comme ils l'étaient dans le passé. En conséquence, ces appareils mobiles deviennent de plus en plus populaires parmi les personnes qui les utilisent, il y a à la fois ceux qui le font pour le travail et d'autres pour le plaisir dans leur vie quotidienne, et cette tendance devrait se poursuivre. Dans le contexte de l'interaction homme-machine, il est défini comme un mode de transport dans lequel un ordinateur est censé être déplacé au cours d'une opération typique.

MC repose sur trois principes fondamentaux : le matériel, les logiciels et la communication. Ces sujets sont discutés en détail ci-dessous. Les appareils mobiles, tels que les smartphones et les ordinateurs portables, ainsi que leurs composants mobiles, peuvent être considérés comme des exemples d'idées matériel (Sahib et al., 2014). Le logiciel informatique mobile comprend les divers programmes mobiles installés sur les appareils, tels que le navigateur mobile, le logiciel antivirus et les jeux, entre autres. L'architecture des réseaux mobiles, les protocoles et le transport des données dans leur utilisation font tous partie de la problématique de la communication. Ils doivent être totalement transparents pour l'utilisateur final. Le Mobile Computing se différencier par les cinq caractéristiques essentielles suivante :

- La déconnexion et la cohérence se produisent fréquemment en raison de facteurs tels que les limitations de puissance de la batterie, les niveaux de charge de la batterie de communication sans fil, les conditions du réseau, etc. En conséquence, les nœuds mobiles ne maintiendront pas toujours une connexion, mais se déconnecteront fréquemment et resteront cohérents avec le réseau sans fil, passivement ou activement.
- Un système de réseau informatique mobile avec une faible fiabilité en raison de signaux sensibles aux interférences et à l'espionnage doit être examiné à partir des terminaux, des réseaux, des plates-formes de base de données, ainsi que du développement d'applications afin de résoudre correctement le problème de sécurité dans les réseaux informatiques mobiles.
- Les nœuds mobiles dans un réseau informatique mobile peuvent établir des connexions avec d'autres nœuds, y compris des nœuds fixes dans un réseau câblé, grâce à l'utilisation d'une station d'assistance mobile pendant qu'ils se déplacent.
- Les conditions du réseau sont de natures diverses. La plupart du temps, les réseaux auxquels les nœuds mobiles se connectent ne sont pas uniques ; par exemple, un réseau filaire à bande passante élevée, un réseau étendu sans fil à faible capacité ou même un réseau déconnecté peuvent tous être utilisés.
- Connectivité réseau qui n'est pas symétrique Les serveurs, points d'accès et autres stations d'assistance mobile ont une capacité d'envoi/réception robuste, cependant une telle capacité dans les nœuds mobiles est un peu limitée. En conséquence, il existe une disparité dans la bande passante de transmission et le sur-débit entre la liaison descendante et la liaison montante.

1.3 Cloud Computing

Au fil des ans, les chercheurs ont discuté de la notion de CC et de nombreux chercheurs ont défini une gamme de concepts de CC (Gai et al., 2018, 2016; Gai and Li, 2012; Qiu et al., 2015). Beaucoup d'entre eux considéraient le CC comme une nouvelle notion plutôt qu'une nouvelle technologie. Sur la base d'études antérieures, il est encore difficile de construire une idée générale reconnue en raison de sa vaste gamme d'applications et de technologies informatiques et de ressources essentielles.

Le mot "Cloud" est une métaphore pour les serveurs qui fournissent des services Internet pouvant être hébergés ou gérés par n'importe quel tiers (Gai and Li, 2012). Le serveur cloud est au cœur du CC, et il peut actuellement prendre en charge la majorité des ressources de calcul en tant que services. Le CC, par opposition aux serveurs loués traditionnels, permet des solutions plus flexibles qui dépendent des demandes des utilisateurs et des ressources de calcul utilisées (Dai et al., 2013; Gai et al., 2020). Les fournisseurs de services cloud gèrent les serveurs basés sur le cloud et résolvent les problèmes technologiques.

1.3.1 Les modèles de services de cloud computing

La Figure 1.2 illustre les différents niveaux du service et les services offerts par le cloud.

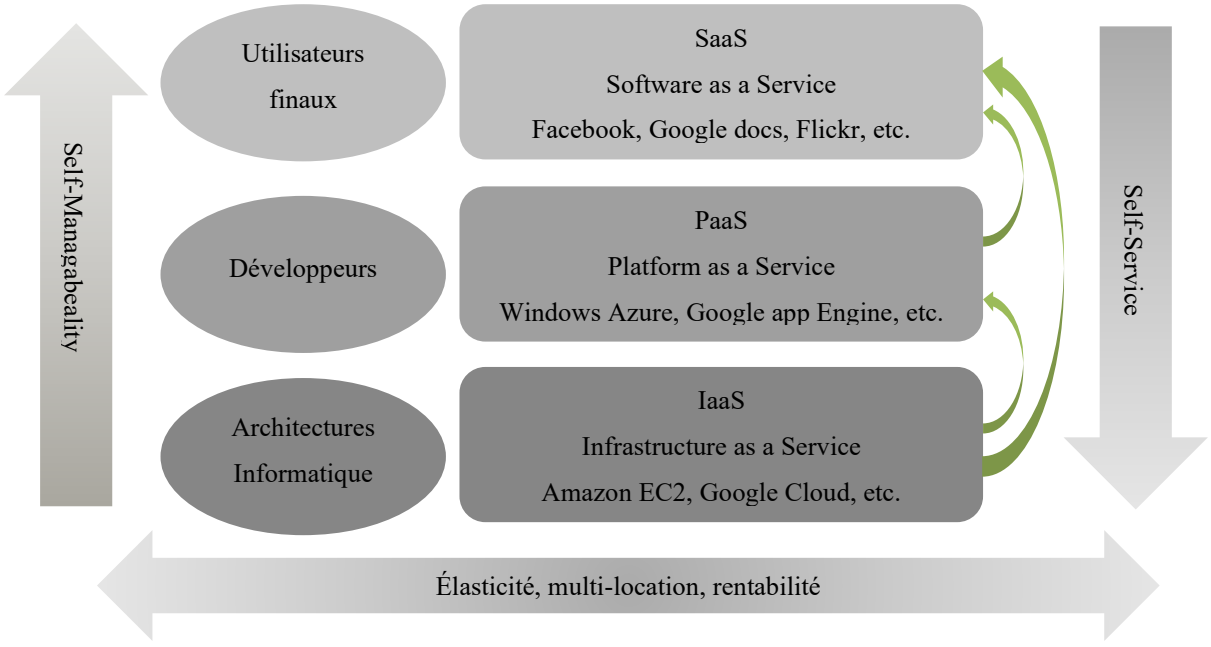

Figure 1.2 Les différents niveaux du service et les services offerts par le cloud (De, 2016).

a) Software as a Service (SaaS)

Le logiciel en tant que service (SaaS) est un paradigme orienté service à long terme. Le SaaS est utilisé pour fournir aux clients des services orientés applications et les processus qui sont déployés dans le cloud et hébergés dans une perspective d'infrastructure du cloud. SaaS offre des services spécifiques à un domaine aux clients enregistrés pour accéder aux applications dans le cloud en tant que service via Internet. Cependant, les consommateurs peuvent utiliser ces services sur une base de paiement à l'utilisation (Amin et al., 2013).

b) Platform as a Service (PaaS)

La capacité fournie au consommateur est la possibilité de déployer des applications créées ou acquises par le consommateur écrites à l'aide de langages de programmation, de bibliothèques, de services et d'outils pris en charge par le fournisseur dans l'infrastructure cloud. Le consommateur ne gère ni ne contrôle l'infrastructure cloud sous-jacente, qui comprend le réseau, les serveurs, les systèmes d'exploitation et le stockage, mais il contrôle les applications déployées et peut-être les paramètres de configuration de l'environnement d'hébergement des applications.

c) Infrastructure as a Service (IaaS)

L'infrastructure en tant que service (IaaS) fournit aux consommateurs une prise en charge de l'infrastructure (tels que le calcul, le stockage, le système d'exploitation et la mise en réseau) en tant que service. Le concept IaaS permet aux clients de démarrer rapidement un nouveau projet en louant des ressources informatiques. L'évolutivité et l'élasticité, qui permettent d'augmenter ou de réduire les ressources informatiques, sont des aspects fondamentaux d'un cloud IaaS. La plupart des fournisseurs de services cloud IaaS offrent une évolutivité sous le contrôle de l'utilisateur via des interfaces de libre-service directes, permettant aux clients de demander le contrôle et la gestion des ressources informatiques ainsi que la latitude de les faire évoluer.

1.3.2 Les caractéristiques de cloud computing

Les caractéristiques de CC sont nécessaires pour une compréhension approfondie de l'idée de CC.

- **Self-service à la demande :** Sans avoir besoin d'une assistance humaine de la part du fournisseur de services, un utilisateur peut fournir des ressources informatiques telles que le temps de serveur et le stockage réseau selon les besoins.

- **Large accès au réseau :** Des techniques standards sont utilisées pour accéder aux fonctionnalités via le réseau, favorisant l'utilisation de plates-formes hétérogènes de clients légers et lourds tels que les ordinateurs portables, les PDA et les téléphones mobiles.
- **Mise en commun des ressources :** Dans un modèle à locataires multiples, les ressources informatiques du fournisseur de services, telles que le stockage, la mémoire, la bande passante du réseau, le calcul et les machines virtuelles, sont regroupées pour servir plusieurs consommateurs. Selon la demande des utilisateurs, diverses ressources physiques et virtuelles sont rapidement attribuées et réattribuées. L'abonné n'a aucune connaissance ni aucun contrôle sur l'emplacement précis des ressources livrées dans cette situation, bien que l'emplacement puisse être spécifié à un niveau d'abstraction plus élevé.
- **Évolutivité et élasticité rapides :** Les fonctionnalités sont fournies rapidement, de manière élastique et parfois de manière autonome afin de pouvoir facilement évoluer. Les consommateurs peuvent acquérir des compétences en nombre à tout moment, et elles semblent souvent illimitées.
- **Service mesuré :** Les systèmes cloud gèrent et optimisent automatiquement les ressources en utilisant une capacité de mesure à un niveau d'abstraction adapté au type de service. En offrant de la transparence aux consommateurs et aux fournisseurs de services, l'utilisation des ressources peut être vue, réglementée et signalée.

1.4 Mobile Cloud Computing

Les appareils mobiles ou objets en réseau hétérogènes (allant des smartphones, ordinateurs portables et appareils portables aux objets embarqués) devraient pouvoir partager des données à la suite de cette évolution (Weber and Weber, 2010). Comme mentionné dans (Schmohl and Baumgarten, 2008), l'hétérogénéité provient des perspectives logicielles, matérielles et architecturales. De nos jours, MC fait partie intégrante de la vie quotidienne, ce qui le rend plus confortable et efficace quel que soit le l'endroit et le temps. Les applications mobiles utilisant le CC peuvent être rapidement provisionnées et publiées avec peu de travail de la part des fournisseurs de services et de l'administration en permettant aux utilisateurs de fournir des services à la demande de manière élastique (Weber and Weber, 2010). D'autre part, MCC ne peut pas être simplement caractérisé comme la fusion des technologies MCC. Avant d'approfondir ses modèles et les vulnérabilités de sécurité restantes, il y a quelques définitions

différentes de MCC à examiner. Les auteurs (Chang et al., 2013) décrivent que Le MCC est un nouveau paradigme de cloud mobile qui combine le MC, la mise en réseau et le CC pour étudier les modèles de services mobiles, créer des infrastructures, des plates-formes et des applications de service cloud mobiles pour les clients mobiles. Son objectif principal est de fournir aux consommateurs des services mobiles sensibles à la localisation qui sont mobiles, en utilisant des ressources cloud mobiles évolutives dans les réseaux, les ordinateurs, le stockage et les appareils mobiles. Son but est de leur fournir des ressources cloud mobiles sécurisées, des applications de service et des données via des ressources cloud mobiles économes en énergie sur une base "pay-as-you-go". Une autre définition d'IBM est la suivante : le MCC est une nouvelle plate-forme qui combine des appareils mobiles avec le CC pour établir une nouvelle infrastructure dans laquelle le cloud effectue le gros du travail des tâches de calcul intensif et stocke de gros volumes de données. Le traitement et le stockage des données ont lieu en dehors des appareils mobiles dans cette nouvelle architecture (“What is mobile cloud computing? - Cloud computing news,” n.d.). (Fernando et al., 2013) proposent une autre définition du MCC : Le terme MCC fait souvent référence à l'exécution d'une application, telle que Gmail de Mobile Google, sur un serveur distant riche en ressources, tandis que l'appareil mobile fonctionne comme une connexion client léger sur un réseau sans fil. D'autres exemples incluent les services de localisation de Facebook. La Figure 1.3 illustre l'architecture générale de MCC.

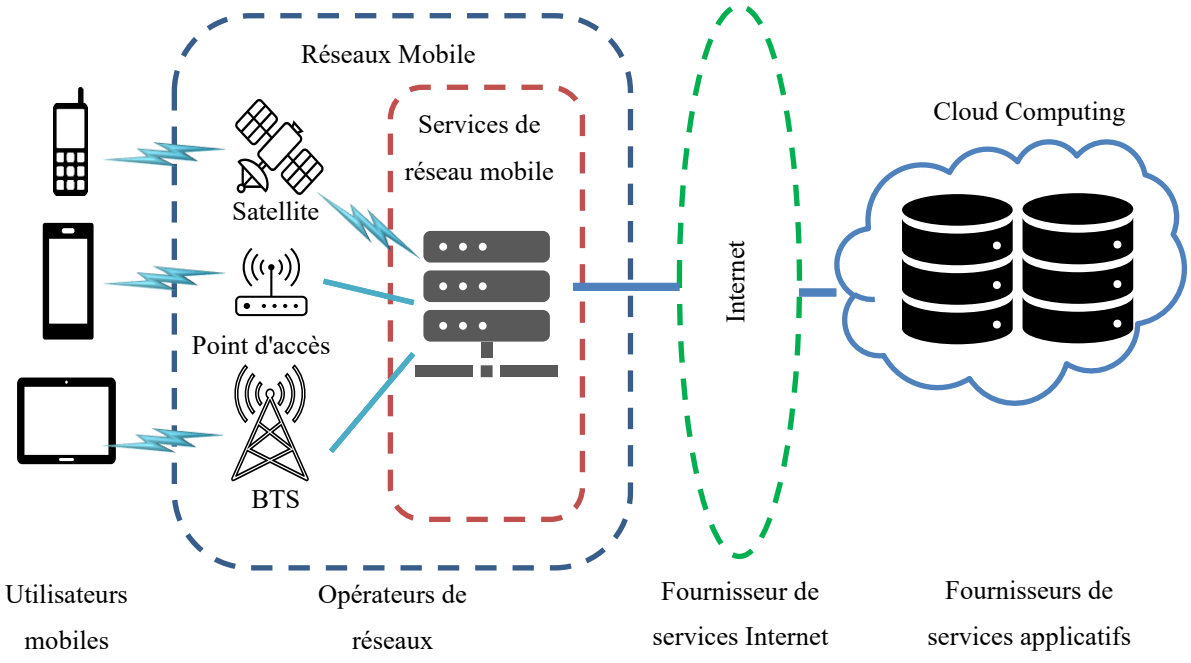

Figure 1.3 L'architecture générale de MCC (Donald and Arockiam, 2014).

1.4.1 Les modèles de Mobile Cloud Computing

Différentes architectures ont été définies dans la littérature pour répondre à différents cas d'utilisation dans le MCC (“A Survey of Mobile Cloud Computing - ztecommunications,” n.d.; Dinh et al., 2013; Fernando et al., 2013; Zhang and Li, 2016) afin de souligner la motivation du MCC. Le principal avantage du CC pour les appareils mobiles est qu'il permet d'exécuter des applications entre des appareils aux ressources limitées et un cloud basé sur Internet. Par conséquent, les appareils disposant de ressources limitées peuvent décharger les processus de calcul, de communication gourmands en ressources vers le cloud. Les applications mobiles de collaboration dans le cloud peuvent déployer leurs composants sur divers emplacements, y compris les téléphones intelligents locaux, les ordinateurs virtuels dans le cloud et les cloudlets. Les sections suivantes décrivent les nombreux modèles de MCC.

a) Serveur Cloud – Modèle client

MCC tente d'étendre les capacités des périphériques de stockage/calcul limitées et de permettre un accès fluide aux données/applications sur un serveur distant riche en ressources depuis n'importe où, comme indiqué précédemment. Un appareil mobile se connecte à un serveur cloud distant, qui sert de fournisseur de services. Pour garantir la qualité de service et une transition transparente, la connectivité réseau de l'appareil au serveur cloud doit être optimisée. Avec le slogan « Pas de cloud sans virtualisation », de nombreuses solutions existantes prennent en charge cette architecture en exploitant des techniques de virtualisation basée sur des machines virtuelles et sur des conteneurs pour réduire le temps de traitement et améliorer l'efficacité énergétique.

b) Cloud Virtuel

Une autre approche (Huerta-Canepa and Lee, 2010), (Barca et al., 2017) consiste à créer un cloud avec des appareils mobiles connectés bout à bout pour le stockage et le traitement des données, les appareils mobiles agissant comme des fournisseurs de ressources cloud virtuelles. Les appareils mobiles de cette architecture fonctionnent soit en tant que fournisseurs de services, soit en tant que consommateurs, chaque appareil mobile peut collaborer avec ses voisins pour collecter et distribuer des informations sur son environnement à des fins spécifiques telles que des applications de trafic, des moniteurs de soins de santé, etc.

c) Modèle cloudlet

Le concept de cloudlet, tel que proposé dans (Satyanarayanan et al., 2009), est une architecture MCC alternative dans laquelle le cloudlet est représenté comme des éléments de déchargement intermédiaires dans une structure à trois niveaux : appareil mobile-Cloudlet-Cloud. La figure 1.4 représente un cloudlet comme un ordinateur riche en ressources, bien connecté et puissant installé dans une infrastructure publique avec accès à un serveur cloud. Il peut être implémenté à l'aide de serveurs hotspot Wi-Fi prenant en charge des hyperviseurs pour la gestion des machines virtuelles, ou il peut correspondre à de puissantes stations de base dans un environnement informatique de périphérie mobile. Cela permet à l'appareil mobile à proximité de se décharger de sa charge de travail tout en maintenant une faible latence et une bande passante élevée. Prenons comme exemple la détection d'événements en temps réel, lorsqu'un voyageur étranger visite un musée local, il est confronté à une barrière linguistique qui l'empêche de comprendre pleinement toutes les œuvres d'art. Si cloudlet n'est pas proche, il devra se connecter à un cloud distant via un réseau mobile 3G/4G, ce qui est cher et pas toujours disponible. Il peut utiliser les services de cloudlet pour la traduction linguistique, le traitement d'images et l'envoi de flux vidéo à ses contacts avec une faible latence, une bande passante élevée et un traitement puissant, grâce au cloudlet, qui est placé partout comme point d'accès Wi-Fi.

Dans (Simanta et al., 2012), Simanta et al. ont proposé un exemple de mise en œuvre de cloudlet dans le but d'améliorer le traitement et de préserver l'énergie de la batterie dans les appareils mobiles, en particulier dans les environnements hostiles où les réseaux sont instables. Les éléments déchargés sont sans état, ce qui est une caractéristique majeure de l'architecture. Ce n'est que pendant la configuration et l'approvisionnement que le cloudlet communique avec le cloud central. Une fois provisionné, il fonctionne selon deux modes : déconnecté du cloud central et connecté à l'appareil mobile. Lorsqu'un appareil mobile est connecté à un cloudlet, la superposition d'application de l'appareil mobile est déchargée sur le ce dernier. La différence entre une machine virtuelle de base avec uniquement le système d'exploitation installé et la même machine virtuelle avec l'application déployée est représentée par une superposition d'application. Plusieurs machines virtuelles peuvent être hébergées sur le cloudlet qui est actuellement proposé pour une application dans une variété de domaines, y compris de véhicule à véhicule (Kotevska et al., 2016) et aussi militaire (Lewis et al., 2014).

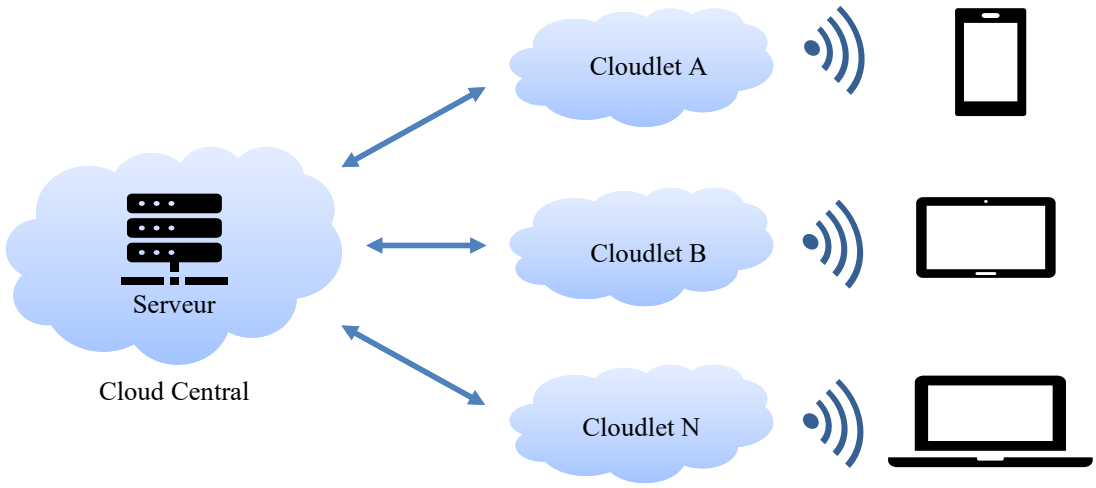

Figure 1.4 Modèle de Cloudlet (Ali, 2020).

1.4.2 Les caractéristiques du Mobile Cloud Computing

Les caractéristiques principales du MCC sont illustrées dans la figure 1.5, et sont décrites en détail comme suit :

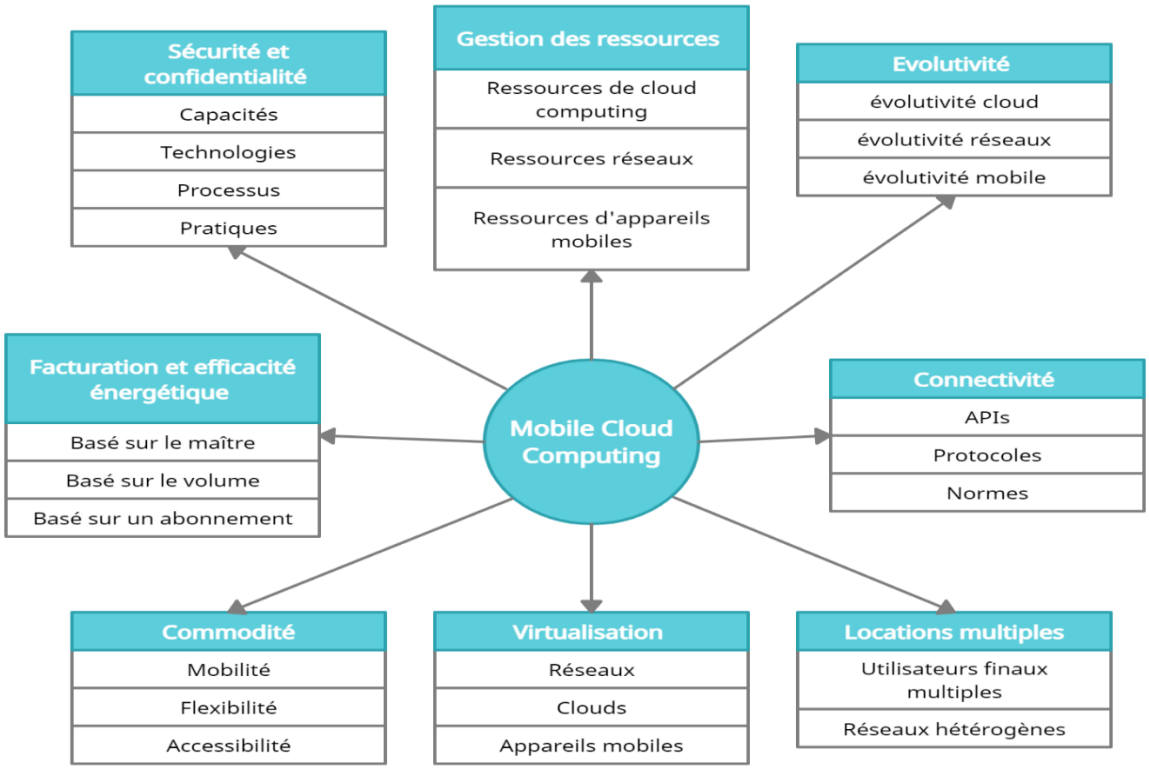

Figure 1.5 Les principales caractéristiques du Mobile Cloud Computing (Yu and Leung, 2015).

- **Gestion des ressources :** Les mobiles clouds peuvent gérer les ressources plus librement et automatiser le provisionnement et le dé-provisionnement des ressources. Les ressources qui doivent être gérées incluent celles de calcul, celles du réseau et celles des appareils mobiles.
- **Sécurité et confidentialité :** Cette fonctionnalité est basée sur un ensemble de capacités, de technologies, de processus et de pratiques de sécurité. elle est conçue pour protéger les appareils mobiles, les réseaux hétérogènes, les clouds et les données contre les attaques, les dommages et les accès non autorisés.
- **Evolutivité :** Cette fonctionnalité prend en compte trois éléments d'évolutivité dans les environnements de mobiles CC: l'évolutivité du cloud, l'évolutivité du réseau et l'évolutivité des appareils mobiles.
- **Facturation et efficacité énergétique :** Plusieurs modèles de facturation de service sont disponibles dans le Mobile Cloud, notamment ceux basés sur les compteurs, les volumes et les abonnements.
- **Commodité :** les utilisateurs finaux peuvent accéder aux ressources du cloud (les services et les applications) n'importe quant et n'importe où, dans l'environnement du MCC.
- **Locations multiples :** Le Mobile Cloud peut désormais gérer de nombreux utilisateurs finaux dans des réseaux hétérogènes grâce à cette capacité.
- **Virtualisation :** il existe trois types de virtualisation (Virtualisation du réseau, virtualisation du cloud et la virtualisation des appareils mobiles) qui peuvent être utilisés dans les environnements du MCC.
- **Connectivité :** cette caractéristique adopte les APIs bien conçus, les protocoles et les normes offerts par les travaux existants dans le domaine du Mobile Cloud pour permettre la connectivité entre les différents réseaux et les applications tiers ou les systèmes d'une façon aisée et sécurisée.

1.4.3 Les Avantages du Mobile Cloud Computing

On améliore les appareils mobiles en déchargeant les calculs exigeants et les éléments de fichiers volumineux vers le cloud dans MCC. Cela présente de nombreux avantages et constitue la principale raison du succès du MCC. Voici les principaux avantages de l'adoption du MCC par rapport aux services non-cloud qui ne s'exécutent que sur les appareils mobiles :

- **Une fiabilité et une disponibilité élevées :** Les utilisateurs peuvent enregistrer en toute sécurité des données et des programmes en les stockant dans le cloud. Même si les appareils mobiles sont cassés, volés, transférés ou ont une batterie faible, les données et les applications sont conservées en toute sécurité. Grâce à leur architecture stable et robuste, le service cloud offre une haute disponibilité (Mohiuddin et al., 2012).
- **Capacités améliorées sur les appareils mobiles :** Les utilisateurs peuvent bénéficier de calculs plus rapides et d'un stockage de données plus important en exploitant la puissance de calcul plus élevée et le stockage de données plus important sur les machines cloud (Vandenbroucke et al., 2014; YangLei et al., 2013).
- **Durée de vie prolongée de la batterie :** Les appareils mobiles peuvent économiser beaucoup d'énergie en déplaçant des calculs intensifs et des traitements sophistiqués vers des serveurs cloud (Ge et al., 2012; Seneviratne et al., 2013).
- **Évolutivité souple et transparente :** L'approvisionnement des services cloud est élastique, ce qui implique qu'il est proposé à la demande. Par conséquent, même si leur utilisation augmente, les utilisateurs d'appareils mobiles ne sont pas toujours conscients du déchargement des calculs et du stockage vers le cloud (Bifulco et al., 2012).

1.4.4 Les systèmes et applications de mobiles cloud computing

Le MCC a été utilisé dans des domaines fonctionnellement variés en raison de ses avantages distincts dans de nombreux aspects, de la finance au divertissement, ce qui n'est que l'un des domaines d'application. En conséquence, ils sont soutenus par une gamme de types distincts de conception de système. Bon nombre de ces applications sont des extensions de services Web existants, les appareils mobiles servant d'outil d'interface utilisateur pratique tout en profitant du puissant environnement de calcul fourni par les serveurs cloud.

- **Healthcare mobile :** La mobilité est très précieuse dans le secteur de la santé. Lorsqu'une situation d'urgence survient, il est simple de contacter les appareils mobiles et de demander de l'aide. Les gadgets mobiles sont également utiles pour rester à proximité des patients pour une surveillance 24 heures sur 24 et consulter leurs dossiers médicaux (Kumar and ManjupPriya, 2014; Zhou et al., 2015).
- **Commerce mobile :** La livraison de services de commerce électronique directement dans la main du client, n'importe où, via la technologie sans fil est connue sous le nom de commerce mobile ou M-commerce (Chang, 2014; Li and Autran, 2009). Le transfert d'argent mobile, les guichets automatiques mobiles, le ticking mobile, les coupons mobiles,

l'achat mobile et la publicité mobile sont tous des exemples de commerce mobile. Le commerce mobile améliore sa sécurité et offre des services omniprésents et synchronisés dans le monde entier en interagissant avec le cloud.

- **Jeu mobile :** Le jeu mobile est une activité lucrative qui se développe rapidement. Les jeux multi-joueurs permettent aux joueurs de communiquer entre eux sur Internet, ce qui rend le jeu plus dynamique et conversationnel. Certains jeux transfèrent une partie ou l'intégralité du moteur de jeu vers un serveur cloud qui nécessite des calculs intensifs, tels que le rendu graphique. Le déchargement peut également préserver l'énergie, permettant aux utilisateurs de pratiquer le jeu plus longtemps (Wang et al., n.d., 2013).
- **Apprentissage mobile :** L'apprentissage mobile a évolué à partir du e-learning, ou apprentissage en ligne. Le coût élevé des appareils et les exigences de performances élevées du système pour la lecture des vidéos ont, au début, entravé les services d'apprentissage mobile. Ce problème a été résolu par l'expansion continue de la capacité de calcul dans les appareils mobiles, ainsi que leur intégration avec les services cloud (Kumar and Pilli, 2012; Picek and Grcic, 2013). Les étudiants peuvent désormais découvrir facilement les enseignants et accéder au matériel d'apprentissage via leurs appareils mobiles, renforçant la popularité de l'apprentissage mobile.

1.4.5 Les Problèmes de sécurité dans le Mobile Cloud Computing

La sécurité est un enjeu clé pour le MCC. Il présente divers défis de sécurité, notamment le contrôle d'accès aux données, la distribution des données sur une infrastructure distribuée, l'intégrité des données, la disponibilité des services, la communication sécurisée et la sécurité des applications. De plus, la mobilité complique les problèmes de sécurité.

En général, le MCC aborde les problèmes de sécurité sous deux angles : le point de vue des mobiles (ou des appareils embarqués légers) et le point de vue du système de provisionnement des ressources virtualisées (par exemple, les clouds Internet ou les ressources informatiques dédiées proches des mobiles). Les appareils mobiles doivent être exempts de logiciels dangereux, y compris les virus et les chevaux de Troie. Les programmes malveillants présentent un risque de sécurité car ils peuvent altérer le comportement d'une application, entraînant une fuite ou une corruption des données. Ainsi, la surveillance et l'analyse de la sécurité doivent être utilisées de manière continue et régulière pour protéger les appareils mobiles des logiciels malveillants. La surveillance et l'analyse sécurisées des applications cloud mobiles, d'autre part,

sont une tâche gourmande en ressources qui nécessite fréquemment des réponses en temps réel difficiles à satisfaire dans un contexte mobile et aux ressources limitées.

(Fernando et al., 2013) décrit sept vulnérabilités de sécurité que les clients doivent prendre en compte lors de l'utilisation du CC en général :

1. *Accès utilisateur privilégié :* Le déchargement de données sensibles vers le cloud impliquerait que les données perdraient le contrôle physique, logique et personnel direct.
2. *Conformité à la réglementation :* Les fournisseurs de services de CC doivent être prêts à se soumettre à des audits externes et à des certifications de sécurité.
3. *Emplacement des données :* L'emplacement physique précis des données de l'utilisateur est inconnu, ce qui peut entraîner une incertitude quant aux pays particuliers et aux obligations de se conformer aux lois locales sur la confidentialité.
4. *Ségrégation des données :* Étant donné que les données du cloud sont souvent conservées dans un emplacement commun, il est essentiel que les données de chaque utilisateur soient cryptées efficacement.
5. *Récupération :* Les fournisseurs de cloud doivent s'assurer que les données et les services sont correctement récupérés en cas de panne technique ou autre sinistre.
6. *Accompagnement d'enquête :* Étant donné que les journaux et les données de plusieurs clients peuvent être localisés, il peut être difficile d'enquêter sur des activités illégales ou contraires à l'éthique.
7. *Viabilité à long terme :* L'assurance que les données des consommateurs resteront sécurisées et accessibles même en cas de faillite du fournisseur de cloud.

L'intégration des appareils mobiles avec l'infrastructure cloud a entraîné une variété de problèmes de sécurité, qui sont à l'étude. Cela englobe l'authentification, l'autorisation, la sécurité des données, la sécurité et l'intégrité des applications, la confidentialité, la gestion des droits numériques et d'autres fonctions et technologies connexes. Tous ces sujets seront discutés en conjonction avec leurs plans actuels.

a) Sécurité des applications

Les appareils mobiles exécutent diverses applications. Ces applications sont principalement utilisées pour la gestion des informations personnelles et à des fins commerciales. Parmi ces applications figurent le chat sur Internet, le courrier électronique, les jeux et les ordonnanceurs. Les services cloud de ces applications cloud mobiles sont essentiels. La majorité de ces

applications sont disponibles au téléchargement sur le Google Play Store, l'Apple App Store, le Nokia App Store ou un magasin d'applications tiers. Ces magasins ne disposent d'aucun mécanisme pour supprimer les logiciels malveillants des applications. Dinh et al. (Dinh et al., 2013) estiment que 10 milliards d'applications ont été téléchargées sur le marché Android en 2010, dont 250 000 contiennent des malwares. Un code malveillant est utilisé pour modifier des applications légitimes, qui sont ensuite distribuées via des référentiels non officiels. De telles applications, par exemple, divulguent des données privées, composent des numéros surtaxés et sont activées par porte dérobée via SMS. En conséquence, certains schémas doivent être mis en place pour gérer la sécurité de ces applications ainsi que la menace posée par les applications cloud mobiles. La section suivante traite de divers schémas de sécurité des applications et des menaces associées.

- **Schémas existants pour la sécurité des applications**

Kilin et al. [9] ont présenté WallDroid, un pare-feu spécifique aux applications. WallDroid est avant tout un pare-feu pour les applications Android avec d'autres fonctionnalités. La technologie VPN et le cadre de messagerie cloud-à-appareil (C2DM) pour Android sont des composants essentiels de cette architecture pour assurer la sécurité. Le cloud est utilisé dans cette architecture pour suivre des millions d'applications et leur réputation, ainsi que pour comparer le trafic à une liste de serveurs IP malveillants connus. Chaque application a son propre identifiant unique, composé d'un certificat et d'une valeur de hachage. Les applications Android sont divisées en trois catégories en fonction de leur réputation : les bonnes, les mauvaises et les inconnues. Les applications bien connues sont les bonnes applications, tandis que celles qui sont reconnues comme malveillantes sont celles qui ne sont pas connues pour être les bonnes et les mauvaises.

Si l'application est bonne, elle est directement connectée ; si elle est réputée dangereuse, la connexion Internet est interrompue. La Figure 1.6 montre comment le service VPN est utilisé pour accéder à Internet via un serveur VPN pour des applications inconnues. Le VPN examine ensuite le flux de données pour déterminer s'il est malveillant et s'il envoie des données personnelles en texte clair. Si le serveur VPN le juge hostile, il limitera son trafic. Cette approche est proposée pour identifier les applications Android dangereuses et inconnues [9].

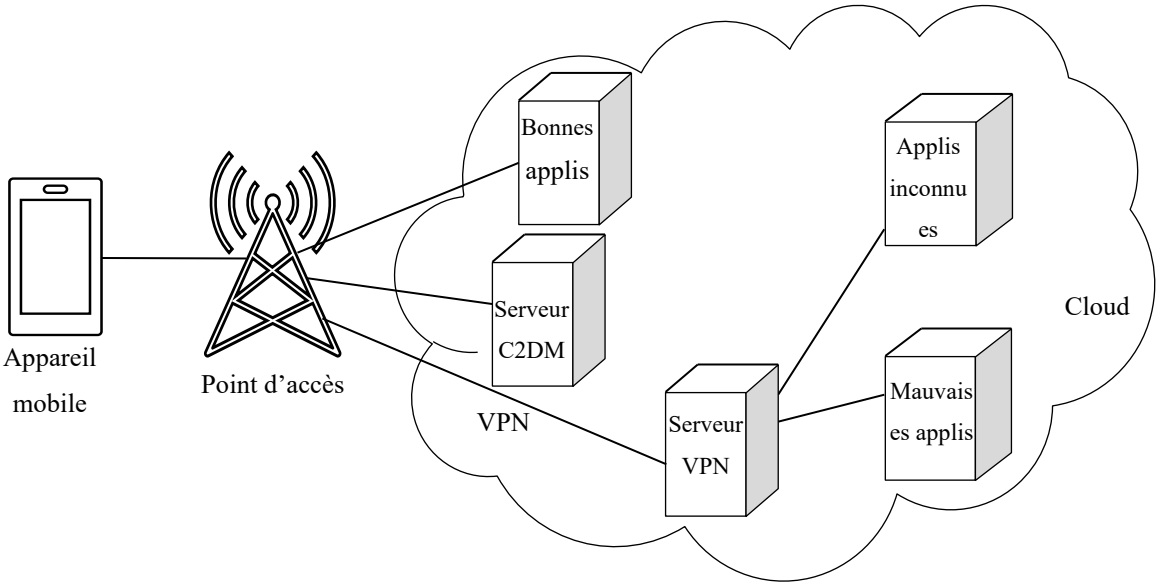

Figure 1.6 L'architecture de WallDroid (Kilinc et al., 2012).

b) Problèmes d'authentification

Le déplacement des données personnelles et professionnelles vers le cloud soulève des inquiétudes en matière de sécurité et de confidentialité. Pour s'assurer que seules les personnes autorisées ont accès à ces données sensibles, un mécanisme d'authentification est utilisé. Traditionnellement, un utilisateur s'authentifie en fournissant son mot de passe au service demandé, qui peut être compromis. L'authentification légale des utilisateurs devient critique dans le cloud mobile. Une illustration simplifiée de la procédure d'authentification est présentée à la figure 1.7 La section suivante traite de divers systèmes d'authentification pour les utilisateurs du cloud qui utilisent leurs appareils mobiles pour se connecter.

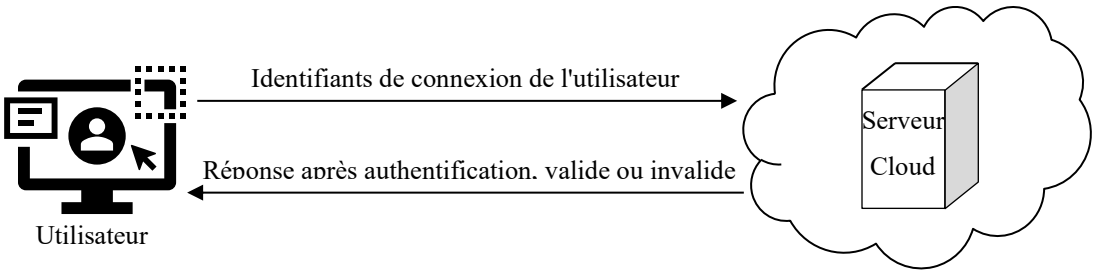

Figure 1.7 Exemple simple de processus d'authentification.

- **Schémas d'authentification existants :**

Chow et al. (Chow et al., 2010) présentent une technique d'authentification qui n'exige pas que l'utilisateur soumette un mot de passe, un nom d'utilisateur ou des données biométriques. Ce framework authentifie les utilisateurs à l'aide de TrustCube et génère un score basé sur leur comportement. Le score d'authentification probabiliste généré est ensuite comparé à une valeur seuil pour déterminer si le client est authentique ou non. Le score d'authentification n'est pas fixe et peut être ajusté pour répondre aux besoins des applications individuelles. Comme le montre la figure 1.8, cette méthode est composée de quatre modules : les appareils clients, le consommateur d'authentification, le moteur d'authentification et l'agrégateur de données. L'appareil client crée un contexte et une activité visibles, tels que l'historique du navigateur Internet, les enregistrements d'appels, l'historique de localisation, les MMS, les SMS et les informations téléphoniques.

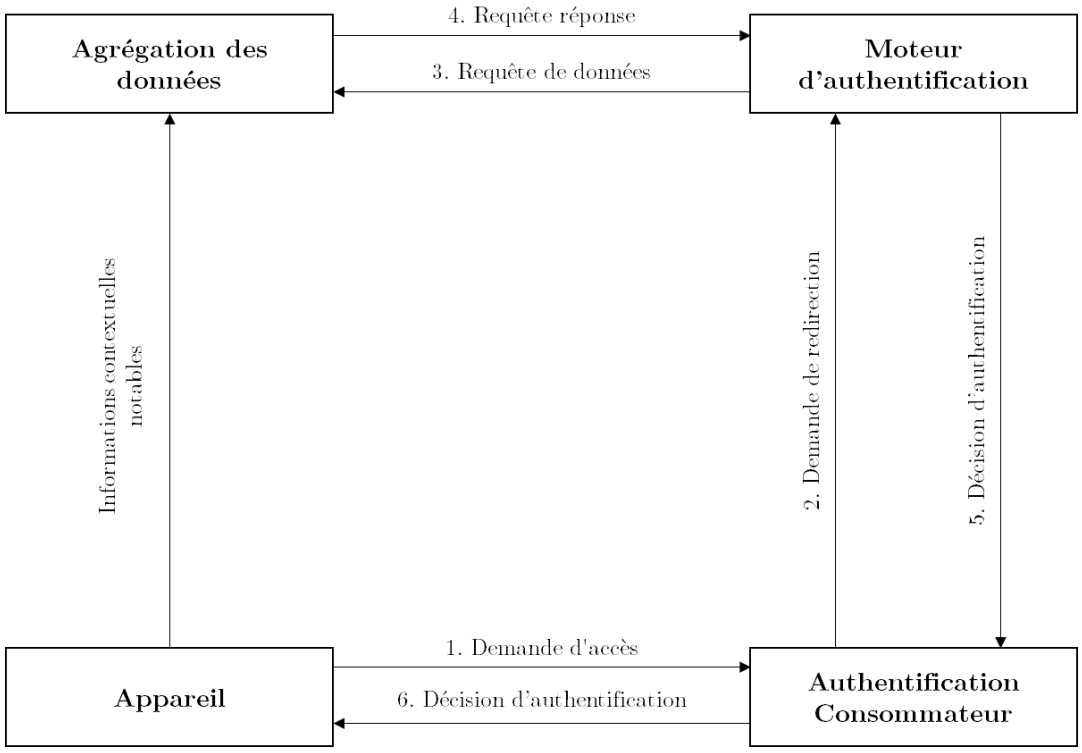

Figure 1.8 L'architecture d'authentification (Chow et al., 2010).

Les données de l'appareil client sont mises en cache localement jusqu'à ce qu'elles soient collectées par l'agrégateur de données. Pour authentifier le dispositif mobile, le moteur d'authentification extrait des informations de contexte notables de l'agrégateur de données et des politiques d'authentification du consommateur d'authentification. Les politiques

d'authentification sont déterminées par la nature de la demande du client. Enfin, le moteur d'authentification répond au client en utilisant les données du consommateur d'authentification.

Grzonkowski et al. (Grzonkowski et al., 2011) présentent une stratégie d'authentification de nouvelle génération pour les appareils mobiles et CE qui utilisent une technique de Zero Knowledge Proof (ZKP) pour authentifier l'ID. Cette stratégie est de nature anti-hameçonnage, car elle ne divulgue pas le mot de passe de l'utilisateur au site Web que l'utilisateur visite. Une fois connecté, l'utilisateur n'est pas redirigé vers d'autres pages Web. SeDiCi 2.0 est le nom donné à ce schéma, qui comprend trois entités : un client (C), un service (S) et des services d'authentification (AS). Le flux de données entre les trois entités est illustré à la figure 1.9. Pour générer la clé publique, le client enregistre un compte dans AS à l'aide du mot de passe de son application cliente.

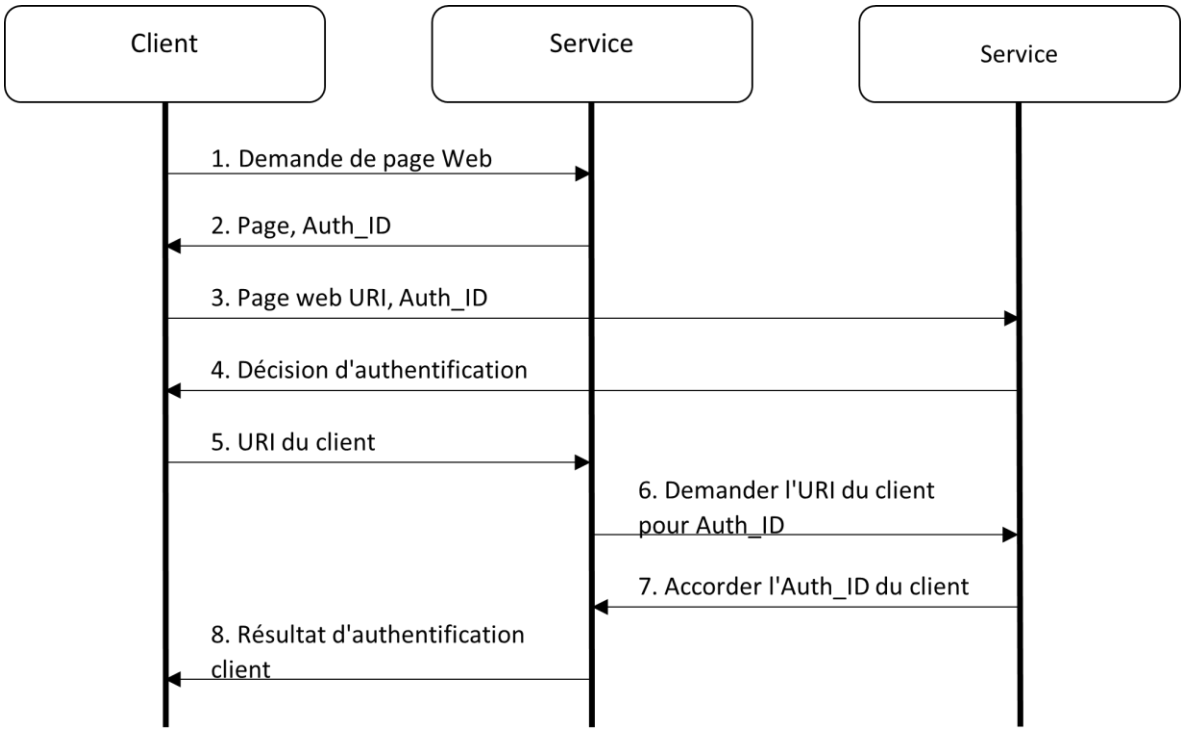

Figure 1.9 Le flux de données de SeDiCi 2.0 pour l'authentification (De, 2016).

Pour utiliser le service, le client doit d'abord s'inscrire auprès de ce dernier. Après cela, le service vérifie le client et garde une trace de ses informations de connexion. Les informations de connexion pour le client ainsi que la clé publique sont envoyées à AS. Pour s'authentifier auprès du service, le client doit revenir au service et obtenir l'identifiant d'authentification du service en guise de réponse. L'identifiant d'authentification et l'URI sont ensuite soumis à AS, où l'URI correspondant à l'identifiant d'authentification est vérifié par AS. Maintenant que

l'URI a été exposé avec l'ID d'authentification fourni, le client peut envoyer une demande de connexion au service qui peut vérifier l'identité du client à l'aide de l'ID d'authentification. Si la vérification réussit, l'identité du client est vérifiée à nouveau.

Zhao et al. (Zhao et al., 2013) proposent un mécanisme d'authentification avancé basé sur le cryptage biométrique, qui est décrit en détail. L'authentification peut être effectuée à l'aide de cette méthode lorsque les appareils mobiles sont équipés de capteurs biométriques, comme le montre la Figure 1.10.

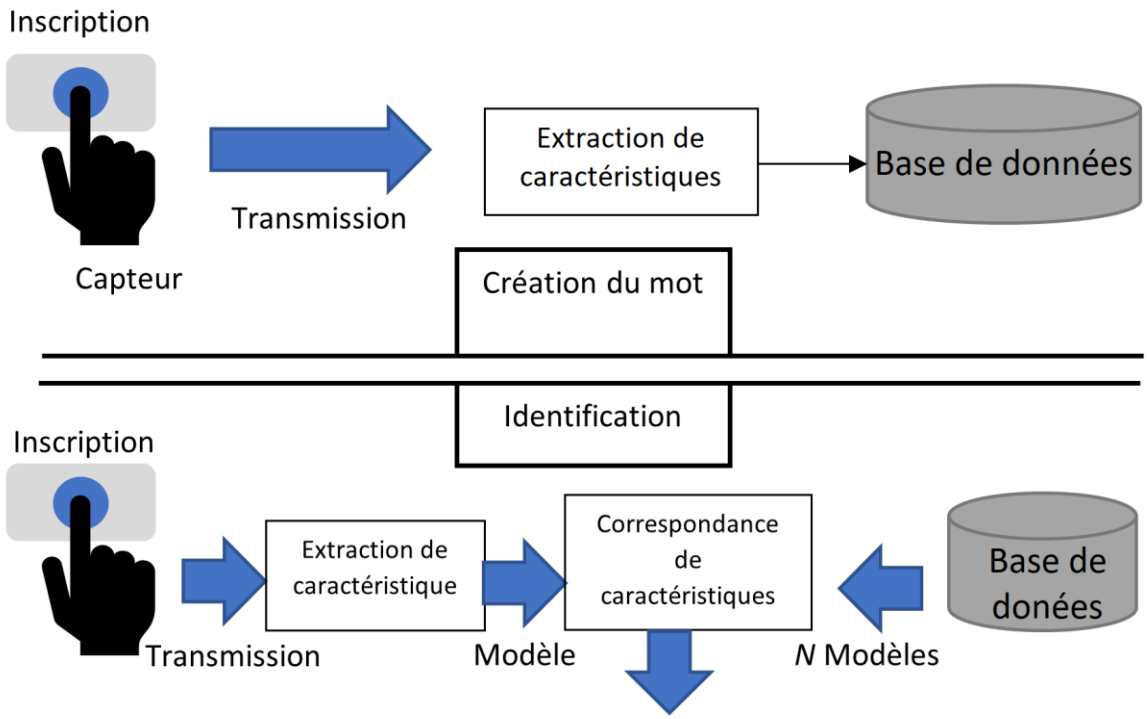

Figure 1.10 Le schéma d'authentification biométrique basé sur le cryptage (Zhao et al., 2013).

En raison de la difficulté d'oublier, de falsifier, de partager ou de perdre des données biométriques, cette méthode est plus fiable que les schémas classiques basés sur un mot de passe. Les données biométriques des utilisateurs sont conservées dans une base de données sur le cloud, à laquelle ils peuvent accéder de n'importe où.

Dans (Al Rassan and Alshaher, 2014), Lehab AL Rassan et al. ont développé un concept de sécurisation du cloud mobile à l'aide de l'authentification biométrique, qui a été mis en œuvre (SMCBA). Ils ont utilisé un système de reconnaissance d'empreintes digitales pour améliorer les ressources du cloud mobile, qui consiste à utiliser la caméra de l'appareil mobile comme capteur pour prendre une image de l'empreinte digitale, puis à effectuer un pré-traitement sur

l'image, suivi de l'étape d'extraction des caractéristiques, et enfin comparer cette image aux données enregistrées pour autorisation.

c) Sécurité des données

Cette section traitera principalement de la sécurité des données envoyées depuis les appareils mobiles vers le stockage dans le cloud. Les données privées, commerciales, financières et d'entreprise sont stockées sur des appareils mobiles. La fuite de ces informations confidentielles à des tiers peut entraîner un préjudice personnel et économique. Lorsque de telles données critiques sont déplacées vers le cloud, des problèmes supplémentaires surviennent. L'utilisateur renonce au contrôle des données stockées hors site. Par conséquent, ces données déchargées doivent rester sécurisées et privées. Il doit y avoir une méthode en place pour assurer l'intégrité et la disponibilité des données en cas de besoin. De plus, l'utilisateur doit être informé de l'emplacement de ses données. La section suivante traite de certaines techniques liées à la sécurité des données dans le MCC.

- **Schémas existants pour la sécurité des données**

Pour protéger les données des attaques, de nombreuses techniques cryptographiques sont utilisées. La cryptographie incrémentielle, le cryptage basé sur les attributs, les signatures numériques, le cryptage basé sur l'identité, les codes d'authentification des messages et les fonctions de hachage sont tous des exemples de ces méthodes. Certains auteurs ont également pris en compte les contraintes de ressources des appareils mobiles lors du développement de leurs solutions. Hsueh et al. (Hsueh et al., 2011) discutent d'une technique d'authentification des utilisateurs mobiles et de l'intégrité des données des appareils mobiles. Des algorithmes de chiffrement standard, des fonctions de hachage, des signatures numériques, des nombres aléatoires et des valeurs secrètes sont utilisés dans cette approche pour garantir la sécurité globale des données des appareils mobiles pendant leur déchargement dans le cloud. SSL est utilisé pour protéger l'accès, et les individus comme les groupes peuvent créer des listes de contrôle d'accès (ACL). Comme le montre la Figure 1.11, cette structure se compose principalement de quatre modules : appareil mobile (MD), fournisseur de services cloud (CSP), autorité de certification (CA) et module de télécommunication (TM).

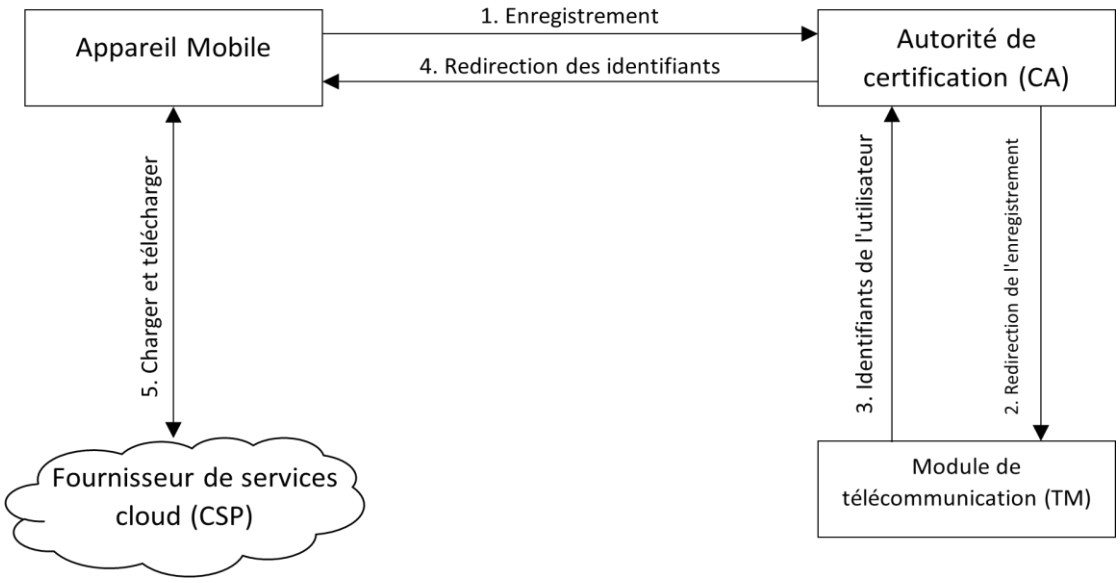

Figure 1.11 L'architecture de stockage sécurisé des données dans le cloud (De, 2016).

Dans ce modèle, l'autorité de certification est responsable de l'authentification des appareils mobiles. Le module de télécommunications génère et stocke des mots de passe et d'autres informations nécessaires pour accéder aux services cloud sur l'appareil mobile.

Il est prévu dans ce cadre que la clé sécurisée (SK), la clé publique (PK) et la clé de session (SEK) soient distribuées de manière sécurisée sur les appareils mobiles, le modèle de communication et l'AC. Pour utiliser les services cloud, l'utilisateur mobile doit d'abord s'inscrire auprès de CA. Une fois l'enregistrement réussi, TM fournit un mot de passe unique (PWD) aux appareils mobiles pour accéder aux ressources cloud. L'Équation 1.1 le démontre.

$$MD \rightarrow CA: E_{PKTM}E(MU, Num, TK), U_N, S_{SKMU}(MU, Num), H(MU, Num)$$

Équation 1.1

Où

MU représente le nom de l'utilisateur mobile

Num représente le numéro de l'utilisateur mobile

TK est une combinaison de *Num* et de cloud *PWD* aléatoire

U_N est le nombre aléatoire généré pour la preuve d'identité

H est la fonction de hachage standard, E_{PKTM} représente le cryptage avec le *PK* de *TM*

S_{SKMU} génère une signature pour l'utilisateur mobile à l'aide d'une fonction cryptographique sur la valeur transmise et la *SK* de l'appareil mobile

L'autorité de certification authentifie l'utilisateur en fonction de la signature qu'elle reçoit dans le message. TM reçoit le message donné dans l'Équation 1.2 si l'utilisateur est légitime.

$$CA \rightarrow TM: E_{PKTM}(MU, Num, TK), U_N, S_{SKCA}\big(H(MU, NUM)\big)$$

Équation 1.2

La TM vérifie l'identité de l'AC à l'aide de la clé S_{SKCA}. Si l'AC est authentifié, le TM enregistre l'utilisateur mobile et stocke ses données dans une base de données locale. Les données seront utilisées dans le futur à des fins de vérification. Pour une transmission sécurisée, la TM génère un PWD pour l'appareil mobile et le crypte à l'aide du PK de l'appareil mobile. PWD est crypté une fois de plus avec TK pour s'assurer qu'il ne peut être décrypté que par un utilisateur autorisé à la réception. Comme le montrent l'Équation 1.3 et l'Équation 1.4, TM transmet des informations sécurisées à l'appareil mobile via CA.

$$TM \rightarrow CA: E_{PKMU}\big(MU, Num, U_N, E_{TK}, (PWD)\big)$$

Équation 1.3

$$CA \rightarrow MD: E_{PKMU}\big(MU, Num, U_N, E_{TK}, (PWD)\big)$$

Équation 1.4

L'appareil mobile crypte maintenant le fichier avec SEK et le télécharge dans le cloud, avec PWD, MU et S_{SKMU}, comme spécifié dans l'Équation 1.5.

$$MD \rightarrow C: PWD, MU, E_{SEK}(Data), S_{SKMU}\left(H\left(MU||SV||E_{SEK}(Data)\right)\right)$$

Équation 1.5

Où SV désigne la valeur secrète de l'appareil mobile, qui n'est connue que de MD, CA et TM. MD doit envoyer PWD, MU et H(MU || SV) afin de télécharger un fichier dans le cloud. Ce dernier produit une nouvelle valeur de hachage à l'aide de MU et SV, puis la compare à la signature reçue pour s'authentifier. Il transfère ensuite le fichier crypté à MD, accompagné de la signature spécifiée dans l'Équation 1.6.

$$C \rightarrow MD: E_{SEK}(Data), H(E_{SEK}(Data)||SV)$$

Équation 1.6

L'appareil mobile décrypte le fichier à l'aide de SEK après avoir reçu la signature.

Le traitement sécurisé des données s'effectue grâce à l'utilisation de la gestion de la confiance et de la séparation des données privées. Pour la gestion de la confiance dans ce modèle, la cryptographie basée sur l'identité et le contrôle d'accès aux données basé sur les attributs sont utilisés (Huang et al., 2011). Il protège la sécurité et la confidentialité des appareils mobiles à l'aide d'une gestion sécurisée des données et d'une gestion de la confiance multi-locataires, ainsi que d'un modèle de traitement des données basé sur des images semi-ombragées étendues (ESSI). Trois domaines composent cette architecture : le service public et le stockage dans le cloud, le cloud de confiance et les mobiles et la détection dans le cloud. Alors que le service cloud et les domaines de stockage fournissent le SaaS, les domaines de confiance cloud supervisent la distribution des certificats et des clés, ainsi que la gestion des identités.

Les attributs publiquement disponibles sont utilisés pour générer des clés privées pour une communication sécurisée dans la gestion des identités basée sur les attributs. Cette identification peut être utilisée conjointement avec une signature pour vérifier l'identité de l'utilisateur. ESSI est également appelé clone d'appareils mobiles qui s'exécutent dans un domaine de confiance basé sur le cloud. ESSI permet aux appareils mobiles d'avoir plus de stockage et de puissance de calcul. De plus, il protège et sécurise les données et les informations de l'appareil. Des politiques et réglementations sécurisées sont mises en œuvre dans le domaine de confiance cloud à l'aide d'un pare-feu distribué qui analyse tous les paquets entrants et sortants à la recherche de logiciels malveillants.

Le système de gestion des données est segmenté en deux types de données : critiques et non critiques. La clé générée par l'utilisateur est utilisée pour chiffrer les données critiques, tandis que la clé générée par le cloud est utilisée pour chiffrer les données non critiques. ESSI classe les données qu'il reçoit comme non critiques ou critiques. Si les données sont jugées critiques, elles sont chiffrées, déchiffrées et vérifiées (EDV) avant d'être conservées dans le stockage sécurisé d'ESSI. Selon la préférence de l'utilisateur, la technique de masquage préserve la confidentialité des données. Cela permet l'évolutivité, la protection des données, le traitement distribué et la résistance aux défaillances ponctuelles.

Le Tableau 1.1 compare deux techniques de sécurité des données en fonction de leurs méthodes de cryptage et de leurs fonctions de sécurité, ainsi que de leurs inconvénients.

Tableau 1.1 La comparaison de différents systèmes de sécurité des données

Schéma de cryptage/Méthode/Principe	**Fonctions de sécurité**				
	Intégrité	Confidentialité	Authentification	Autres caractéristiques	Inconvénients
Fonction de hachage standard, signature numérique (Hsueh et al., 2011)	Oui	Oui	Oui	Simple et facile à mettre en œuvre	Moins économes en énergie et évolutif
Chiffrement basé sur les attributs et cryptographie basée sur l'identité (Huang et al., 2011)	Non	Oui	Oui	Résistance à la défaillance ponctuelle, évolutive, économe en énergie	L'appareil mobile est compromis si ESSI est attaqué et manipulé.

d) Gestion des droits numériques

Les livres électroniques, les photos, les sons et les films, entre autres contenus numériques, sont désormais enregistrés dans le cloud. Ces contenus sont accessibles aux utilisateurs mobiles via Internet à partir de serveurs cloud. Ces contenus numériques pourraient être piratés et distribués illégalement. En restreignant l'utilisation du contenu, la gestion des droits numériques empêche ce type de vulnérabilité. Le système DRM restreint l'accès à ces contenus aux utilisateurs autorisés qui ont une licence.

- **Système de gestion des droits numériques existants**

Une stratégie SIM DRM (CS-DRM) basée sur le cloud pour l'environnement cloud mobile se compose de quatre entités principales : une carte SIM, un agent DRM, un lecteur personnalisé et un navigateur compatible CS DRM (Wang et al., 2010).

Lorsqu'un abonné s'inscrit à un service, la carte SIM est utilisée pour valider son identité, s'authentifier auprès des clients cloud et vérifier la validité de sa licence. L'agent DRM est chargé de faciliter la communication entre les clients cloud ainsi que de mettre en œuvre des règles logiques.

Un lecteur personnalisé est utilisé pour lire du contenu numérique qui ne peut pas être distribué illégalement. Le navigateur CS-DRM est utilisé pour explorer le site Web principal ainsi que pour alerter l'agent DRM de la prochaine étape en fonction d'une réponse ou d'un événement. La préparation, la gestion des droits, l'acquisition des licences, la lecture et le chargement/téléchargement sont les cinq étapes de cette approche. L'étape de préparation commence par l'initialisation du backend, la génération de clés pour le chiffrement symétrique, le transfert de l'ID de contenu vers un serveur sous licence, etc. La phase de gestion des droits personnalise les contenus numériques, tandis que la phase d'acquisition de licence obtient la licence du contenu numérique auprès du serveur de licences. Après avoir obtenu une licence de contenu numérique, l'utilisateur décrypte le contenu afin de le lire. Pendant le processus de téléchargement, il peut changer d'appareil et télécharger la licence sur son nouvel appareil afin de pouvoir profiter du matériel numérique. Le processus de téléchargement est utilisé pour assurer l'intégrité du contenu numérique. La mise en œuvre de la technique CS-DRM montre qu'elle est efficace, sécurisée et faisable.

1.5 Conclusion

Nous avons passé en revue les caractéristiques, l'architecture, les avantages et les applications de MCC dans ce chapitre. MCC est une combinaison de MC et de CC. MCC intègre le CC dans l'environnement mobile, permettant aux utilisateurs d'accéder aux ressources à la demande. MCC permet le développement d'infrastructures simples pour les applications et services mobiles en stockant et en traitant les données en dehors des appareils mobiles et dans le cloud. Cela se traduit par une diminution de la consommation d'énergie de l'appareil mobile. De plus, en utilisant l'internet, les appareils mobiles avec une capacité de stockage et une autonomie de batterie limitées peuvent accéder à une variété d'applications telles que le m-commerce, le m-learning, les soins de santé et le m-gaming. Les principales préoccupations de MCC sont le manque de ressources, la latence, la gestion de la mobilité et spécialement la sécurité. De nombreux systèmes ont déjà été créés pour répondre à ces préoccupations. Cependant, ces problèmes ne peuvent pas être entièrement éliminés. Dans ce chapitre, nous avons discuté des défis actuels de la sécurité particulièrement l'authentification et la confidentialité des données.

Chapitre 2 - Les approches basées sur les modalités biométriques pour l'authentification

2.1 Introduction

La biométrie est dérivée des termes grecs bios et metrikos. La biométrie est le domaine d'étude qui se concentre sur l'identification des personnes en fonction de leurs caractéristiques biologiques ou comportementales (Jain et al., 2011). La biométrie combine la biologie et les technologies de l'information pour identifier l'identité d'une personne en utilisant les caractéristiques physiques ou comportementales du corps humain afin de remplacer ou d'améliorer les méthodes existantes d'identification personnelle.

La biométrie est utilisée à deux fins principales : la vérification de l'identification et la reconnaissance. Lorsqu'une personne revendique une identité, le système doit répondre par une option binaire, l'acceptation ou le rejet. Cependant, l'identification de l'identité nécessitera que le système accède à une base de données préexistante de caractéristiques et trouve celle qui correspond aux caractéristiques de l'individu inconnu. Historiquement, les technologies biométriques ont évolué à partir d'une variété de contextes historiques.

La biométrie est apparue comme une technologie permettant d'améliorer les approches d'identification en vérifiant ou en reconnaissant automatiquement l'identité d'un individu vivant. Par rapport aux identifiants basés sur des jetons et des connaissances, les identifiants biométriques sont difficiles à falsifier, partager, oublier ou perdre, et offrent ainsi une sécurité, une efficacité et un confort d'utilisation accrus. L'introduction de la biométrie simplifie, accélère et améliore l'authentification. De plus, les identifiants biométriques sont plus performants et fiables que les approches d'identification traditionnelles et ont acquis une solide réputation.

2.2 Les systèmes biométriques

Un système biométrique, en général, est un système informatique mis en œuvre à l'aide de méthodes, de techniques et de technologies d'identification biométrique. Les systèmes biométriques peuvent être considérés comme des systèmes de reconnaissance de formes dans lesquels un ensemble de caractéristiques est extrait des données acquises puis comparé à un ensemble de modèles stockés pour déterminer l'identité d'un individu. Il peut être utilisé dans

deux applications : l'authentification et l'identification. Le choix en mode vérification est de savoir si une personne est " qui elle prétend être ? " La décision en mode d'identification est " à qui appartiennent ces données biométriques ? " Ainsi, un système biométrique devient un système de reconnaissance de formes à deux ou plusieurs classes.

En règle générale, un système biométrique se compose de quatre modules clés : l'acquisition de données, l'extraction de caractéristiques, l'appariement et la base de données du système (Tistarelli and Champod, 2017). Le module d'acquisition de données collecte les données biométriques d'un individu via un capteur tel qu'un capteur d'empreinte digitale ou un appareil photo numérique pour le visage. Les données acquises sont analysées dans le module d'extraction de caractéristiques pour extraire un ensemble de caractéristiques discriminantes. Le module d'appariement compare les caractéristiques à l'ensemble de modèles stockés afin de déterminer l'identification d'un individu. Le module de base de données système crée et maintient une base de données pour stocker les modèles biométriques des utilisateurs inscrits. L'extraction et la mise en correspondance de caractéristiques sont deux des défis les plus difficiles de la recherche en reconnaissance biométrique et ont attiré des chercheurs de diverses disciplines, notamment la biométrie, la vision par ordinateur, la reconnaissance de formes, le traitement du signal et les réseaux de neurones.

2.2.1 Le système d'identification par empreinte digitale

Pendant des millénaires, la technique d'identification des empreintes digitales a été utilisée en raison de son caractère unique et distinctif inhérent. En raison de la haute précision de l'identification des doigts, cette technique d'identification personnelle s'avère fiable et infaillible (Maio et al., 2002). Elle est principalement basée sur le motif des crêtes et des vallées à la surface du bout du doigt, qui est déterminé au cours des sept premiers mois de chaque personne. Pendant des décennies, les forces de l'ordre ont utilisé des points cruciaux sur les extrémités des crêtes et les bifurcations pour classer et identifier les individus. Les empreintes digitales sont uniques du fait qu'il n'y en a pas deux qui soient identiques parmi les milliards d'êtres humains, même des jumeaux identiques ou des empreintes sur chaque doigt de la même personne (Maio et al., 2002).

2.2.2 Le système d'identification faciale

La reconnaissance faciale est à l'origine une branche de la vision par ordinateur, et la recherche sur la reconnaissance faciale remonte à l'aube de l'intelligence artificielle et de la vision par

ordinateur. Les images faciales humaines sont idéales pour être utilisées comme attribut biométrique pour l'authentification personnelle, car elles peuvent être recueillies de manière non intrusive, mains libres et continue, ce qui est généralement acceptable pour la majorité des utilisateurs (ZhaoW. et al., 2003). La reconnaissance faciale est un terme général qui fait référence au processus de vérification ou de reconnaissance d'un ou de plusieurs individus à partir d'une base de données d'images et de visages stockée en comparant les traits de différenciation du visage. L'authentification d'une personne à l'aide de son image faciale peut être réalisée de diverses manières, notamment en capturant une image du visage dans le spectre visible avec une caméra peu coûteuse ou en analysant les modèles infrarouges d'émission de chaleur faciale. L'identification ou la vérification du visage est principalement basée sur la structure générale du visage, la distance entre la bouche, le nez, les yeux et les lignes de la mâchoire, puis sur la correspondance de ces traits avec une base de données d'images de visage.

2.2.3 Le système d'identification de l'iris

Alors que les systèmes de reconnaissance utilisent une variété de caractéristiques physiques et comportementales pour identifier les individus, le modèle de biométrie de l'iris a attiré l'attention des chercheurs (Andersen-Hoppe et al., 2017; Climent and Hexsel, 2012; Jain et al., 2011; Matin et al., 2017; Rapaka and Kumar, 2018; Tajouri et al., 2017; Tiwari and Jain, 2015). La reconnaissance de l'iris est un moyen prometteur d'obtenir une identification d'utilisateur automatisée, sécurisée, fiable, rapide et de haute précision qui est généralement précise à 90 % avec des taux d'erreur ne dépassant pas les 10 %. (Daugman, 2016). De plus, c'est un système autonome qui mesure l'iris humain à l'aide d'approches complexes de reconnaissance de formes mathématiques, de traitement d'images et d'apprentissage automatique (Daugman and Downing, 2016). Selon des études, les micro-caractéristiques du modèle d'iris sont restées relativement stables pour la reconnaissance (Shen, n.d.), car l'iris est un organe interne qui est visible de l'extérieur du corps humain et produit un motif unique, qui sert de modèle distinctif parmi différents individus (Bowyer et al., 2008). Néanmoins, la caractéristique unique de l'iris n'est conservée que pendant une période de temps limitée (Poonguzhal and Ezhilarasa, 2015), (Bowyer and Ortiz, 2015) et pour un maximum de six ans (Grother et al., 2013). En effet, la structure du gabarit de l'iris ne dure que huit mois (KRONFELD, 1962).

Il existe de nombreuses micro-caractéristiques distinctes appelées gouttes dans le modèle de l'iris humain, telles que les cryptes, les sillons radiaux, les sillons concentriques, la collerette, les taches de rousseur, la pupille et les taches pigmentaires, qui distinguent les traits réels d'une

personne. Ainsi, les qualités uniques d'une personne la rendent parfaite pour la reconnaissance de l'iris. En effet, les caractéristiques de l'iris révèlent le groupe sanguin d'une personne, qu'elle soit myope ou hypermétrope, son âge et son état de santé.

2.2.4 Le système d'identification d'empreinte de paume

La paume est la partie intérieure de la main humaine, s'étendant du poignet jusqu'au bout de nos doigts, et l'empreinte de la paume est caractérisée par les motifs de peau qui s'y trouvent, composés des propriétés physiques. La reconnaissance d'empreintes palmaires utilise un modèle de crêtes et de vallées similaire à celui de la reconnaissance d'empreintes digitales pour exécuter les propriétés correspondantes. Parce que les paumes humaines couvrent une zone beaucoup plus grande que le doigt, les empreintes palmaires devraient être beaucoup plus distinctives et leur identification beaucoup plus forte et efficace. De plus, des propriétés distinctives supplémentaires des empreintes palmaires, telles que les rides, la texture et les lignes principales, pourraient être proposées comme aides à l'identification. De plus, les caractéristiques ponctuelles telles que les points minuties, les points delta et les points de référence peuvent être utilisées dans les systèmes d'identification d'empreintes palmaires. Initialement, ces systèmes d'identification ont été étudiés pour leur capacité à extraire et à faire correspondre les points solitaires et les minuties à partir d'images d'empreintes palmaires haute résolution. Cependant, un scanner d'empreintes palmaires haute résolution est coûteux et long à utiliser, ce qui limite l'utilisation des systèmes de reconnaissance d'empreintes palmaires en ligne. Par la suite, un dispositif de capture en ligne a été conçu pour collecter des images d'empreintes palmaires basse résolution en temps réel, et l'identification d'empreintes palmaires basse résolution a régulièrement suscité un intérêt considérable dans la communauté biométrique ces dernières années (Xu et al., 2015; Zhang and Lu, 2013; ZhaoW. et al., 2003). De nombreux algorithmes d'identification d'empreintes palmaires à basse résolution ont été développés, la majorité appartenant à l'une des trois catégories suivantes : techniques holistiques, basées sur les caractéristiques ou hybrides. Pour ce faire, de tels systèmes de reconnaissance d'empreinte palmaire intègrent souvent toutes les propriétés de la paume, y compris la géométrie de la main, les caractéristiques des crêtes et des vallées, les lignes principales, la texture, les rides et les caractéristiques des points, afin de créer un système extrêmement précis.

2.3 L'apprentissage automatique

L'apprentissage est le processus d'acquisition de connaissances ou de compétences et est l'une des caractéristiques les plus fondamentales de l'intelligence (Simon, 1983). La capacité d'apprentissage d'un agent – biologique ou artificiel – lui permet d'accomplir une tâche plus efficacement que le reste de la population (Simon, 1983). Depuis la fin des années 1940, lorsque le postulat de Hebb a été introduit, de nombreuses descriptions ont été conçues pour s'adapter à diverses topologies de l'intelligence artificiel (IA) (Judd, 1990). Arthur Samuel a caractérisé l'IA en 1959 comme un "domaine d'étude concerné par le potentiel des ordinateurs à apprendre sans être explicitement programmé" (Samuel, 1959). Bien que le concept soit relativement nouveau, il a suscité un attrait considérable dans la communauté scientifique ces dernières années. La raison fondamentale derrière cela est que les données nécessaires à la formation de l'IA n'étaient pas disponibles jusqu'à récemment.

De nos jours, il y a une croissance significative de la quantité de données disponibles et utilisables. En effet, avec la prolifération des assistants numériques et des ordinateurs parlants, il est facile de croire que la révolution de l'IA a déjà commencé. Lorsque Google a lancé son principal assistant domestique en 2016, le PDG Sundar Pichai a déclaré que l'informatique était en train de passer du monde mobile au monde de l'intelligence artificielle. Des entreprises telles que Google, Tesla et Facebook présentent fréquemment l'IA comme une innovation. Alors que beaucoup à la pointe de la recherche affirment qu'il reste encore beaucoup à faire et que de nombreux obstacles importants doivent être résolus avant que la véritable révolution de l'IA puisse commencer, ce que nous vivons actuellement n'est que l'illusion de l'IA (Kurzweil and Jaroch, 1992; Muganda and Standley, 2009; Nath, 2009). La relation entre les différentes approches d'IA et certains des mots standards utilisés dans ces systèmes, est illustrée à la Figure 2.1.

Comme indiqué précédemment, ML est un sous-ensemble de l'IA qui permet à l'ordinateur de se comporter et de porter des jugements basés sur des données afin d'accomplir une tâche. ML a été fondé au début des années 1990. Elle s'est détournée des approches symboliques héritées de l'IA et s'est tournée vers des méthodologies statistiques et probabilistes (Bishop, 2013; Brown and Sandholm, 2019; Wermter et al., 1996). Lorsqu'ils sont exposés à de nouvelles données, ces algorithmes sont construits de manière à pouvoir apprendre et s'améliorer au fil du temps. Dans ML, une machine conserve les informations et s'améliore avec le temps.

Cependant, contrairement aux humains, il n'est pas sensible à des choses comme la surcharge d'informations de perte de mémoire à court terme et les distractions.

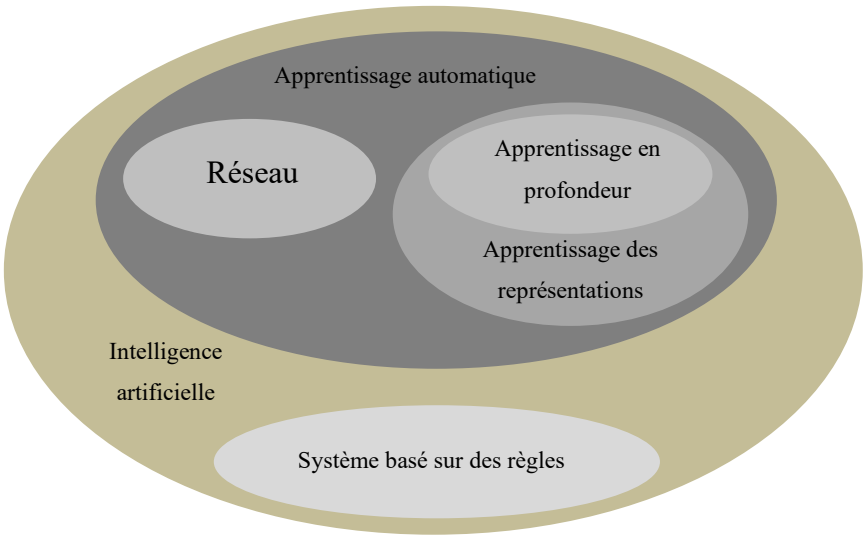

Figure 2.1 Les différents termes couramment utilisés dans l'IA (Roche, 2020).

Envisagez d'identifier si une image représente un chat ou un chien. Lorsque l'on compare l'apparence physique d'un chat et d'un chien, la distinction peut être assez floue. Bien sûr, on pourrait dire que les oreilles d'un chat sont pointues et que les oreilles d'un chien sont souples, mais ce ne sont pas des lois universelles. Il existe de nombreuses classifications basées sur la longueur de la queue, la texture de la fourrure et la couleur.

Dans le cas de la programmation informatique traditionnelle, cela implique un grand nombre de règles fastidieuses qui doivent être écrites manuellement pour aider un ordinateur à faire la distinction entre chat et chien. D'autre part, ML consiste à apprendre à une machine comme à une personne, ce qui, comme tout enfant, nécessite de l'expérience. Avec ML, les programmes analysent des centaines d'échantillons afin de créer un algorithme. Il affine ensuite l'algorithme selon qu'il atteint ou non son objectif. Comme pour le développement cognitif d'un enfant, l'algorithme devient plus sage et plus apte à résoudre les problèmes au fil du temps. C'est ainsi que des machines comme IBM Watson peuvent diagnostiquer le cancer, composer des symphonies classiques.

Avec les réseaux de neurones, certains algorithmes reproduisent la façon dont le cerveau humain est formé. L'apprentissage en profondeur capitalise sur la force des réseaux de neurones profonds. Il modifie simplement les connexions de données de tous les neurones artificiels conformément au modèle de données. Un réseau de neurones profond a une structure similaire

à celle d'un réseau de neurones ; il a une couche d'entrée, une couche de sortie et des couches cachées connectées (Arel et al., 2010; Heaton, 2015). Le travail principal d'un réseau de neurones profonds est de percevoir une entrée avant d'effectuer un calcul complexe. La sortie est une classification et une matrice de solution pour un problème avec différentes catégories.

Bien que l'apprentissage en profondeur soit un choix populaire, ce n'est pas le seul type d'algorithme ML (Nielsen, 2015). De nombreuses variétés existent : régression logistique, machine à vecteurs de support (SVM) et baies naïves. Par exemple, supposons que nous voulions créer un classificateur capable de prévoir si le temps sera agréable ou désagréable, et tout ce que nous avons, ce sont les conditions environnementales, la date, la température et la pression atmosphérique. Un score élevé implique que le temps sera désagréable, tandis qu'un score faible indique qu'il sera agréable. Dans n'importe quelle situation, prévoir le temps en se basant uniquement sur la date ou la température est impossible. L'inclusion d'un paramètre tel que la pression atmosphérique, en plus de la date et de la température, peut donner des résultats plus précis. Dans cette situation, le classificateur donnerait la priorité à la pression atmosphérique plutôt qu'à la date ou à la température.

Ces types de classificateurs sont généralement utilisés lorsque la sortie est classée en au moins deux groupes. Bien que les distinctions entre chaque algorithme d'apprentissage automatique puissent être légères, il est essentiel de les considérer comme des entités distinctes au sein de la même famille. En effet, ils sont optimaux pour une variété d'applications. Semblable à la structure compartimentée et interconnectée du cerveau humain, chaque circuit remplit une fonction distincte.

2.3.1 Paradigmes et méthodes d'apprentissage automatique

Les trois types d'apprentissage automatique les plus populaires sont supervisés, non supervisés et semi-supervisés. Alors que l'apprentissage supervisé est une branche plutôt établie de l'apprentissage automatique, l'apprentissage non supervisé et l'apprentissage semi-supervisé sont toujours considérés comme des nourrissons par certains. Bien que les paradigmes d'apprentissage plus récents gagnent en importance, la majorité des recherches utilisent des approches d'apprentissage automatique supervisé. La Figure 2.2 illustre trois paradigmes d'apprentissage automatique, décrits dans ce chapitre, ainsi que quelques exemples des différentes formes d'apprentissage.

L'apprentissage automatique d'aujourd'hui est différent de l'apprentissage automatique d'autrefois. Né de la reconnaissance des formes et de la conviction que les ordinateurs peuvent apprendre sans être entraînés à exécuter certaines tâches, beaucoup de choses ont changé. De nos jours, les données sont omniprésentes et générées à une vitesse étonnante, soulignant la nature itérative de l'apprentissage automatique. Compléter l'essor de l'apprentissage automatique avec les progrès de la puissance de calcul a entraîné une augmentation massive de la recherche sur la mobilité intelligente. Malgré la publication de nouveaux algorithmes (Arulkumaran et al., 2017; Kiumarsi et al., 2018; Lee, 2017; Liu and Wang, 2018; Mousavi et al., 2016; Schmidhuber, 2015), ces avancées ne parviennent pas à résoudre les défis du monde réel. Cela s'explique en partie par la nature multidimensionnelle de l'environnement de travail. Cela ne veut pas dire que la communauté scientifique n'a pas apporté de contributions significatives.

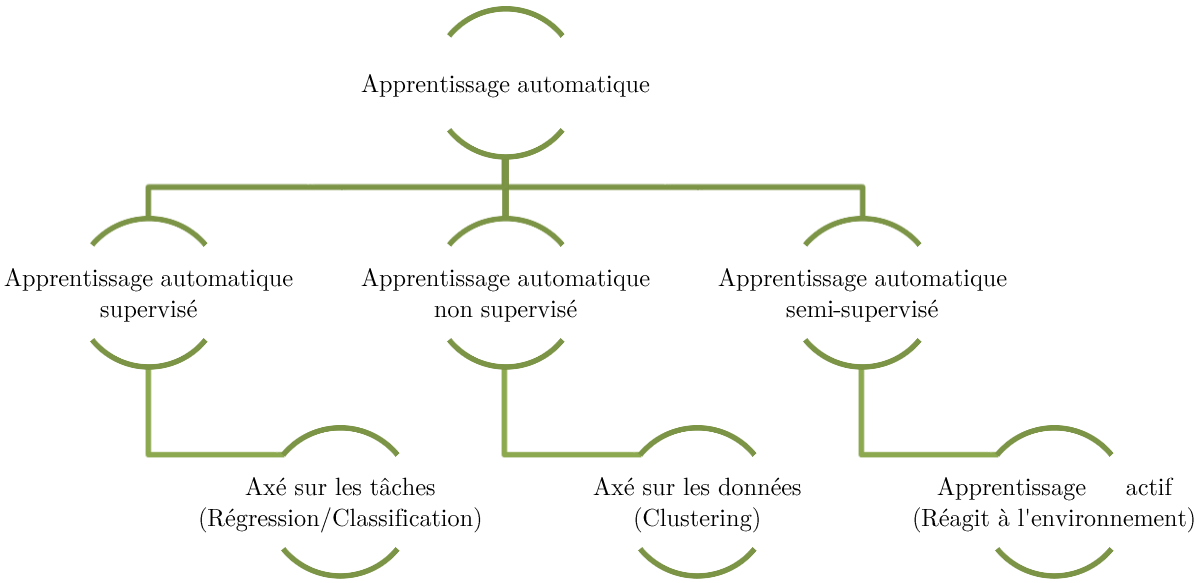

Figure 2.2 Les types d'apprentissage automatique (Roche, 2020).

L'une des discussions les plus fascinantes en matière d'apprentissage automatique concerne la sécurité des véhicules autonomes avant qu'ils ne soient autorisés sur la voie publique (Kalra and Paddock, 2016). D'un côté, d'autres soutiennent que ces voitures doivent être totalement sûres (Hewitt et al., 2019). Ceci est quelque peu surprenant si l'on considère que les gens conduisent des voitures qui sont intrinsèquement dangereuses à n'importe quelle vitesse (Nader,

2011). Une autre école de pensée consiste à les faire connaître et à les laisser s'améliorer avec le temps, ce qui se traduira par des véhicules plus sûrs.

Les techniques de programmation traditionnelles sont incompatibles avec les paramètres qui nécessitent un degré élevé de dimension. Par conséquent, les chercheurs doivent s'appuyer sur une variété de modèles d'apprentissage automatique pour combler l'écart. Même s'ils ne répondront pas à toutes les questions, ils constituent le meilleur instrument disponible compte tenu de la complexité des défis à relever.

a) L'apprentissage supervisé

En 1958, Frank Rosenblatt, un psychologue, a été motivé pour construire un seul neurone artificiel capable d'effectuer des tâches de classification binaire. Sous sa direction, il visait à apprendre à une machine à classer une seule forme (Rosenblatt, 1959). Considéré comme une étude fondamentale dans le domaine de l'apprentissage supervisé, Rosenblatt a construit un mécanisme et l'a connecté à une caméra de 400 pixels ; il a inventé le terme "Perceptron" (Rosenblatt, 1958). Ses études consistaient à présenter la machine avec des images de triangles ou autres. Chaque pixel enverrait un signal électrique distinct au perceptron en fonction de ce qu'il voyait. Si la charge totale était supérieure au seuil, il transmettrait un signal pour activer une lumière, signalant qu'il avait détecté un triangle. Lorsque la charge électrique était insuffisante pour franchir le seuil, la lumière ne s'allumait pas. Rosenblatt a formé la machine sous observation en utilisant les boutons oui et non. Chaque fois que Rosenblatt appuyait sur le bouton non, la machine ajustait la charge fournie à la synapse synaptique du perceptron, modifiant ainsi les niveaux de seuil de la machine. Ce processus a amélioré les chances que la machine réussisse la prochaine fois ; d'où le terme d'apprentissage supervisé.

Comme frontière de décision, le perceptron de Rosenblatt a utilisé une simple fonction d'activation par étapes. Souffrant d'un défaut il n'apprenait que lorsque les choses allaient mal, et il repartait de zéro sans aucune compréhension passée de ce qu'il était censé apprendre. Dans les années 1990, l'apprentissage automatique passe d'une méthode symbolique à une méthode pilotée par les données (Bishop, 2013; Wermter et al., 1996). De nombreux outils ont été développés depuis que les chercheurs ont commencé à développer un algorithme permettant aux ordinateurs d'examiner de grandes quantités de données. Le SVM est l'une de ces avancées. Il a été inventé par Vladimir Vapnik et largement reconnu comme l'une des techniques les plus utiles de l'apprentissage automatique statistique moderne. Le SVM intègre des concepts et des principes d'apprentissage fondamentaux, une conception de problème bien définie et une

théorie mathématique autonome (VAPNIK and V., 1963). Peut-être la meilleure technique d'apprentissage prédictif, elle se compare favorablement à d'autres méthodologies plus empiriques basées sur un raisonnement intuitif, asymptotique et biologique.

L'objectif fondamental de l'apprentissage supervisé est de trouver le modèle reliant les entrées et les sorties lorsque $D = \{(X_i, Y_i)\}_{i=1}^{N}$ et étant donné un ensemble de données *D* de taille *N* contenant des paires entrée-sortie étiquetées (Brownlee, 2016; Victor Roman, 2019). Pour le dire simplement, chaque valeur d'entrée contient un vecteur de dimension d'entiers représentant les données que l'algorithme d'apprentissage automatique doit apprendre. Le vecteur dimensionnel, également appelé vecteur de caractéristiques, représente la compréhension de *X* par l'algorithme pendant l'apprentissage. La sortie, du point de vue de *Y*, peut être n'importe quoi, mais l'hypothèse est qu'elle correspond à une variable catégorielle ou nominale dans l'ensemble de données d'apprentissage.

Lorsque le résultat *Y* est catégorique, on dit que l'algorithme d'apprentissage automatique effectue une tâche de classification ; lorsque *Y* est un nombre réel, on dit que la méthode effectue une régression. Le but fondamental de la classification est de découvrir le modèle reliant les entrées *X* aux sorties *Y*, où $Y \in 1, \ldots, C$ ou *C* est le nombre de classes (Borchani et al., 2015). Lorsque *C* est égal à deux, la tâche de classification est considérée comme un problème de classification binaire ; lorsqu'il dépasse deux, le travail de classification est considéré comme un problème de classification multi-classes. Une classe peut appartenir à deux ou plusieurs groupes dans un problème de classification multi-classes. Sauf indication contraire, lorsque nous utilisons le terme classification, nous entendons un problème de classification multi-classes. Il peut formaliser ce problème en supposant $y = f(x)$ pour une fonction inconnue *f*. Si l'objectif est d'apprendre la fonction à partir d'un ensemble d'apprentissage étiqueté, puis de faire des prédictions, ces dernières peuvent être exprimées en termes de *f* comme $\hat{y} = \hat{f}(x)$ dans cette situation, l'objectif n'est pas simplement d'apprendre les données d'entraînement et de reconnaître le modèle, mais de faire une prédiction sur des données inconnues. Bien que ce terme prête quelque peu à confusion, il fait référence à la généralisation des types de données, et non à la capacité du classifieur à résoudre des problèmes génériques.

b) L'apprentissage semi-supervisé

L'apprentissage automatique semi-supervisé est une technique qui combine l'apprentissage automatique supervisé et non supervisé. L'apprentissage actif en ligne

est une synthèse de l'apprentissage automatique en ligne et actif. Généralement reconnu comme deux paradigmes d'apprentissage automatique indépendants et distincts. Les deux approches ont été combinées pour faciliter la description, telle qu'illustrées à la Figure 2.3, et classées comme un type d'apprentissage automatique semi-supervisé. De nombreux chercheurs étudient déjà ces deux disciplines scientifiques et leurs applications à l'évitement d'obstacles à l'aide d'une caméra monoculaire (Muller et al., 2006), à l'estimation de la profondeur à partir de l'imagerie monoculaire (Michels et al., 2005) et à la classification de l'espace libre à l'aide d'une combinaison de capteurs monoculaires et LiDAR (De Silva et al., 2018). Bien que les techniques traditionnelles d'apprentissage automatique soient bénéfiques pour l'analyse des flux de capteurs, elles nécessitent une quantité importante de données annotées pour s'entraîner. De plus, bien que les algorithmes d'apprentissage automatique typiques fonctionnent bien dans certains domaines, ils ne parviennent souvent pas à se généraliser à de nouveaux contextes (Zhang et al., 2021).

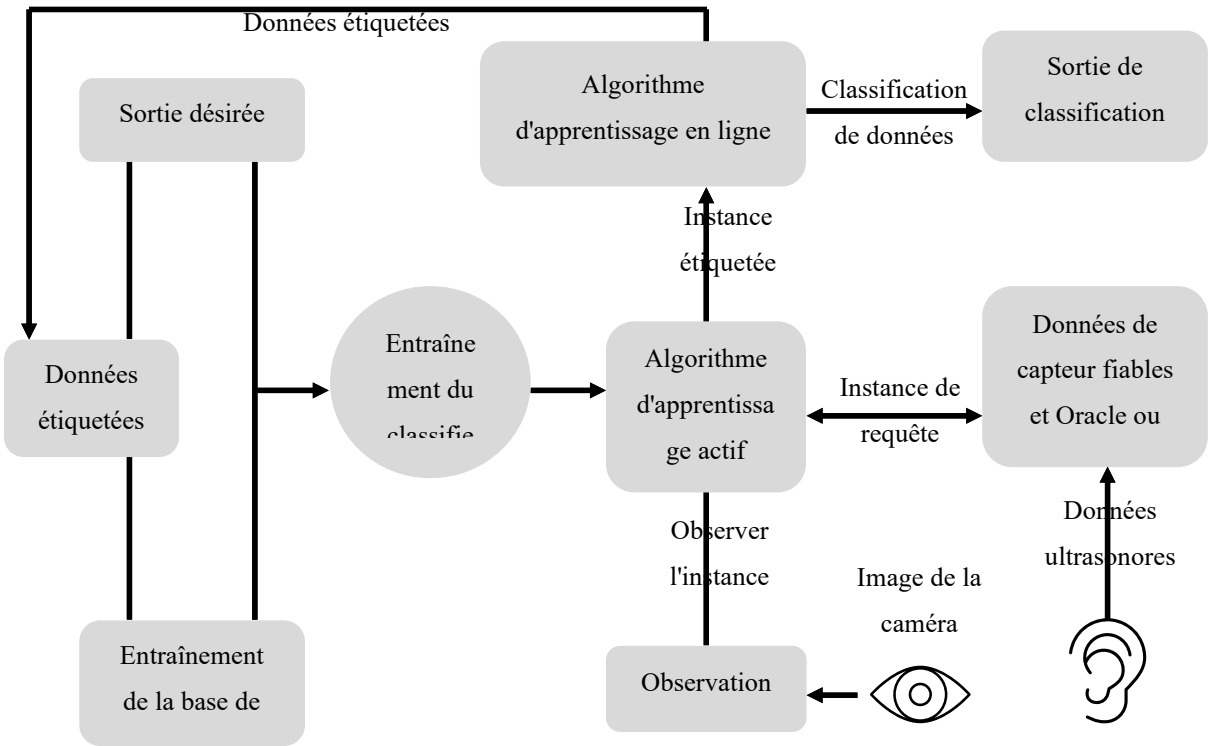

Figure 2.3 Le processus de ML actif en ligne. (Roche, 2020).

Pour relever ces défis, l'apprentissage actif en ligne est utilisé, dans lequel le robot mobile intelligent s'auto-apprend et modifie sa vision de son environnement en réponse à de nouvelles entrées. L'objectif est de tirer parti d'un flux de capteurs robustes pour l'auto-apprentissage et d'améliorer l'incertitude relative des nouvelles données. Pour comprendre l'apprentissage automatique actif en ligne, nous étudions les deux composants indépendamment. Cela nécessite cependant une prise de conscience de deux modes d'apprentissage distincts. L'apprentissage automatique en ligne est un sous-ensemble de l'apprentissage automatique supervisé, c'est une stratégie dans laquelle les données étiquetées nouvellement disponibles sont progressivement introduites dans l'ensemble de données afin de mettre à jour le classificateur à chaque étape (Ghatak, 2017), ce dernier évolue indéfiniment en utilisant cette stratégie, en ajoutant de nouvelles données et en ajustant l'algorithme au fur et à mesure.

L'apprentissage automatique en ligne est utilisé dans les situations où la formation de l'algorithme sur l'ensemble de données complet est difficile. Dans le cas de l'apprentissage en ligne, les informations ne sont pas encore devenues accessibles et, par conséquent, le classificateur ne peut pas être mis à jour tant que les nouvelles données ne sont pas disponibles.

D'autre part, l'apprentissage automatique actif est un sous-ensemble de l'apprentissage automatique semi-supervisé qui se situe entre l'apprentissage automatique supervisé et non supervisé. Traditionnellement, les algorithmes d'apprentissage automatique actifs interrogent l'utilisateur pour l'étiquetage des données nouvellement rencontrée (Kamath and Choppella, n.d.). L'apprentissage automatique actif est particulièrement avantageux dans les cas où les données sont abondantes mais non étiquetées. Il commence généralement par des données étiquetées, puis nécessite l'assistance de l'utilisateur lorsque de nouvelles données non étiquetées deviennent disponibles. Lorsqu'il est intégré à d'autres techniques d'apprentissage automatique, telles que l'apprentissage automatique en ligne, il devient un outil très puissant.

c) L'apprentissage non supervisé

L'apprentissage non supervisé, bien qu'il ne soit pas aussi prolifique que l'apprentissage supervisé, a une histoire tout aussi longue et riche. Il y a l'apprentissage Hebbian, qui a eu une influence durable sur les réseaux de neurones et les paradigmes d'apprentissage automatique (Attneave et al., 1950). Ensuite, il y a les opinions moins évidentes de (Marr, 1970), qui a établi une approche du fonctionnement du cerveau basée sur une compréhension approfondie des vérités fondamentales régissant l'esprit humain. Les recherches de (Marr, 1970) ont établi l'implication critique des cellules de Purkinje dans le cortex cérébelleux dans le générateur de

schémas de base de l'esprit. Le générateur de motifs central est essentiel pour initier la locomotion humaine et est également essentiel pour l'apprentissage non supervisé (Marr, 1970). Son travail a expliqué comment le corps humain établit des modèles pour effectuer des tâches spécifiques et sert de modèle pour l'apprentissage non supervisé.

Une contribution peut-être moins abstraite mais tout aussi significative est venue de Geoffrey Hinton sous la forme de la machine de Boltzmann (Ackley et al., 1985). Cette dernière intègre un certain nombre de notions statistiques qui ont fini par dominer l'estimation de la densité et le regroupement (Ziegel, 2012). Ces machines sont un type de réseau symétrique de neurones dans lequel les neurones prennent des décisions aléatoires pour savoir s'ils doivent être activés ou désactivés. Pour ce faire, ils construisent des vecteurs binaires qui mappent l'entrée sur 0 ou 1.

Récemment, le concept de clustering a gagné du terrain, c'est une technique qui divise les données en groupes en fonction de certains critères, traduisant les points de données dans un espace de caractéristiques de dimension supérieure (Victor Roman, 2019). En établissant des frontières entre les différents groupes - similaires à un SVM - nous pouvons créer une division entre les caractéristiques de dimensionnalité supérieure et les organiser de manière utile. Le clustering K-means est un autre type d'apprentissage automatique non supervisé et une technique de quantification vectorielle largement utilisée dans l'exploration de données. La procédure est conçue pour diviser *n* observations en clusters en affectant chaque observation à un cluster avec la moyenne la plus proche. Il commence cependant à être supplanté avec l'apparition de l'apprentissage en profondeur.

L'apprentissage non supervisé est un problème beaucoup moins organisé que l'apprentissage supervisé et donc plus sujet aux erreurs. Les avantages d'un tel système sont que toutes les données ne doivent pas être étiquetées, et il ressemble donc étroitement à la façon dont les humains acquièrent des capacités importantes. Ce type d'apprentissage a pris de l'importance en tant que technique permettant de découvrir des modèles de données jusque-là inconnus. Appelé aussi apprentissage auto-organisé, son rôle majeur est de catégoriser ses sorties en modélisant les densités de probabilité des entrées fournies (Hinton and Sejnowski, 1999; Tucker, 2004). Contrairement à l'apprentissage supervisé, qui utilise une distribution de probabilité conditionnelle pour déduire, il est utilisé pour dériver une distribution de probabilité a priori uniquement par un raisonnement déductif.

2.4 Les réseaux de neurones artificiels (ANN)

Les ANN, ou réseaux de neurones, sont un sous-ensemble d'algorithmes d'apprentissage automatique supervisé qui effectuent des problèmes de classification en déduisant des modèles à partir d'instances précédemment étiquetées. En général, les ordinateurs effectuent des calculs répétitifs et des instructions spécifiques mais ont du mal à reconnaître les formes (Kothari and Oh, 1993; Pavlus, 2016). Ce défi est relevé par les réseaux de neurones, qui décomposent des modèles complexes en une séquence de modèles plus simples (Nielsen, 2015). Par exemple, lorsqu'une machine doit déterminer si une image contient un objet spécifique, un réseau de neurones utilise les bords pour reconnaître les différents attributs de la classe. Le réseau ne peut pas estimer l'identité de l'objet tant que toutes les caractéristiques ne sont pas combinées pour reconstruire la classe cible (Arel et al., 2010; Heaton, 2015). Dans sa forme la plus simple, un ANN est un type de modèle informatique utilisé pour résoudre des problèmes en reconnaissant des modèles dans un ensemble de données particulier. Il existe de nombreuses formes de réseaux de neurones artificiels.

2.4.1 Les réseaux de neurones feedforward

Le type le plus simple d'ANN est le réseau de neurones Feedforward (Rosenblatt, 1958), (Bishop, 2013). Dans ces réseaux de neurones, les données voyagent dans une seule direction du début à la fin. Un réseau de neurones FeedForward a une architecture relativement simple, comme le montre la Figure 2.4 ; il se compose d'une couche d'entrée, d'une couche de sortie et d'une ou plusieurs couches cachées (Arel et al., 2010; Heaton, 2015). Chaque connexion, semblable à la synapse d'un neurone biologique, transfère des informations aux neurones précédents -propagation FeedForward- avant de générer un score (Liu et al., 2011). Lorsqu'un réseau de neurones Feed-Forward est mis en œuvre, le signal d'entrée est un nombre réel représentant les données de classification (Iliadis et al., 2013).

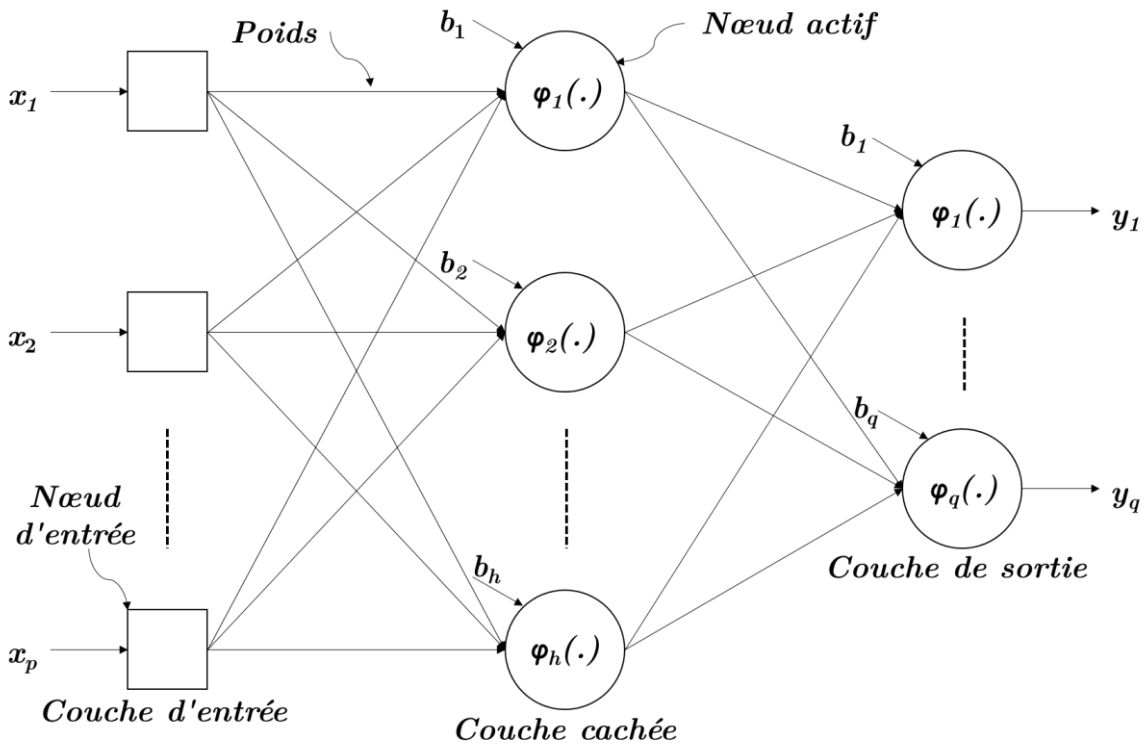

Figure 2.4 Réseau de neurones feedforward (Ojha et al., 2017).

Le réseau de neurones Feedforward a été développé pour remédier à l'inexactitude du perceptron de Frank Rosenblatt (Nielsen, 2015). Généralement utilisé dans les paradigmes d'apprentissage automatique supervisé où les données apprises ne sont pas séquentielles ou dépendantes du temps, Ces réseaux ont démontré que lorsqu'ils sont confrontés à des tâches multi-classes complexes, un réseau multicouche de perceptrons surpasse un seul perceptron (Nielsen, 2015). Les principaux inconvénients des réseaux de neurones Feedforward sont leur vulnérabilité au bruit, ce qui les rend sujets à une mauvaise classification. Généralement, lors de l'analyse de situations simples, des technologies de classification fondamentales telles que les perceptrons suffisent ; Cependant, au fur et à mesure que la tâche devient plus sophistiquée, les réseaux de neurones commencent à surpasser les moteurs de classification classiques.

Alors que l'objectif initial de l'IA était d'imiter le cerveau humain dans son intégralité, l'accent a été mis sur l'exécution de tâches spécifiques en utilisant les réseaux de neurones au fil du temps. Certains considèrent cela comme un écart par rapport aux objectifs fondamentaux de l'intelligence artificielle. D'autres, comme ceux qui voient le cerveau de manière compartimentée, pensent que certaines parties remplissent des fonctions spécifiques et que, par conséquent, certains réseaux sont bien adaptés à des tâches spécifiques.

2.4.2 Backpropagation

La Backpropagation est le mécanisme qui minimise les pertes. Ceci est accompli en ajustant progressivement les poids et les biais tout au long du processus de formation. Il a un effet sur l'algorithme de descente de gradient jusqu'à ce que la perte minimale tolérable soit obtenue (Iliadis et al., 2013). Il facilite ces ajustements et permet à un réseau d'apprendre son périmètre en voyant l'effet de minuscules changements de poids et de valeurs de biais sur la sortie. Lorsqu'un changement mineur dans l'entrée entraîne un petit changement dans la sortie, seul un petit changement s'est produit dans le réseau. Les réseaux qui ne font que peu de changements n'ont jamais la possibilité d'apprendre et ne subiront jamais les modifications massives du réseau, nécessaires à la prise de décision autonome ("CUDA Spotlight: GPU-Accelerated Deep Neural Networks | NVIDIA Developer Blog," 2014). De plus, le gradient de sortie du réseau concernant les paramètres dans les premières couches devient extrêmement faible ; d'où le terme de problème de la disparition du gradient ("What is the vanishing gradient problem? - Quora," 2015).

Le problème de la disparition du gradient est principalement déterminé par la façon dont la fonction d'activation transmet de manière non linéaire les entrées dans une petite plage de sortie ("What is the vanishing gradient problem? - Quora," 2015). Par exemple, les fonctions sigmoïdes transfèrent des valeurs réelles dans la plage de 0 à 1, ce qui entraîne le transfert de vastes zones de l'entrée dans une petite plage. Même un petit changement dans l'entrée entraîne une grande différence dans la sortie. Par exemple, la première couche d'un réseau profond transfère une grande partie d'une image vers une petite région de sortie, qui est ensuite transférée vers la couche suivante jusqu'à ce qu'elle atteigne la sortie. En conséquence, un petit changement dans la production se produit malgré un changement substantiel dans l'entrée. Les non-linéarités s'accumulent, aggravant le problème et réduisant le gradient (Graves, 2012; "What is the vanishing gradient problem? - Quora," 2015).

Des travaux révolutionnaires sur le problème de disparition du gradient ont été publiés en 2006 par Hinton, Osindero et Yee-Whye Teh (Heaton, 2015), (Graves, 2012). Pour le dire autrement, considérons la pente comme une colline et l'entraînement comme une roue descendant cette colline jusqu'à la destination souhaitée, lorsque la pente est raide, la roue se déplace rapidement, mais lorsqu'elle est à plat, elle ralentit. C'est la même chose avec un réseau profond, où il y a une courbe d'apprentissage abrupte et une croissance modeste dans les premières phases du

réseau. Cependant, le réseau s'accélère vers la fin, lorsque la courbe d'apprentissage est plus raide (Graves, 2012).

Les couches au début d'un réseau d'images cèdent la place à une singularité. Si les niveaux initiaux du réseau interprètent mal les choses, les couches suivantes le feront aussi. Lorsqu'un réseau souhaite apprendre, il examine d'abord les erreurs afin de déterminer quels poids et biais affectent la sortie, avant de tenter de réduire l'erreur en ajustant les poids (Hinton et al., 2006). C'est ce qu'on appelle la Backpropagation, et il est utilisé pour entraîner les réseaux. Il résout le problème de la disparition du gradient (Hinton et al., 2006).

La mise à jour des poids se fait comme illustre l'Équation 2.1:

$$* w_x = w_x - a(\frac{\delta \ Error}{\delta \ w_x})$$

Équation 2.1

2.4.3 Les réseaux de neurones convolutifs

Les réseaux de neurones convolutifs (CNN :Convolutional Neural Network) sont une sous-classe des réseaux de neurones qui sont souvent utilisés pour classer les images. Bien qu'il soit possible d'utiliser divers algorithmes d'apprentissage automatique tels que le SVM (Nielsen, 2015), (Anthony et al., 2007), les CNN se sont révélés être un outil très utile dans ce processus (He et al., 2016). La représentation des données est l'un des enjeux clés associés aux travaux de classification d'images. Dans le sens le plus simple, les images numériques sont une collection de pixels disposés dans un ordre spécifié et auxquels une couleur spécifique est attribuée.

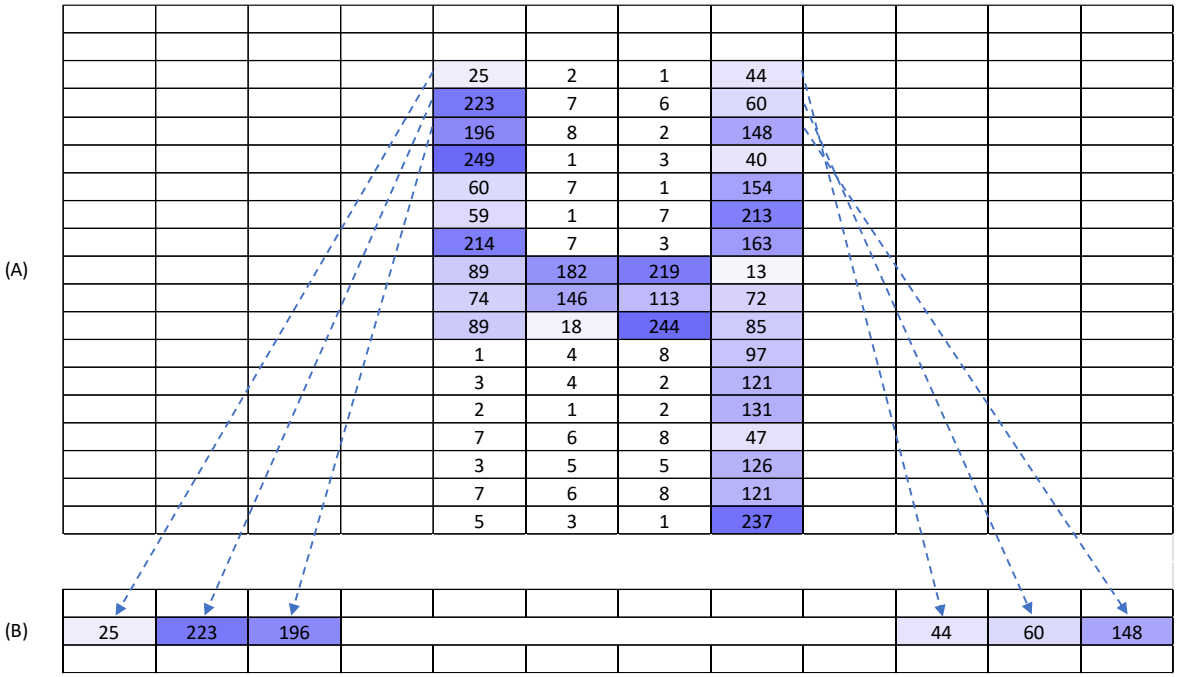

Figure 2.5 (a) La couche bleu de l'image en couleurs vraies du chiffre quatre. (b) Aplatissement de la couche dans un seul tableau alignant une colonne après l'autre (Roche, 2020).

Les images en couleurs vraies, par exemple, sont formées d'une matrice m-par-n-par-3. Chaque couche de la matrice correspond à une composante de couleur distincte, telle que le bleu, le vert ou le bleu. Si la position de l'élément bleu, vert ou bleu est modifiée, l'image est également modifiée. En revanche, si l'une des couches bleu, verte ou bleue est supprimée du tableau, l'image est conservée mais dans une seule couleur.

Considérez le numéro quatre dans toute sa splendeur glorieuse de couleurs réelles. Si nous séparons la couche bleu.

Des autres, nous retenons le nombre quatre, mais dans la couleur bleu uniquement - comme illustré à la Figure 2.5 (a). Si nous devions analyser cette image à l'aide d'un ANN, nous aurions besoin de l'aplatir dans un vecteur de colonne (Planche et al., 2019) et d'aligner les données une colonne après l'autre - comme illustré à la Figure 2.5 (b). Si les données sont traitées comme un vecteur colonne et que la taille ou la résolution de l'image est inconnue, le réseau de neurones aura du mal à comprendre la représentation - il perdra la trace de la disposition spatiale des pixels individuels qui composent l'image.

	25	2	1	44					25.6	2.3	14.2	
	223	7	6	60					225.1	8.8	24	
	196	8	2	148					198.4	8.6	46.4	
	249	1	3	40					249.3	1.9	15	
	60	7	1	154					62.1	7.3	47.2	
	59	1	7	213	Facteur de sous-échantillonnage				59.3	3.1	70.9	
	214	7	3	163		1	0.3		216.1	7.9	51.9	
	89	182	219	13					143.6	247.7	222.9	
	74	146	113	72					117.8	179.9	134.6	
	89	18	244	85					94.4	91.2	269.5	
	1	4	8	97					2.2	6.4	37.1	
	3	4	2	121					4.2	4.6	38.3	
	2	1	2	131					2.3	1.6	41.3	
	7	6	8	47					8.8	8.4	22.1	
	3	5	5	126					4.5	6.5	42.8	
	7	6	8	121					8.8	8.4	44.3	
	5	3	1	237					5.9	3.3	72.1	

(A) (B)

Figure 2.6 (a) Les données originales de l'image du chiffre quatre. (b) Les dimensions horizontales réduites des données d'image (Roche, 2020).

CNN traite ce problème en utilisant un certain nombre de filtres de sous-échantillonnage et de mise en commun. Lorsqu'ils transforment l'image en représentation, ils préservent la relation entre les points de données. Si nous extrayons les caractéristiques de l'image originale tout en préservant l'arrangement spatial (Kakaletsis et al., 2019), la procédure de classification devient plus facile. Les Figure 2.6 (a) et (b) illustrent ce processus, dans lequel le facteur de sous-échantillonnage affecte les données d'origine. Une fois exploitées, les données compriment la taille de l'image tout en gardant son organisation spatiale.

Il convient de noter que le facteur de sous-échantillonnage utilisé dans la Figure 2.6 n'affecte que les dimensions horizontales des données. De plus, le facteur de sous-échantillonnage n'affecte qu'une seule fois les points de données les plus à gauche et les plus à droite. Par conséquent, les données situées sur les bords droit et gauche de l'image sont moins influencées que les données proches du centre de l'image.

En réduisant la dimension de l'image, on peut conserver le lien entre les données de l'image et la représentation apprise par le réseau. À l'occasion, on peut augmenter les dimensions de l'image plutôt que de les diminuer. Lorsque nous ne souhaitons pas diminuer la dimensionnalité de l'image, nous la remplissons de zéros, minimisant ainsi l'impact sur les points de données périphériques (Hemanth and Estrela, 2017). Alternativement, lorsque nous voulons réduire la dimensionnalité de l'image et l'effet du facteur de sous-échantillonnage sur les points de données périphériques, nous capturons plusieurs poids en un seul tour et fusionnons les deux images (Hemanth and Estrela, 2017). Les données d'image de la Figure 2.7 (a) et (b) ont été

modifiées respectivement par les valeurs de poids (1 0.3) et (0.5 1. Dans les deux situations, la dimensionnalité des données d'image a été réduite de 17 par 4 à 17 par 3. Lorsque les Figure 2.7 (a) et (b), sont combinées, une image dimensionnelle réduite est créée qui conserve plus d'informations sur l'image d'origine qu'une simple représentation vectorielle de colonne.

	25.6	2.3	14.2					22.5	6	220.5	
	225.1	8.8	24					146.5	33.5	303	
	198.4	8.6	46.4					138	14	741	
	249.3	1.9	15					129.5	15.5	201.5	
	62.1	7.3	47.2					65	8.5	770.5	
	59.3	3.1	70.9					34.5	35.5	1068.5	
	216.1	7.9	51.9					142	18.5	816.5	
	143.6	247.7	222.9					954.5	1186	174.5	
	117.8	179.9	134.6					767	638	416.5	
	94.4	91.2	269.5					134.5	1229	547	
	2.2	6.4	37.1					20.5	42	489	
	4.2	4.6	38.3					21.5	12	606	
	2.3	1.6	41.3					6	10.5	656	
	8.8	8.4	22.1					33.5	43	239	
	4.5	6.5	42.8					26.5	27.5	632.5	
	8.8	8.4	44.3					33.5	43	609	
	5.9	3.3	72.1					17.5	6.5	1185.5	

(A) (B)

Figure 2.7 (a) & (b) Affichent les données d'image après le traitement par le facteur de sous-échantillonnage (Roche, 2020).

L'utilisation d'un facteur d'échantillonnage inférieur de deux pixels horizontaux consécutifs jusqu'à présent. Dans la plupart des cas, il est nécessaire de maintenir la disposition spatiale des caractéristiques horizontales et verticales de l'image (Hemanth and Estrela, 2017). Deux rangées de deux pixels horizontaux consécutifs ou une matrice 2 par 2 ont été utilisées pour accomplir cela. Il convient de noter que la même diminution de dimension qui se produit sur le plan horizontal se produit également sur le plan vertical, abaissant davantage la taille à une matrice de 16 par 3 - comme illustré dans la Figure 2.8 (a) et (b).

Cette procédure d'extraction des caractéristiques d'une image tout en conservant les relations spatiales horizontales et verticales est essentielle pour que le réseau comprenne la disposition des pixels. Dans sa forme la plus élémentaire, un CNN est un paradigme d'apprentissage en profondeur qui peut prendre un lot d'images, appliquer un facteur de sous-échantillonnage à divers composants de l'image, puis regrouper au maximum les données d'image échantillonnées avant de les faire passer par le système neuronal entièrement connecté au réseau pour effectuer la classification (LeCun et al., 1998). L'utilisation de cette méthode, un CNN apprend à catégoriser une image à partir de données précédemment étiquetées pendant la formation

(Weiss et al., 2018). À l'instar du concept de plasticité neuronale de Hebb, lorsque la sortie anticipée ne correspond pas à la sortie connue pour être correcte, les poids changent pendant l'entraînement. La différence - souvent appelée perte - diminue au fur et à mesure que le réseau mûrit via la rétropropagation (Nielsen, 2015). Tout au long de ce processus, le réseau se familiarise avec les entités jusqu'à ce que les prédictions correspondent étroitement aux entrées connues pour être correctes. Alors que les pondérations du réseau sont optimisées lors de la formation, les couches de sous-échantillonnage et de regroupement maximal (Max-pooling) sont sélectionnées en fonction des données et du processus pour lequel le réseau est destiné.

	25	2	1	44					172.1	36.8	317.2	
	223	7	6	60					363.1	22.8	765	
	196	8	2	148					327.9	24.1	247.9	
	249	1	3	40					314.3	10.4	785.5	
	60	7	1	154					96.6	42.8	1115.7	
	59	1	7	213	Facteur de sous-échantillonnage				201.3	21.6	887.4	
	214	7	3	163		1	0.3		1170.6	1193.9	226.4	
	89	182	219	13		0.5	5		910.6	885.7	639.4	
	74	146	113	72					252.3	1408.9	681.6	
	89	18	244	85					114.9	133.2	758.5	
	1	4	8	97					23.7	18.4	643.1	
	3	4	2	121					10.2	15.1	694.3	
	2	1	2	131					35.8	44.6	280.3	
	7	6	8	47					35.3	35.9	654.6	
	3	5	5	126					38	49.5	651.8	
	7	6	8	121					26.3	15.9	1229.8	
	5	3	1	237								

(A) (B)

Figure 2.8 (a) L'image originale du chiffre quatre. (b) L'image avec le facteur de sous-échantillonnage horizontale et verticale (Roche, 2020).

L'architecture d'un CNN peut être généralisée comme le montre la Figure 2.9(LeCun et al., 1998). Le CNN est composé de trois composants principaux illustrés à la Figure 2.9 : les couches convolutives, les couches de Pooling et la couche de sortie (Chih-Ching et al., 2019). Bien sûr, des agencements alternatifs des éléments et certains réseaux utilisent une modification des couches existantes, mais pour la plupart, ils peuvent être représentés de cette manière. Les couches de convolution fonctionnent de la manière décrite ci-dessus. De toute évidence, les tailles de l'image et de la matrice de sous-échantillonnage sont définies, cette dernière définissant la manière dont les caractéristiques spécifiques des données sont extraites.

Entre les couches de convolution, une couche de pooling est introduite occasionnellement. Le pooling est utilisé pour consolider et minimiser la taille de la couche qui la précède. Effectué sur chaque couche de l'image, il permet de conserver les couches de données tout en réduisant la taille de l'image par échantillonnage. La technique de pooling la plus souvent utilisée est le

Max Pooling (Romanuke, 2017). En outre, la couche d'Average Pooling, la couche de pooling GlobalMax et la couche d'Average Globale sont souvent utilisées comme couches de Pooling.

Max pooling est une technique de discrétisation basée sur la valeur maximale à l'intérieur d'une certaine fenêtre. Average pooling fait la même chose en utilisant la moyenne dans une fenêtre spécifiée. Au cours des couches de pooling GlobalMax et Global Average, un processus similaire se produit. Dans chaque scénario, l'objectif est de sous-échantillonner une représentation d'entrée afin de réduire la taille de l'image. Intrinsèquement, la procédure fera des hypothèses sur les caractéristiques de la fenêtre (Scherer et al., 2010).

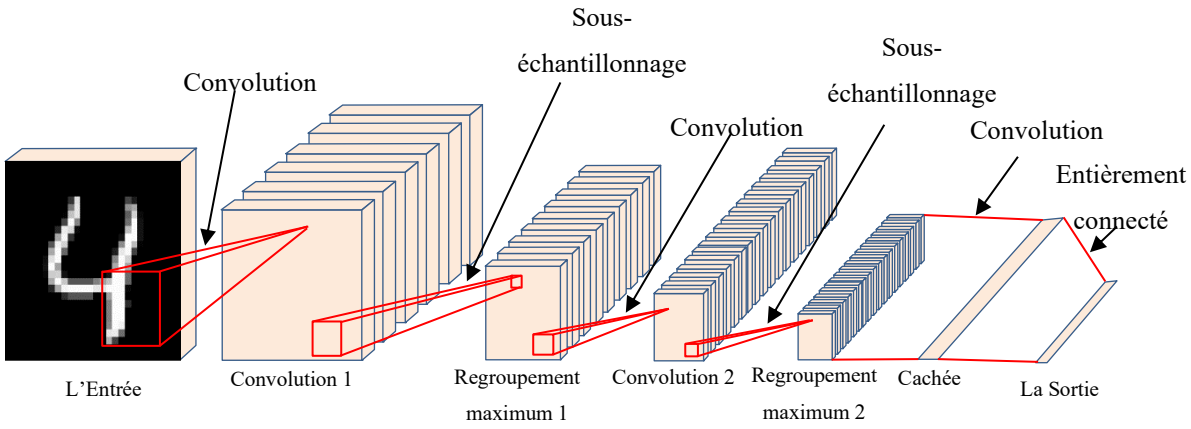

Figure 2.9 L'architecture général du Réseau de Neurones Convolutifs (Roche, 2020).

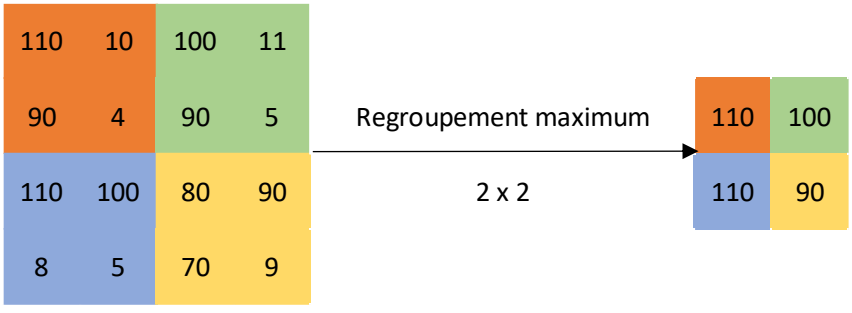

Figure 2.10 Le processus de Max-pooling (Roche, 2020).

Considérons un échantillon de quatre pixels sur quatre données extraites d'une représentation d'image. Nous pouvons extraire certaines caractéristiques requises en passant un filtre 2 par 2 sur les données d'entrée par étapes incrémentielles de 2 pixels par stride sans chevauchement. Dans le cas de la couche Max pooling, la région de traversée de la fenêtre récupère la valeur

maximale de la matrice de sortie. La matrice de sortie qui en résulte comprend la valeur maximale pour chaque fenêtre dans une région. La Figure 2.10 illustre cette approche.

La couche de sortie est la dernière couche du CNN généralisé. Cela se produit après que la représentation de l'image ait subi de nombreuses couches de convolution, de remplissage de données et de sous-échantillonnage. La couche de sortie est l'endroit où les différentes classes du réseau sont formées. Nous avons besoin de la couche de sortie car la convolution ne peut pas générer une classe et les couches de pooling sont incapables de le faire.

L'utilisation d'un réseau de neurones entièrement connecté pour fournir une sortie égale au nombre de classes. Le réseau calcule l'erreur de classification dans la couche de sortie en utilisant une fonction d'activation telle que l'unité linéaire de redressement (ReLU) et une fonction de perte telle que l'entropie croisée catégorielle. L'utilisation de la propagation directe et la rétropropagation, la couche entièrement connectée apprend les caractéristiques de représentation transmises par les couches convolutives, exactement comme le fait un réseau de neurones.

2.4.4 Les composants essentiels d'un réseau de neurone

a) Les fonctions d'activation

Une fonction d'activation est la fonction qui agit sur les entrées d'un ANN. Elle est également connue sous le nom de fonction de transfert et se présente sous diverses formes. Parce que les fonctions d'activation des neurones sont les mêmes pour chaque élément du réseau, le score est influencé par les poids et les biais.

En 1943 (McCulloch and Pitts, 1943), McCulloch et Pitts ont établi l'architecture fondamentale des réseaux de neurones modernes. Un réseau de neurones diffère d'un perceptron en ce qu'il comporte trois éléments de base : un élément de traitement de l'information, l'organisation des connexions (entièrement connectées ou connectées par convolution) et les procédures d'entraînement utilisées pour mettre à jour les poids et le biais (fonction de perte).

McCulloch et Pitts suggèrent un neurone biologique qui traite les entrées en utilisant une fonction d'intégration connectée à l'entrée d'un neurone. D'autre part, les réseaux de neurones modernes utilisent une variété de fonctions d'activation non linéaires. Il convient de noter que si nous appliquons une fonction d'activation linéaire, le résultat sera le même qu'un réseau à

une seule couche. En conséquence, les fonctions d'activation sont généralement invariablement non linéaires, comme le montrent les figures ci-dessous.

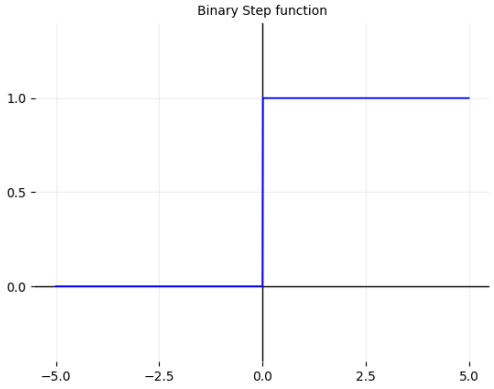

Figure 2.11 Binary Step.

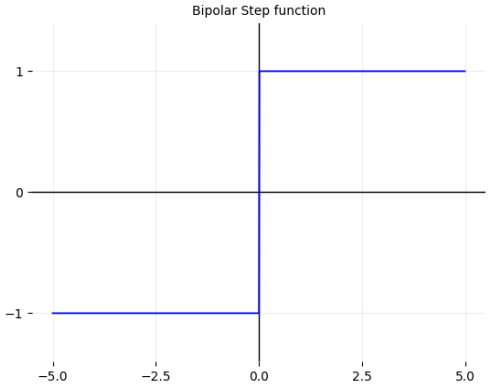

Figure 2.12 Bipolar.

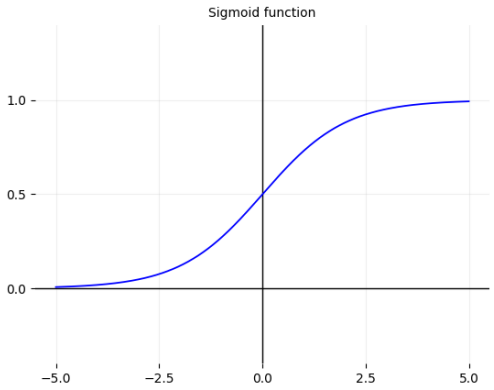

Figure 2.13 Sigmoid.

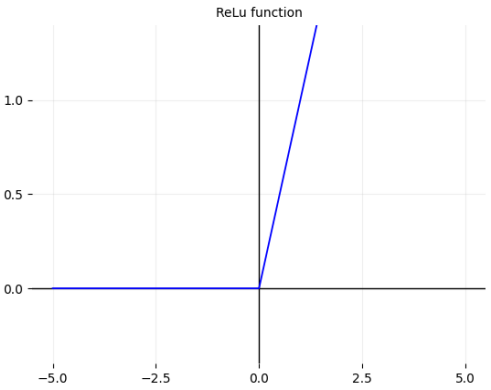

Figure 2.14 ReLu.

La fonction d'activation Binary Step (Berg, 1929) est couramment utilisée dans les réseaux à une seule couche pour convertir l'entrée en sortie sous forme binaire (1 ou 0) - comme illustré à la Figure 2.11 et défini comme (Sivanandam et al., 2006) :

$$f(x) = \begin{cases} 1 \; if \; x \geq 0 \\ 0 \; if \; x < 0 \end{cases}$$

Équation 2.2

La fonction Bipolar Step (Berg, 1929) illustrée à la Figure 2.12 est largement utilisée dans un réseau à une seule couche pour transformer l'entrée en une sortie +1 ou -1 définie comme (Gonzalez et al., 2009) :

$$f(x) = \begin{cases} 1 \; if \; x \geq 0 \\ -1 \; if \; x < 0 \end{cases}$$

Équation 2.3

La fonction Sigmoid (Wilson and Cowan, 1972), illustrée à la Figure 2.13, concerne la relation entre la valeur de la fonction et sa valeur dérivée. Cela a réduit les exigences de calcul du réseau. La fonction Sigmoid, qui est souvent employée dans les réseaux de rétropropagation, est classée en deux types : les fonctions Binary Sigmoid et Bipolar.

Le Binary Sigmoid - également connu sous le nom de fonction Unipolar Sigmoid - est une fonction qui prend un paramètre de pente et renvoie des valeurs comprises entre 0 et 1. Le Bipolar Sigmoid a le même paramètre de pente que le Sigmoid mais affiche des valeurs comprises entre -1 et 1. Le Binary et le Bipolar Sigmoid sont caractérisés comme suit (Gonzalez et al., 2009) :

$$sig(x) = \frac{1}{1 + e^{-\beta x}}$$

Équation 2.4

$$sig(x) = \frac{1 + 2}{1 + e^{-\beta x}}$$

Équation 2.5

La popularité de la fonction d'activation ReLU a augmenté grâce à l'apprentissage en profondeur et aux CNN (Hahnloser et al., 2000). ReLU est souvent un premier choix efficace pour traiter des images ou mener des recherches dans le domaine de la vision par ordinateur (LeCun et al., 2015). La caractéristique distinctive de ReLU est qu'il a une identité linéaire pour toutes les valeurs positives et une valeur nulle pour toutes les valeurs négatives.

Ces caractéristiques signifient que ReLU est économe en ressources ; il faut moins de temps pour s'entraîner et exécuter; il converge plus rapidement, garantissant que la pente ne plafonne pas à mesure que les entrées deviennent importantes ; et – peut-être le plus important – il ne souffre pas du problème de la disparition du gradient que certains de ses concurrents connaissent (Iliadis et al., 2013). Le problème de la disparition de gradient est une faiblesse importante des réseaux de neurones Feedforward. Jusqu'a 2016, lorsque les chercheurs ont introduit ResNet, la majeure partie des approches du problème de la Disparition du Gradient était basée sur le matériel (He et al., 2016). Avant ResNet, lors de l'entrainement d'un réseau, le gradient d'erreur diminuait plus rapidement au début. À la fin de l'entrainement, le réseau est incapable de propager les informations pertinentes à partir de la sortie et le taux d'erreur ralentit considérablement. ReLU surmonte ce problème en raison de son comportement unique lorsqu'il s'agit d'entrées négatives - il ne se déclenche que pour les entrées positives. La fonction d'activation de ReLU illustrée à la Figure 2.14 est la suivante (Patterson and Gibson, 2017) :

$$f(x) = max(x, 0)$$

Équation 2.6

Contrairement à l'activité nerveuse biologique que l'ANN est censée imiter, presque toutes les fonctions d'activation sont toujours activées. En revanche, l'activité neuronale est rare et les différents circuits neuronaux du cerveau humain sont actifs à des périodes variables. Par exemple, le lobe occipital du cortex cérébral est principalement responsable de la vision. Le lobe pariétal (Tortora and Evans, 1986) est situé à côté du lobe occipital et est principalement responsable de la compréhension des relations spatiales entre les éléments. Bien que les deux fonctions se déclenchent fréquemment ensemble, il y a des occasions où elles se déclenchent séparément.

Lorsqu'il s'agit d'entrées négatives égales à zéro, la fonction ReLU imite cette procédure. Ainsi, lorsque ReLU se déclenche, il est plus probable que le neurone artificiel traite des informations pertinentes sur le problème plutôt que des données non pertinentes. Les effets de sphéricité ne complètent pas toujours ReLU et peuvent parfois aller à l'encontre de son utilisation. Étant donné que la pente de ReLU équivaut à des plages négatives à zéro, il est peu probable qu'un neurone se rétablisse après avoir atteint zéro. Bien que ces neurones ne compensent pas toujours la difficulté de discerner l'entrée, avec le temps, les zéros s'accumulent. Enfin, nous découvrons qu'une partie importante du réseau est inactive. Cet effet, communément appelé dying, se

produit généralement lorsque le taux d'apprentissage est trop élevé ou qu'il existe un biais négatif important (Géron, 2017); cependant, un taux d'apprentissage plus faible atténue souvent le problème.

b) Les fonctions de perte

L'impact le plus important sur les performances du réseau de neurones est probablement la fonction de perte. L'objectif principal de la fonction de perte est de quantifier la performance du réseau par rapport aux classes cibles et prédites (Zafar et al., 2018). La différence entre les deux est grande au début de la formation. Dans des circonstances idéales, la perte diminuera progressivement jusqu'à zéro. Alors que le taux de variation de la perte dépend des pondérations et du biais, la fonction réelle génère un scalaire qui décrit les performances globales du réseau. Ce n'est ni un vecteur ni un scalaire. La fonction de perte, dans sa version la plus simple, optimise les paramètres d'un réseau de neurones en minimisant la perte.

En pratique, nous calculons la perte en comparant la valeur de classe cible à la valeur de classe prédite du réseau (une probabilité). Ensuite, en utilisant la descente de gradient, les poids et les biais sont ajustés pour minimiser la perte. De nombreuses fonctions de perte sont accessibles, basées sur les objectifs du réseau et la fonction d'activation. Elles sont classées en trois catégories dans la Figure 2.15 : fonctions de perte de régression, fonctions de perte de classification binaire et fonctions de perte de classification multi-classes.

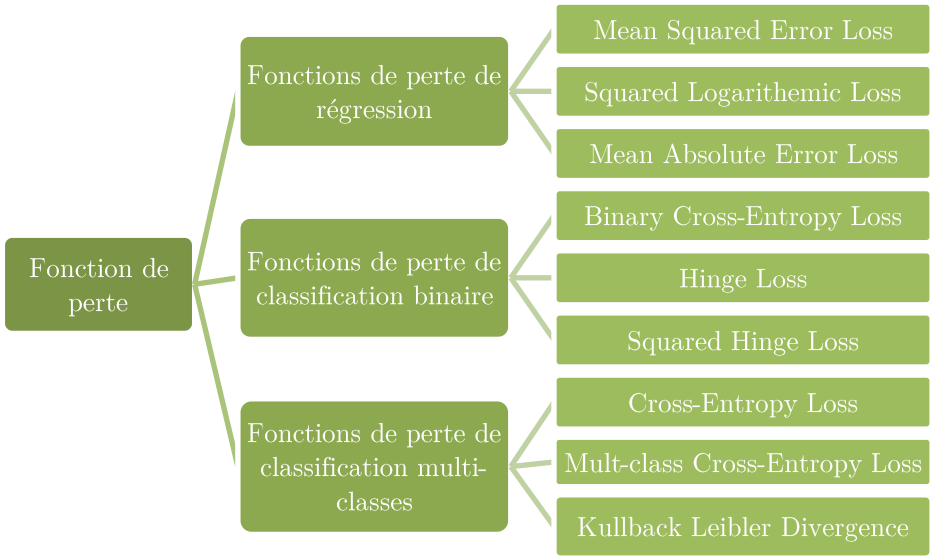

Figure 2.15 Les fonctions de perte de régression, perte de classification binaire, perte de classification multi-classes et leurs sous-divisions.

Dans la majorité des problèmes de régression, la fonction de perte mean squared error est utilisée. Elle est considérée comme la fonction de perte préférée pour l'estimation du maximum de vraisemblance lorsque la distribution de la classe cible est gaussienne (Brownlee, 2018). En pratique, mean squared error est calculée en faisant la moyenne de la différence quadratique entre les classes attendues et réelles. En raison de la valeur idéale de zéro de la fonction, elle fournit toujours un résultat positif qui a un effet sur les erreurs significatives.

La fonction de perte Binary Cross-Entropy est le choix optimal pour les tâches de classification binaire. Elle est principalement utilisée lorsque la classe cible est une valeur numérique 0 ou 1. En pratique, c'est la fonction de perte préférée dans le cadre du maximum de vraisemblance de l'inférence (Brownlee, 2018). Lorsque la fonction de perte Binary Cross-Entropy renvoie un 1, le coût moyen de la différence entre les valeurs réelles et prédites est additionné. En revanche, lorsque la valeur de Cross-Entropy est de 0, le score est minimisé.

La fonction de Multi-class Cross-Entropy est la fonction de perte la plus souvent utilisée pour les tâches de classification multi-classes. Semblable à la fonction de perte Binary Cross-Entropy, elle est destinée à être utilisée avec des valeurs cibles du type (Classe 1, Classe 2, Classe 3, ... Classe n). Dans cet exemple, chaque classe se voit attribuer une valeur entière indiquant sa vraisemblance, ce qui est en fait la fonction de perte préférable dans le cadre d'inférence de vraisemblance maximale. Le score est résumé de la même manière que la fonction de perte Binary Cross-Entropy dans la pratique. Quelle que soit la fonction de perte utilisée, elle doit correspondre à la fonction d'activation puisque le bénéfice de perte est évalué en permanence, lors de la comparaison de la sortie prévue à la sortie réelle.

2.5 Les techniques d'apprentissage en profondeur pour les systèmes biométriques

L'apprentissage en profondeur est une avancée évolutive dans le domaine de l'apprentissage automatique. La technique a été adoptée dans plusieurs domaines où l'ordinateur, après avoir traité des volumes de données, devrait prendre des décisions intelligentes. Un domaine d'application important pour l'apprentissage en profondeur est le domaine de la biométrie dans lequel les modèles dans les traits humains uniques sont reconnus. Récemment, de nombreux systèmes et applications ont appliqué l'apprentissage en profondeur pour les systèmes biométriques. Le réseau profond est entraîné sur la vaste gamme de modèles, et une fois que le réseau a appris toutes les caractéristiques uniques de l'ensemble de données, il peut être utilisé

pour reconnaître des modèles similaires. La technologie biométrique largement utilisée par les applications de sécurité comprend la reconnaissance basée sur le visage, les empreintes digitales, l'iris, l'oreille, l'empreinte palmaire, la voix et la démarche.

2.6 Conclusion

Dans ce chapitre nous avons présenté les différentes approches basées sur l'identification. Nous avons les systèmes biométriques comme système d'authentification sur plusieurs modalités biométriques comme l'empreinte digitale, le visage, l'iris et empreinte palmaires.

L'apparition de l'apprentissage automatique a permet au système de simuler des activités d'apprentissage humain sans être explicitement programmé. L'apprentissage automatique étudie également les topographies biométriques pour simuler les activités d'apprentissage d'identification d'un individu.

L'apprentissage automatique a rendu possible le fonctionnement de l'identification biométrique et a également fait beaucoup de progrès dans la reconnaissance des formes biométriques. Les paradigmes de l'apprentissage automatique sont divisés en trois types : apprentissage supervisé, apprentissage non supervisé et apprentissage demi supervisé. Ces paradigmes aident dans les tâches d'identification, de classification, de regroupement, de réduction de la dimensionnalité et de reconnaissance qui sont nécessaires pour développer des systèmes biométriques.

L'apprentissage en profondeur, une méthode d'apprentissage automatique, a considérablement amélioré les résultats dans de nombreux domaines, notamment la vision par ordinateur, la reconnaissance vocale et la traduction automatique. De nombreux problèmes économiques, notamment ceux liés à la santé, aux transports, au commerce, à la finance et à l'énergie, peuvent être résolus à l'aide de la technique d'apprentissage en profondeur.

Chapitre 3 - Les systèmes biométriques et l'apprentissage automatique

3.1 Introduction

L'inclusion de la biométrie, spécialement l'apprentissage automatique dans l'environnent du Mobile Cloud Computing pour sécuriser l'accès au cloud, a créé un nouvel élan de recherche. Dans ce chapitre nous allons voir les travaux connexes liés à cet axe de recherche. Ensuite, une étude `analytique pour dégager les avantages et les inconvénients. Enfin, d'après cette analyse principalement les inconvénients des recherches précédents, nous avons pu proposer des solutions convenables pour que les utilisateurs mobiles puissent s'authentifies au cloud en toute sécurité.

3.2 Les travaux connexes

La littérature sur la sécurité et le traitement d'images s'est développée ces dernières années. Par exemple, (Osadchy et al., 2010) ont proposé le Secure Computation of Face Identification (SCiFI) dans lequel la reconnaissance a été effectuée de manière à préserver la confidentialité des sujets et la sécurité de la base de données. En utilisant un processus d'image dépendant du patch local, chaque image de visage est décrite par un vecteur binaire. (Luong et al., 2013) ont suggéré un moyen de cibler le système SciFI en restaurant un visage brisé.

(Derawi et al., 2011) ont proposé une approche de l'utilisation des caméras de téléphones mobiles pour la capture d'une image d'empreinte digitale et testée sur des applications intégrées. Les tests ont révélé un taux d'erreur comparable (EER) de 4,5 %.

(Li et al., 2014) suggèrent un nouveau schéma de localisation Wifi Finger (PriWFL) préservant la confidentialité pour protéger les données des utilisateurs contre les vulnérabilités. Pour assurer la protection de l'emplacement d'un client, Li et al. utilisent le chiffrement homomorphe.

La classification sous chiffrement homomorphe dans le modèle semi-fiable a été introduite par (Nassar et al., 2016) ce travail présente une protection lors de la classification pour les systèmes d'authentification biométrique cloud basés sur le chiffrement homomorphe empirique de Paillier et des interactions client-serveur pour mesurer les distances et évaluer la précision de la classification. En outre, bien que le serveur fournisse aux utilisateurs un service de classification, il ne partage aucune information ou spécification de son ensemble de données

d'entraînement. La reconnaissance faciale préservant la confidentialité avec calcul externalisé est proposée dans la littérature basée sur le chiffrement entièrement homomorphe (FHE) (Xiang et al., 2016) , pour aider à réduire ces vulnérabilités de confidentialité et le coût du calcul.

(Wang et al., 2019; Wang and Nakachi, 2020) ont proposé une architecture de reconnaissance faciale sécurisée basée sur une représentation de rechange dans les réseaux edge et le cloud. Afin de garantir l'anonymat, une transformation unitaire aléatoire est mise en œuvre, sous laquelle la précision de la reconnaissance ne sera pas affectée. Cette approche implémente l'apprentissage du dictionnaire et du classificateur sur chaque serveur périphérique et la reconnaissance est gérée sur le cloud. Cela réduit à la fois les exigences de calcul pour chaque système et les exigences de connectivité entre la périphérie et le cloud. De plus, l'approche tire parti de la diversité des multi-dispositifs en trois phases. L'entrainement des images se fait en deux étapes, la première implique l'entrainement du dictionnaire et du classificateur, la deuxième consiste en un entrainement de groupe. Le modèle de décision est généré par les vecteurs d'étiquettes approximatifs en fonction de l'ensemble d'entrainement de groupe pour chaque classe dans l'espace intermédiaire. La reconnaissance est connue lorsque les similitudes entre le profil de décision de l'exemple de test et chacun des modèles de décision sont atteintes.

(Hu et al., 2020) ont proposé un algorithme de reconnaissance faciale sous chiffrement utilisant une combinaison de deux cartes chaotiques (Logistic Chaotic Mapping et Since Chaotic Mapping) avec un réseau de neurones. La clé de chiffrement a été générée par le mappage chaotique combiné pour chiffrer l'image du visage. Ensuite, la reconnaissance faciale a été effectuée à l'aide d'une analyse en composantes principales (PCA) et d'un réseau de neurones. Les expérimentations ont montré que l'algorithme donne une précision significative du côté de la reconnaissance sous données chiffrées. De plus, l'algorithme a prouvé sa robustesse et sa résistance à des attaques classiques.

(Ma et al., 2017) ont introduit un système de vérification faciale sécurisé utilisant CNN pour récupérer les caractéristiques du visage. Pour ce faire ils ont utilisé deux serveurs ; un serveur de données pour contenir les caractéristiques du visage cryptés de l'utilisateur ; et un serveur de vérification qui est ensuite utilisé pour exécuter la vérification chiffrée. Le chiffrement Paillier a été utilisé pour protéger les caractéristiques du visage. Toutes les données sont transférées sous formes chiffrées, de sorte qu'aucune entité ne puisse les décoder à l'exception du serveur de vérification. De plus, Ma et al. ont utilisé CNN pour extraire les caractéristiques. Ensuite, ils ont binarisé le vecteur de caractéristiques pour calculer la distance de Hamming entre les deux

vecteurs sous des données chiffrées. Le Tableau 3.1 résume les avantages et les inconvénients des méthodes proposées dans la littérature connexe.

Tableau 3.1 L'analyse des avantages et des inconvénients des travaux existants.

Références	Algorithmes et stratégies	Avantages	Inconvénients	Années
(Osadchy et al., 2010)	Algorithme de Paillier et transfert oublieux (OT) protocole	- Tolérant à une variété de situations de visualisation, telles que l'éclairage et les occlusions. - Préserver la confidentialité des données	- Avec l'expansion de la base de données, les coûts de traitement et de communication vont croître de manière linéaire.	**2010**
(Derawi et al., 2011)	Neurotechnology VeriFinger	- Taux de précision important.	- Testé sur une petite base de données. - Le système ne préserve pas la confidentialité des données.	**2011**
(Xiang et al., 2016)	Chiffrement entièrement homomorphique	- Préservez la confidentialité de la reconnaissance faciale.	- Surcharge de traitement plus élevée et limitations de l'algorithme de reconnaissance.	**2016**
(Wang et al., 2019; Wang and Nakachi, 2020)	Représentation et reconnaissance fragmentées sécurisées basées sur une transformation unitaire aléatoire	- Le système garantit que la confidentialité est protégée. - Les données chiffrées n'affectent pas la précision.	- Le taux de précision qui est égal à 95,44 % peut être amélioré.	**2019, 2020**
(Hu et al., 2020)	Cartographie chaotique combinée (cartographie chaotique sinusoïdale et cartographie chaotique logistique) + réseau de neurones à rétropropagation	- Préserver la confidentialité des données. - Résistant à de nombreuses attaques.	- Possibilité d'améliorer la précision qui est égale à 92,5% sur l'image cryptée et 81,5% avec les images non cryptées. - Le temps de reconnaissance est considérablement élevé, égal à 9,5 s.	**2020**
(Ma et al., 2017)	Réseau de neurones convolutifs, chiffrement homomorphe et distance de Hamming	- Capacité à atteindre un taux de précision élevé. - Préserver la confidentialité des données.	- Nécessite des ressources puissantes car le CNN implémenté est Complexe. - La binarisation du vecteur de caractéristiques pour calculer la distance de Hamming pour la correspondance affecte le taux de précision.	**2017**

A partir de cette analyse nous avons pu dégager trois solutions qui peuvent améliorer les systèmes précédents, comme illustrées dans la Figure 3.1.

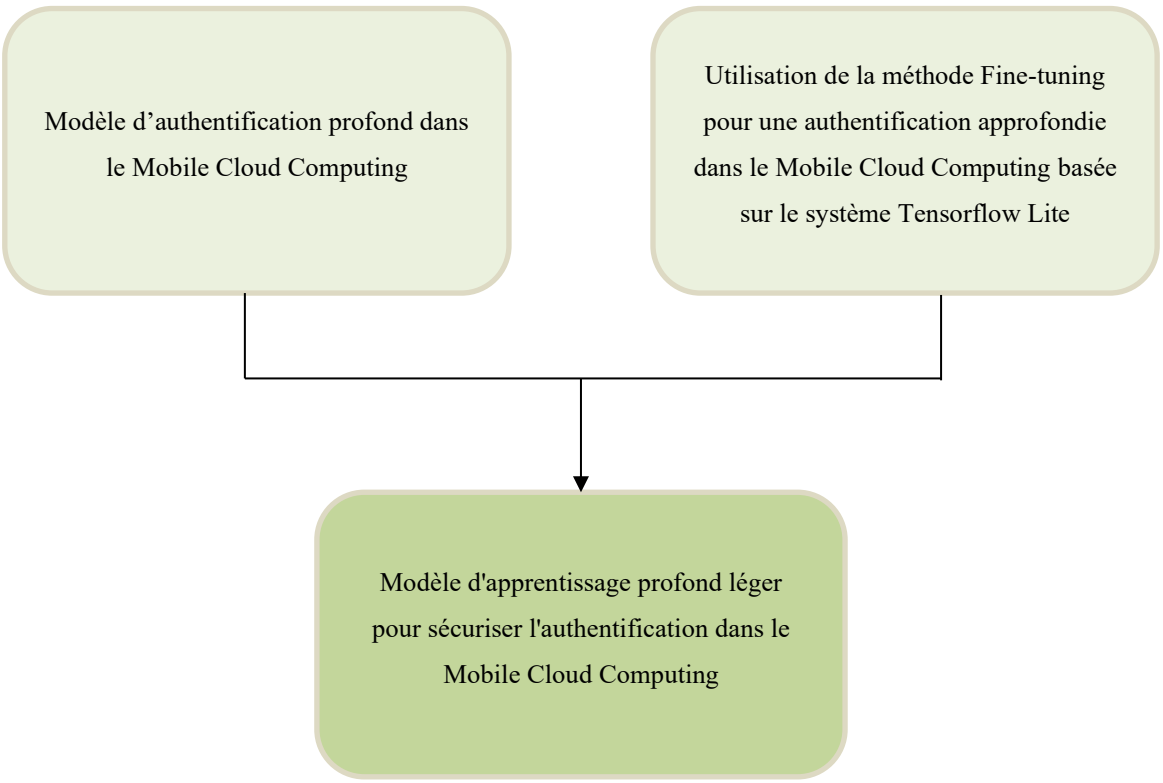

Figure 3.1 Contributions proposées.

Dans la première solution l'idée est de proposer un modèle d'authentification profond dans le Mobile Cloud Computing, a l'aide de la reconnaissance faciale basé sur l'apprentissage profond. Après une analyse de cette solution en a pu améliorer cette proposition en utilisant l'apprentissage par transfert et le framework Tensorflow lite. Les deux propositions nous ont aidé à suggérer une approche d'authentification légère sous des données chiffrées dans l'environnement du Mobile Cloud.

3.3 Les contributions proposées

3.3.1 Modèle d'authentification profond dans le MCC

La sécurité dans le Mobile Cloud Computing (MCC) est devenue obligatoire de nos jours. Cela est dû à l'utilisation croissante d'appareils mobiles pour accéder à divers comptes (par exemple, dossier médical, jeux, Facebook, Gmail, etc.). De nombreux chercheurs ont proposé l'authentification

biométrique dans le MCC, avec un modèle classique de formation et de classification comme l'utilisation du modèle binaire local (LBP) pour l'extraction des caractéristiques et de la machine à vecteur de support (SVM) pour la classification, etc., le réseau de neurones à convolution profonde (DeepCNN) surpasse les modèles classiques dans un certain nombre de cas.

En se basant sur le modèle SMCBA proposé dans (Al Rassan and Alshaher, 2014), nous avons suggéré un modèle d'authentification profond dans le Mobile Cloud Computing (Zeroual et al., 2018) qui utilise un réseau de neurones convolutifs profonds (DeepCNN) pour l'extraction des caractéristiques et la fonction Softmax pour la classification. Ce choix dépend des avantages de DeepCNN (Wicht, 2017) cité ci-dessous :

- Le processus d'extraction de caractéristiques est effectué automatiquement à partir des données d'apprentissage.
- Pour un réseau de neurones typique, il y a beaucoup plus de poids à prendre en compte, mais le nombre de poids à évaluer est beaucoup plus petit.
- Chaque couche apprend un ensemble de caractéristiques plus spécifiques en plus des caractéristiques de la couche précédente tout en apprenant les représentations profondes des images.

Ce modèle comprend un algorithme de reconnaissance faciale approfondie pour s'authentifier dans MCC. DeepCNN est la base de ce modèle, qui est utilisé à la fois pour l'entraînement et les tests. Ce modèle se compose de trois parties (MU : Utilisateur mobile, CS : Côté Cloud et AS : Serveurs d'application). En raison des ressources limitées des appareils mobiles et du processus d'apprentissage en profondeur, qui nécessite un matériel puissant, l'utilisation du cloud est primordiale. Comme illustre la Figure 3.2.

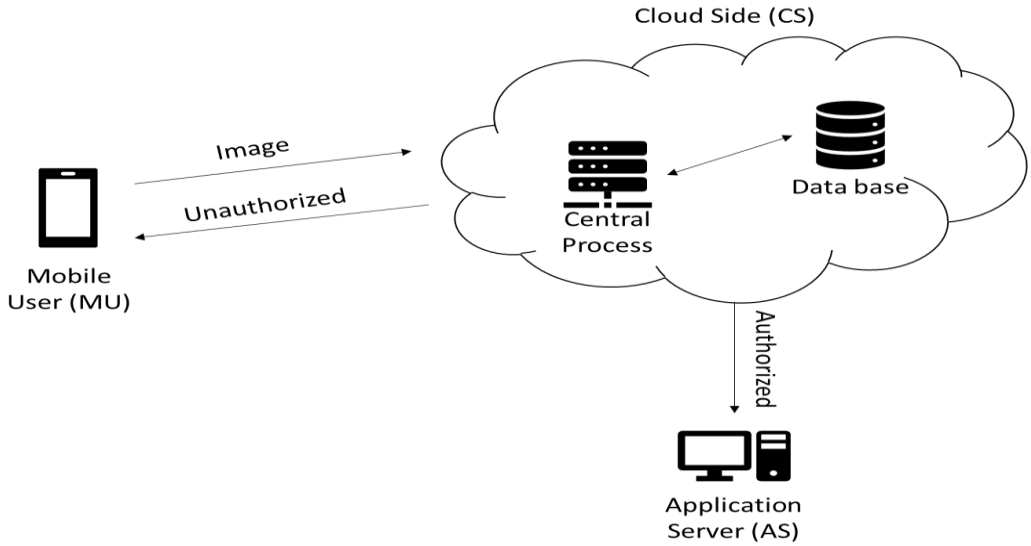

Figure 3.2 Architecture proposée pour cette approche.

- **Utilisateur mobile**

Une image du visage de l'utilisateur est prise et réduite à (28, 28) avant d'être envoyée au cloud pour authentification.

- **Coté cloud**

Pour l'authentification, nous avons utilisé un système de reconnaissance faciale profond basé sur DeepCNN. La Figure 3.3 illustre l'implémentation de DeepCNN pour la formation et la classification. Nous avons utilisé un DeepCNN pour l'extraction de caractéristiques la fonction Softmax pour la classification pendant l'entraiment. Le MU, dans l'évaluation, s'est déjà enregistré. Après avoir reçu l'image de l'utilisateur, le CS la compare à celles déjà classées. Si la réponse est affirmative, le MU reçoit l'autorisation d'accéder à l'AS. Si le résultat est négatif, le CS envoie un message d'accès non autorisé au MU.

a) L'architecture de DeepCNN

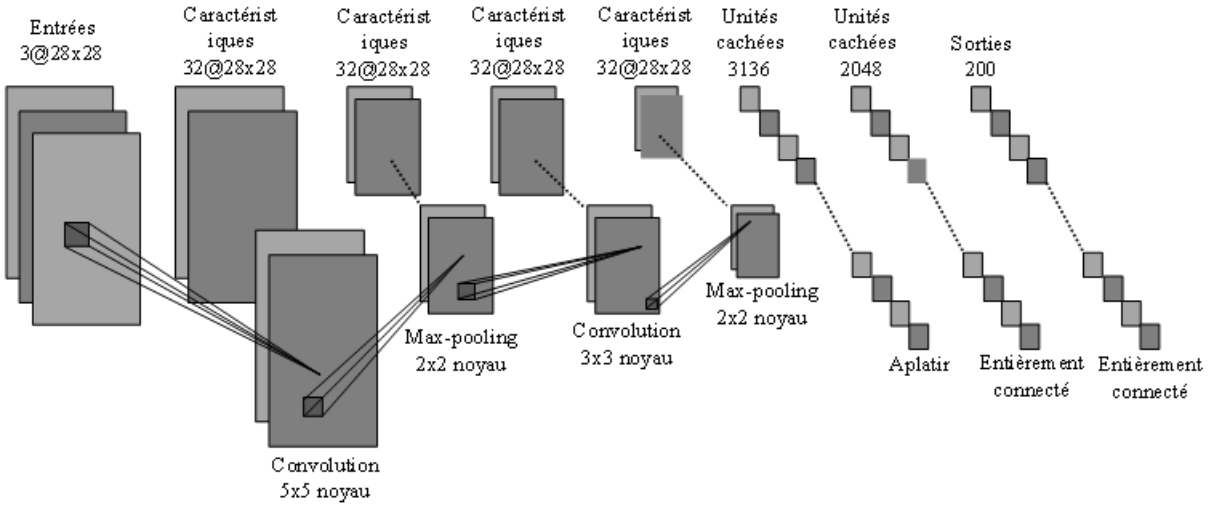

Figure 3.3 L'architecture de DeepCNN proposé (Zeroual et al., 2018).

La conception de DeepCNN est structurée comme suit : INPUT-(CONV/RELU)-POOL-(CONV/RELU)-POOL-FC :

Une image avec des dimensions de largeur 28 et hauteur 28 et trois canaux de couleur RGB sera placée en entrée [28x28x3].

À l'aide d'une couche convolutive, la sortie des neurones connectés à des zones spécifiques d'entrée sera donnée en calculant le produit scalaire entre les poids de chaque neurone et les poids de la région d'entrée à laquelle il est connecté. Si nous décidions d'utiliser un filtre de 32 et padding pour garder la dimension spatiale constante après convolution et pour optimiser la vitesse, nous pourrions nous retrouver avec une dimension de [28x28x32]. Si nous ne définissons pas le padding, la taille diminuera et les informations aux frontières seront perdus. Après chaque opération convolutive, nous utilisons ReLu comme fonction d'activation, cela laisse la taille du volume inchangée.

L'image d'entrée [28x28x32] peut être réduite en taille [14x14x32] en ajoutant la couche MaxPooling (2,2).

De plus, ces processus sont répétés une fois de plus pour augmenter la précision et l'efficacité de l'extraction des caractéristiques.

La matrice résultante de taille 7x7 est transformée en un vecteur unidimensionnel, qui est finalement transmis à la dernière couche (FC).

Couche entièrement connectée : cette couche est responsable de la classification des données. Nous calculons les scores de classe de chaque personne à l'aide de la fonction Softmax pour la classification. Nous avons 200 personnes dans notre cas.

- **Serveur d'application**

Microsoft Office, les sites de réseaux sociaux, Gmail et d'autres applications dépendent de la réception ou non d'une décision de la part de CS de leur fournir l'accès.

Cette méthode a été évaluée sur une base de données FEI (Thomaz, 2006), qui contient 2800 images de visage de 200 personnes, chaque personne possède 14 images. La taille de chaque image est de 640x480 pixels et toutes les images ont des positions différentes (rotation de 180 degrés). Le nombre d'images masculines et féminines est égal (100 hommes et 100 femmes). L'âge des personnes varie entre 19 et 40 ans.

Les résultats obtenus lors des tests sont satisfaisants. Nous avons obtenu un taux de 99.50% de précision et une perte de 0.01%. Ce travail a été publié dans une conférence indexée IEEE (Zeroual et al., 2018). Le principal problème de cette méthode est lorsque l'attaquant récupère l'image transmise, il peut s'authentifier en tant qu'utilisateur authentique.

Cela nous a motivé à opter pour une authentification basée sur une approche d'apprentissage en profondeur pour sécuriser l'accès au MCC. Pour cela nous avons utilisé une nouvelle bibliothèque nommée Tensorflow lite, qui permet aux utilisateurs d'utiliser des modèles entrainés par machine sur des appareils mobiles avec une faible latence. La bibliothèque n'est pas encore désignée pour les modèles d'entrainement, nous localisons l'entrainement sur la plate-forme cloud et le reste se fait sur les appareils mobiles.

3.3.2 Utilisation de la méthode ajustement fin pour une authentification approfondie dans le Mobile Cloud Computing basée sur le système Tensorflow Lite

Des progrès sont remarquables se sont fait ressentir dans les domaines de l'apprentissage profond et de l'environnement Mobile Cloud. La sécurité est devenue la partie la plus difficile sur le Mobile Cloud, cela est dû à la croissance du nombre de personnes qui utilisent leur mobile pour accéder aux services fournis par le cloud tels que les soins de santé, le stockage, les jeux, etc. Cette contribution vise à suggérer d'utiliser le framework d'apprentissage en profondeur pour mobile Tensorflow Lite pour effectuer la reconnaissance sur mobile sans avoir besoin du cloud ou de ressources informatiques et pour éviter que les utilisateurs envoient leur image à chaque fois. Amélioration de la précision du travail effectué avec une précision de 99,50 % à 100 % en appliquant la méthode d'ajustement fin.

a) Tensorflow lite

Une autre raison qui nous a motivés à proposer ce modèle est de réduire le temps de transfert des données (images) du mobile vers le cloud et d'éviter que les attaquants n'interceptent nos données à chaque fois. Pour atteindre cet objectif, nous proposons d'utiliser la bibliothèque TensorFlow Lite ("TensorFlow Lite | ML for Mobile and Edge Devices," n.d.) pour appareil mobile, qui consiste à convertir le modèle de fichier généré après la phase d'entrainement en fichier adapté au mobile avec l'extension .tflite. La Figure 3.4 Explique la mise en œuvre de TensorFlow Lite.

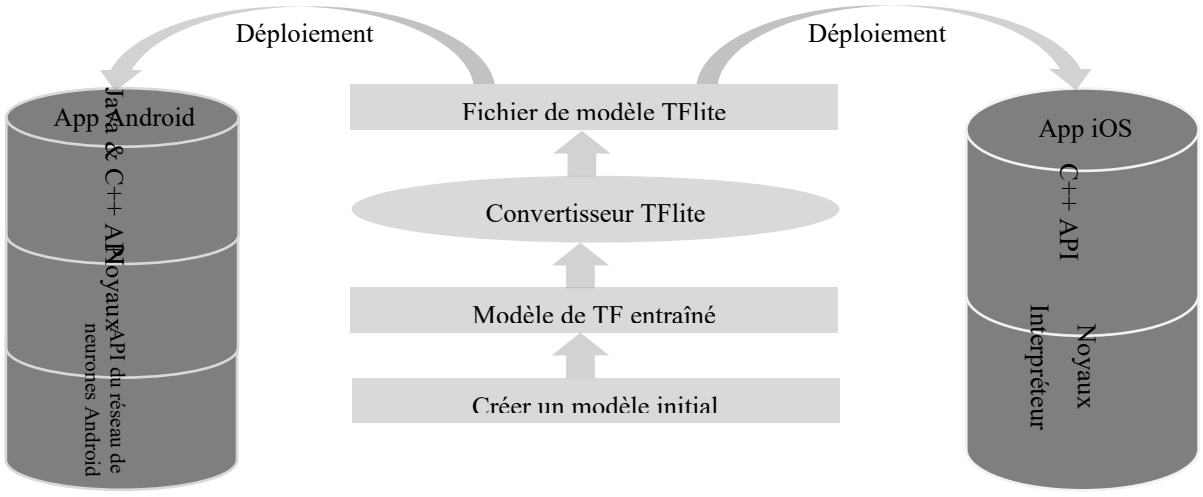

Figure 3.4 L'organigramme de Tensorflow Lite (Zeroual et al., 2019).

Une autre raison qui nous a motivé à utiliser l'approche de l'apprentissage par transfert (ajutement fin) est que la base de données que nous utilisons est plus petite. Nous nous sommes concentrés sur le modèle VggNet pré-entrainé avec une grande base de données (ImageNet), qui contient environ 1,2 million d'images à travers 1000 classes. Ensuite, nous testons notre modèle sur les dernières couches, puisque la couche de caractéristique précédente de DeepCNN couvre des caractéristiques plus génériques, mais les dernières couches deviennent de plus en plus spécifiques aux détails.

b) L'apprentissage par transfert

L'apprentissage par transfert (Pan and Yang, 2009) est une méthodologie d'apprentissage automatique qui utilise les données de problèmes connexes pour résoudre le problème cible. Le domaine source et le domaine cible sont l'expéditeur et le destinataire du transfert de connaissances.

L'apprentissage par transfert est extrêmement efficace lorsque le domaine de destination a une insuffisance de données d'apprentissage mais une grande quantité de données dans le domaine source. De plus, l'apprentissage est plus efficace lorsque les connaissances sont transférées d'un domaine très lié au domaine cible. En revanche, un transfert négatif se produit lorsque des informations sont transférées d'un domaine présentant une faible ressemblance avec le domaine cible.

La limite maximale des performances d'apprentissage dans le domaine d'entrainement est souvent déterminée par la limite maximale des performances d'apprentissage dans le domaine source. En d'autres termes, une précision accrue dans le domaine source augmente la probabilité d'accroître l'efficacité d'apprentissage dans le domaine cible.

En se basant sur notre précédent travail un modèle à partir de zéro pour l'authentification profonde dans le cloud computing mobile (Zeroual et al., 2018). Ce dernier travail a atteint une précision de 99,50% avec l'architecture de DeepCNN qui contient deux couches de convolution et deux couches MaxPooling. Afin d'améliorer la précision, nous avons proposé l'utilisation d'une méthode de ajustement fin pour une authentification profonde dans le Mobile Cloud Computing basée sur le framework Tensorflow lite (Zeroual et al., 2019), un modèle basé sur le modèle pré-entraîné VggNet qui contient 13 couches de convolution, 5 couches MaxPooling et 3 couches entièrement connectées. La grande tâche de VggNet dans ILSVRC14 a prouvé que l'utilisation d'une petite convolution et d'une forte intensité de réseau peut améliorer efficacement les performances du modèle. Réduire la taille du

filtre et augmenter la quantité de couches en se concentrant sur ces deux aspects VggNet peut atteindre une précision comparable (Yang et al., 2018).

Après les tests et les évaluations de ce dernier, le taux de précision a été amélioré à 100%. L'inconvénient de ce modèle est qu'il prend beaucoup de temps lors de la phase d'apprentissage.

3.3.3 Modèle d'apprentissage profond légé pour améliorer l'authentification dans le Mobile Cloud Computing

En analysant les travaux connexes, nous avons proposé une nouvelle approche qui consiste à combiner deux méthodes (Deep Convolutional Neural Network et Local Ternary Pattern DeepCNN LTP) pour la reconnaissance faciale, suivie de chiffrement partiellement homomorphe pour sécuriser l'authentification dans l'environnement MCC. L'objectif de cette proposition est d'augmenter le taux de reconnaissance, diminuer le temps d'exécution et préserver la confidentialité des données lors de l'authentification par rapport aux travaux existants.

a) Modèle local ternaire (Local Ternary Pattern: LTP)

Le modèle ternaire local est une dérivation de modèle binaires local (LBP) introduits dans (Tan and Triggs, 2010) qui convertit les images en niveaux de gris en trois valeurs -1, 0, 1, contrairement au LBP qui convertit l'image en niveaux de gris en deux valeurs 0 et 1. Cette propriété de LTP le rend plus sensible à la variation de lumière. L'expression LTP est décrite comme suit dans l'Équation 3.1 et l'Équation 3.2 :

$$LTP_{P,R} = \sum_{i=0}^{P-1} S(i_p - i_c)2^P$$

Équation 3.1

Où P est le nombre de voisins dans le rayon R qui définit le cercle de la position i_p des voisins en fonction du pixel central i_c. t désigne le seuil défini par l'utilisateur et S est égal à :

$$S(i_p - i_c) = \begin{cases} 1 \; if \; i_p \geq i_c + t \\ 0 \; if \; i_c - t \leq i_p \leq i_c + t \\ -1 \; if \; i_p \leq i_c - t \end{cases}$$

Équation 3.2

L'utilisateur définit la valeur de t pour calculer l'intervalle dans lequel les pixels voisins lui sont comparés. Comme indiqué dans l'Équation 3.1 et l'Équation 3.2, LTP génère trois valeurs en fonction du seuil défini. Si le pixel voisin i_p est supérieur au pixel central plus t la valeur générée est 1, si le pixel voisin i_p est située entre i_c- *1* et i_c+ *1* la valeur générée pour coder ce pixel est 0, sinon LTP génère 1 pour coder le pixel en niveaux de gris. Par exemple, si le seuil t est égal à 5 et le pixel central i_c est égal à 34 alors l'intervalle déduit pour coder les pixels en niveaux de gris est *[29, 39]*. Après le code est divisé en deux LBP (LBPUpper, LBPLower). Cela se fait en convertissant la valeur générée en valeurs 0, 1. Dans le cas de LBPUpper, si la valeur LTP est égale à -1, convertissez-la en 0. Dans le cas de LBPLower, si la valeur LTP est égale à 1, convertissez-la en 0 et -1 en 1, comme illustré à la Figure 3.5.

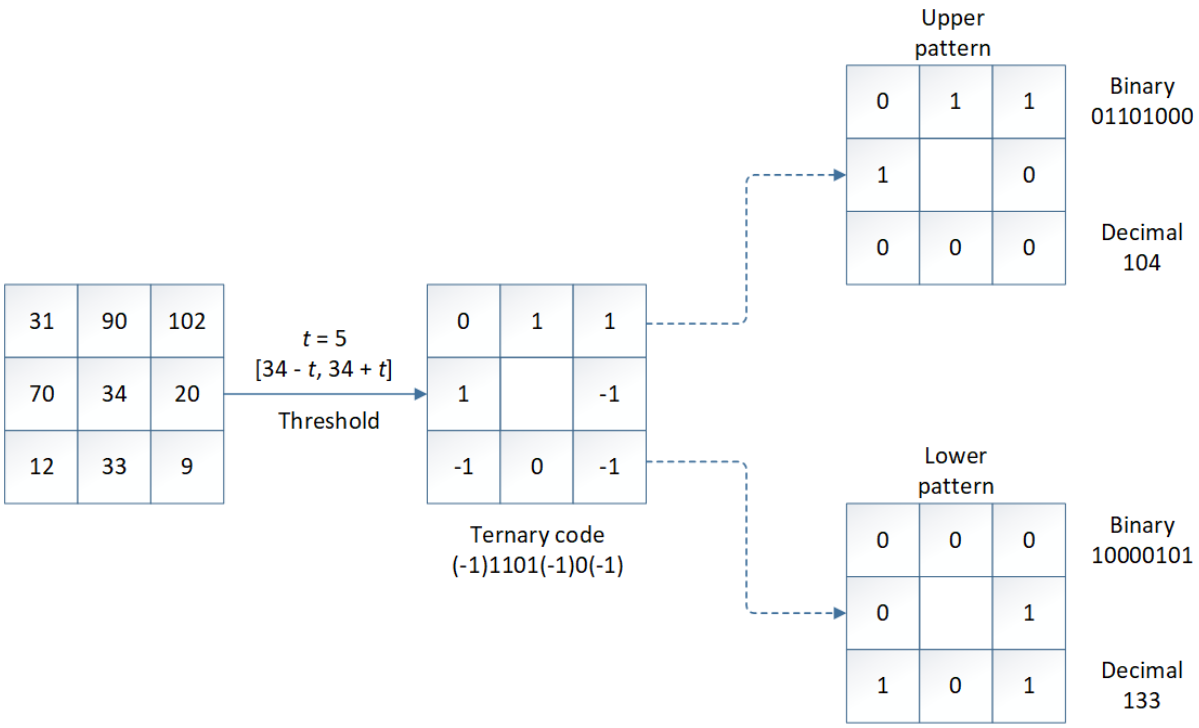

Figure 3.5 L'encodage LTP pour un bloc de 3x3 (Zeroual et al., 2021).

b) Le chiffrement partiellement homomorphe (PHE)

Le chiffrement homomorphe partiel (PHE), les textes chiffrés ne peuvent être qu'additionnés ou multipliés (ElGamal, 1985; Paillier, 1999; Rivest et al., 1978). Les PHE jettent les bases des méthodes

de chiffrement homomorphe, même si les chercheurs ont déjà atteint le cap du chiffrement quelque peu homomorphe (SWHE) et du chiffrement entièrement homomorphe (FHE) (Gentry, 2009).

c) Le schéma de Paillier

Le problème de résidu composite (Jager, 2012; Rivest et al., 1978) a été utilisé pour créer ce système probabiliste de chiffrement à clé publique (Paillier, 1999).

L'algorithme de génération de clé : Pour trouver $n = pq$ et $\lambda = lcm(p - 1, q - 1)$, choisir de grands nombres premiers p et q tels que $pgcd(pq, (p - 1)(q - 1)) = 1$. Afin de générer un nombre aléatoire g dans le sous-groupe $g \in Z_{n^2}^*$, nous devons voir si l'expression $pgcd(n, L(g^{\lambda \bmod n2})) = 1$, où L est défini comme $L(u) = (u - 1)/n$ pour chaque u dans le sous-groupe multiplicatif $Z_{n^2}^*$. Les clés publiques et secrètes dans ce schéma sont (n, g) et (p, q).

L'algorithme de chiffrement : L'Équation 3.3 suivante (Rivest et al., 1978) peut être utilisée pour chiffrer m et générer r au hasard :

$$c = E(m) = g^m r^n = (mod\ n^2)$$

Équation 3.4

L'algorithme de déchiffrement : Récupérez le message en utilisant l'Équation 3.5 (Rivest et al., 1978) pour tout texte chiffré $c<n^2$:

$$D(c) = \frac{L\left(c^{\lambda}(mod\ n^2)\right)}{L\left(g^{\lambda}(mod\ n^2)\right)}(mod\ n)$$

Équation 3.6

D'où (p,q) est une clé secrète.

Propriété homomorphe : Le schéma de chiffrement de Paillier est homomorphe à l'addition pour chaque opération de multiplication sur le texte chiffré (Rivest et al., 1978).

$$E(m_1) \times E(m_2) = \left(g^{m_1} r_1^n (mod\ n^2)\right) \times \left(g^{m_2} r_2^n (mod\ n^2)\right) = g^{m_1+m_2}(r_1 \times r_2)^n (mod\ n^2)$$
$$= (m_1 + m_2)$$

Équation 3.7

L'architecture de cette approche est illustrée dans la Figure 3.6 pour plus de détails. Le travail est composé en deux parties, la première concernant l'apprentissage basé sur le DeepCNN qui se fait au niveau du cloud. La deuxième partie concerne l'authentification de l'utilisateur qui utilise le modèle reçu par le cloud converti avec Tensorflow Lite pour être déployé par les utilisateurs mobiles. Le choix de la localisation de l'apprentissage au niveau du cloud au lieu que ce soit au niveau du mobile, est dû aux ressources limitées du mobile.

Après la réception du modèle entrainé par le cloud, l'utilisateur utilise son mobile pour prendre une image de visage pour s'authentifier au niveau du cloud. Ensuite, à ce niveau-là, l'image va être traitée pour en extraire les caractéristiques à l'aide du modèle reçu de manière précise. Le vecteur de caractéristiques doit être chiffré avec le chiffrement partiellement homomorphe afin que les données transmises au cloud soient confidentielles. Comme le montre dans la Figure 3.6.

Une requête d'authentification est envoyée au cloud qui contient l'Identifiant de l'utilisateur et le vecteur chiffré.

Lors de la réception de cette demande, le cloud cherche l'image de visage correspondante à l'utilisateur, ensuite, le processus du traitement et de l'extraction des caractéristiques de l'image est fait pour comparer les deux vecteurs afin que l'utilisateur puisse s'authentifier au cloud et ce en fonction de la décision reçue par le cloud.

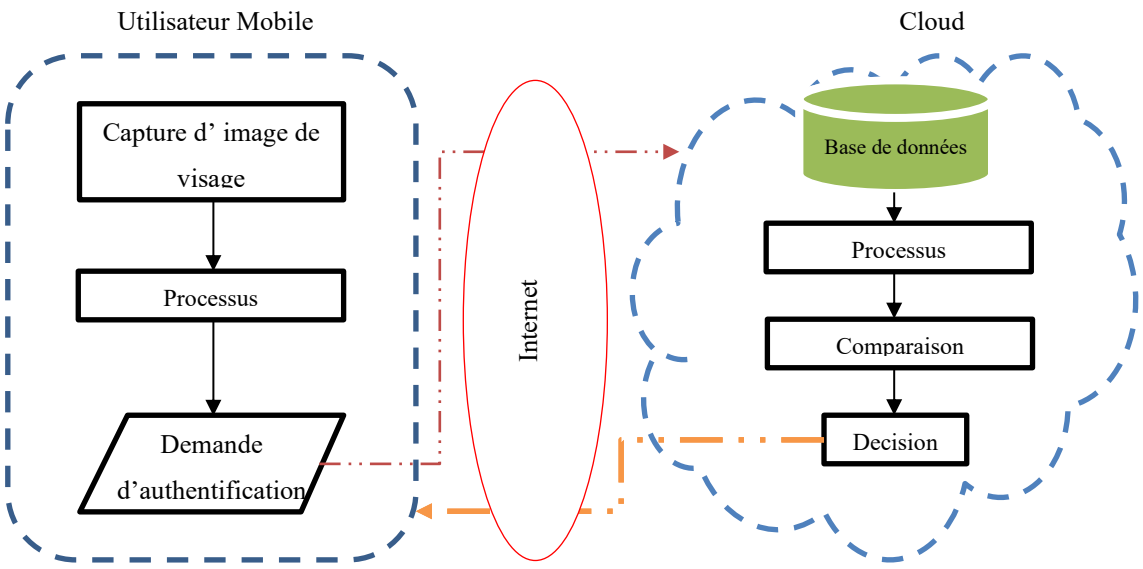

Figure 3.6 L'architecture de l'approche proposée.

La proposition - comme illustré dans la Figure 3.7 - se compose de cinq étapes :

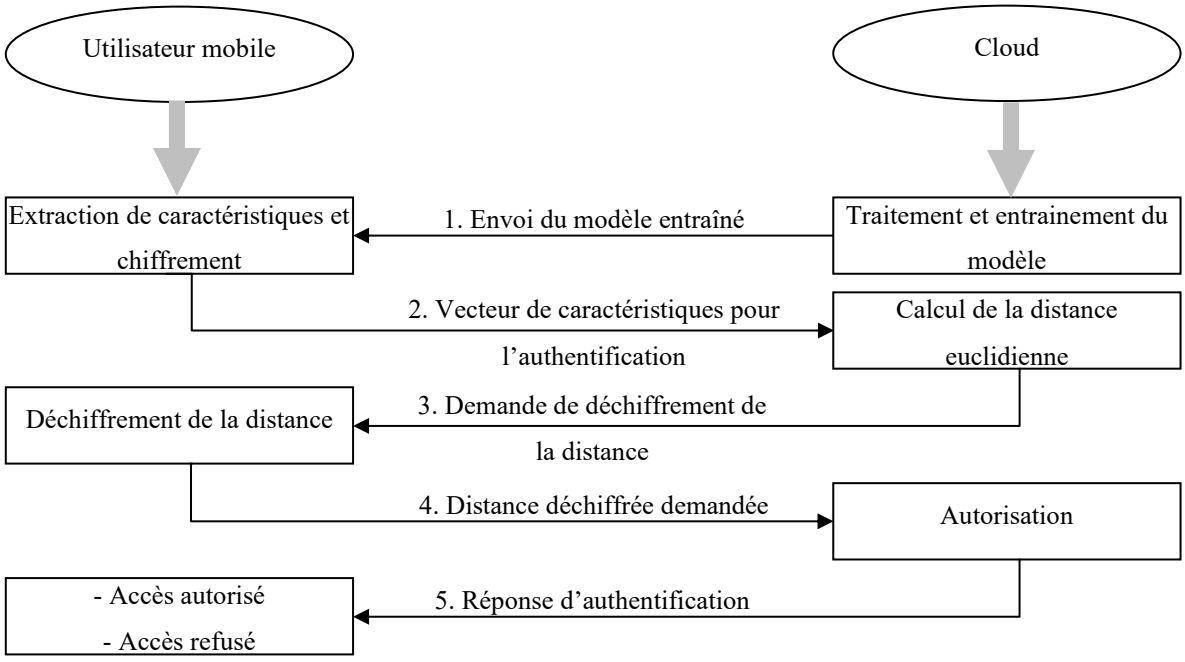

Figure 3.7 Le système d'authentification proposé.

- **Etape 1 - Traitement et entrainement du modèle**

Utilisation de LTP et DeepCNN combinés. LTP est utilisé pour prétraiter toutes les images de la base de données, ce qui permet à DeepCNN d'extraire précisément les caractéristiques importantes parce que LTP est plus sensible à la variation de lumière. L'architecture du DeepCNN est composée de deux modèles séquentiels combinés concaténés au niveau d'une couche aplatie (Flatten), chaque modèle séquentiel est le même proposé dans notre précèdent travail (Zeroual et al., 2018). Le modèle résultant, après concaténation, est connecté à une couche entièrement connectée suivie d'une couche de classification. Chaque modèle contient deux couches de réseau neuronal convolutif, deux couches de Max-pooling et une couche Flatten, cette derniére est responsable de la génération du vecteur de caractéristiques de l'image du visage - comme illustré à la Figure 3.8 - où le nombre 15 dans la dernière couche définit le nombre de classes. Le modèle résultant est ensuite converti en un modèle compatible à utiliser par l'utilisateur mobile à l'aide de TensorFlow Lite ("TensorFlow Lite | ML for Mobile and Edge Devices," n.d.). Cela signifie que le résultat de cette étape est un modèle TensorFlow Lite entrainé pour les utilisateurs sur mobile.

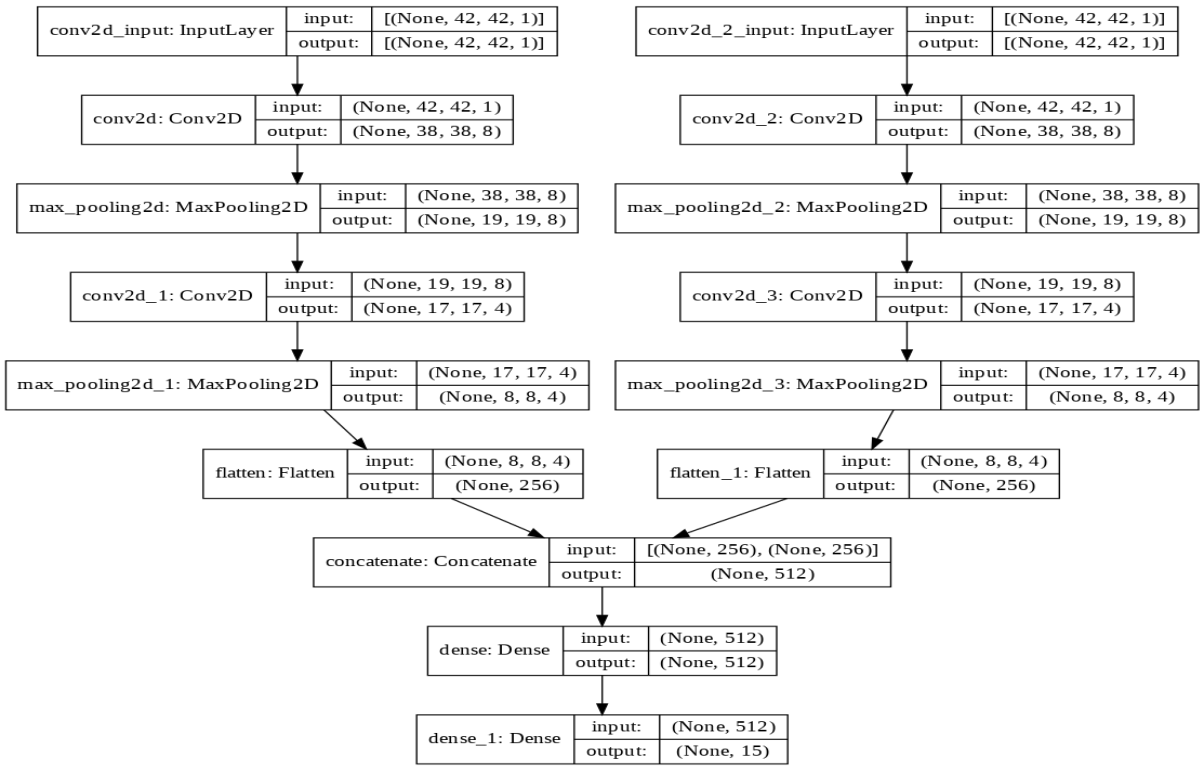

Figure 3.8 L'architecture de réseau de neurones convolutifs proposée (Zeroual et al., 2021).

- **Etape 2 - Extraction de caractéristiques et chiffrement**

Lorsque l'utilisateur reçoit le modèle entrainé avec TensorFlow Lite depuis le cloud, il applique LTP sur son image du visage afin de générer les entrées (images positives et négatives). Ces données sont transmises au modèle entrainé pour extraire le vecteur de caractéristiques *V'*. Ensuite, il génère une clé publique et privée comme expliqué dans la sous-section 3.3.1 pour chiffrer le vecteur de caractéristiques *V'*, suite à cela, l'utilisateur calcule et crypte la somme ($SV = \sum_{i=0}^{m} V'^{2}_{i}$) de toutes les valeurs du vecteur *V'* en utilisant un chiffrement homomorphe et les envoie vers le Cloud avec son *ID* pour authentification. Nous avons utilisé l'algorithme de Paillier dans notre approche (expliquée dans la sous-section 3.3) pour prendre en compte l'aspect sécurité de notre processus. La sortie de cette phase est l'*ID*, le vecteur caractéristique chiffré *V'* avec *SV* pour calculer la distance euclidienne à l'étape suivante. *(ID, V', SV).*

- **Etape 3 - Calcul de la distance euclidienne**

Après avoir reçu l'*ID*, *V'* et la valeur *SV*, le serveur d'authentification cherche l'image de visage correspondante à l'aide de l'ID reçu. Il procède alors à l'extraction des caractéristiques de l'image correspondante comme décrit à l'étape 2. Le vecteur résultant est comparé au vecteur chiffré par le calcul de la distance euclidienne. Pour masquer cette distance, le serveur ajoute un nombre aléatoire *x* à cette distance car cette distance est chiffrée et prête à être envoyée à l'utilisateur pour l'opération de déchiffrement telle qu'expliquée dans l'étape 4.

- **Etape 4 - Déchiffrement de la distance**

Dans cette étape, l'utilisateur déchiffre cette distance. Il ne connaît pas la valeur exacte de la distance puisqu'elle a été voilée dans l'étape 3 ci-dessus afin de le protéger d'éventuels attaques. Une fois cette distance déchiffrée, l'utilisateur l'envoie au serveur d'authentification. La sortie de cette étape est une valeur de distance masquée.

- **Etape 5 - Autorisation**

Après la réception de la distance déchiffrée, le serveur d'authentification soustrait la valeur *x* ajoutée et compare la distance minimale au seuil *n* d'autorisation. Si la distance obtenue est inférieure au seuil

n, le serveur d'authentification autorise l'utilisateur à accéder au Cloud, sinon, l'authentification est refusée.

d) L'extraction de caractéristiques de l'image du visage

L'extraction des caractéristiques dans la littérature précédente a été effectuée par des méthodes classiques telles que les SIFT et les caractéristiques de Gabor. Il a été démontré, cependant, que DeepCNN fonctionne mieux pour la reconnaissance faciale (Li et al., 2014). Les neurones de chaque couche de DeepCNN indiquent des données d'entrée différentes, tandis que la dernière couche (couche Flatten) génère le vecteur de caractéristiques de longueur *n*, comme illustré à la Figure 3.9. L'application du LTP pour chaque visage générera deux images (positive et négative), ce qui augmente la taille de la base de données et produira de meilleurs résultats en utilisant DeepCNN. Cela signifie que la taille de la base de données se double. Cela augmente également la précision du DeepCNN. L'idée de créer deux modèles séquentiels est liée au LTP lorsqu'il produit les images positives et négatives à ce stade. La création de deux modèles séquentiels, dont l'un est pour l'image positive tandis que l'autre est pour l'image négative fonctionnant en parallèle. Nous procédons ensuite à l'étape de chiffrement du vecteur de caractéristiques généré.

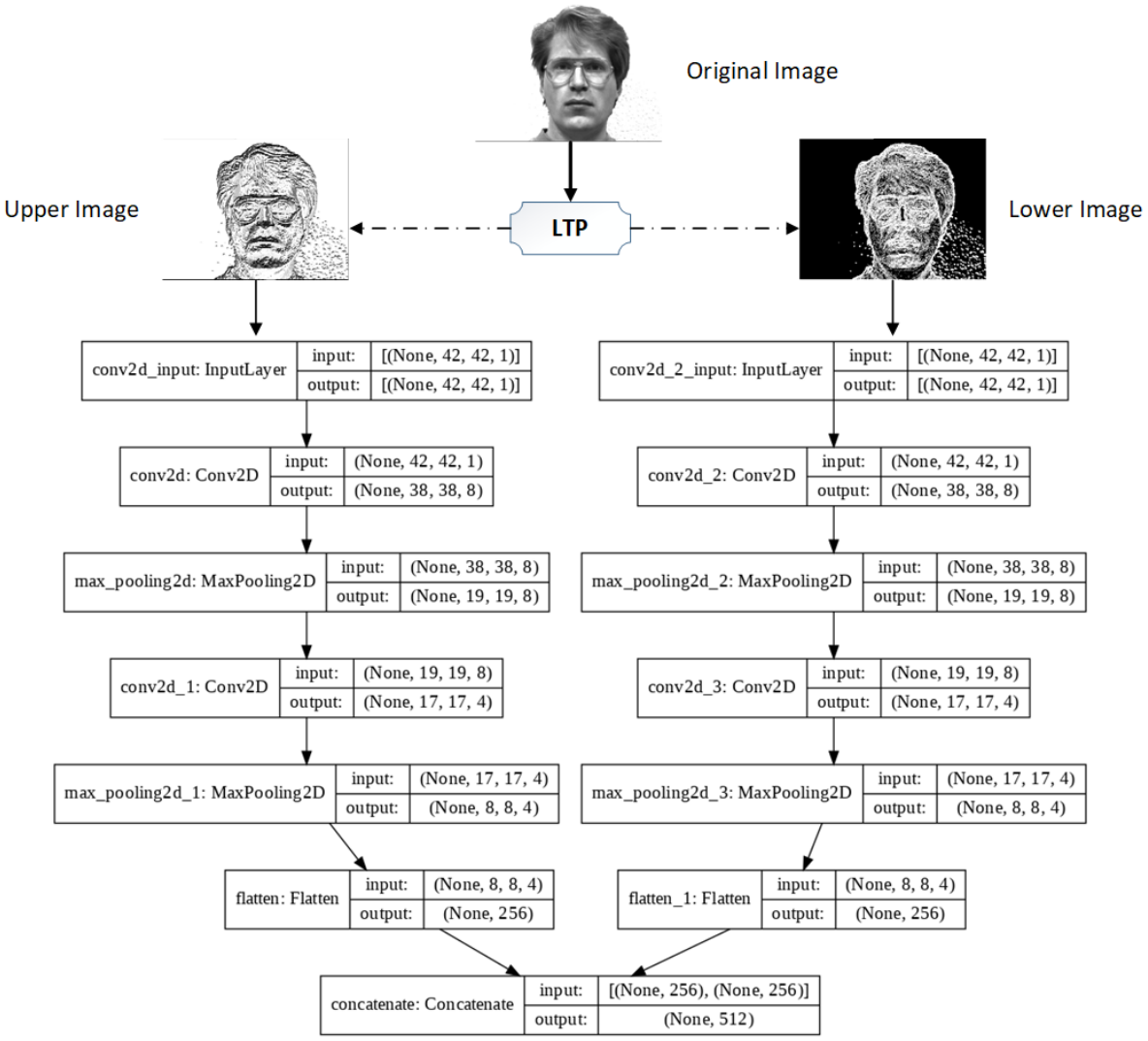

Figure 3.9 L'extraction de caractéristiques (Zeroual et al., 2021).

e) L'étape d'enregistrement

Dans cette étape d'enregistrement, l'utilisateur a besoin de s'enregistrer auprès du serveur de cloud en fournissant ses données d'identification comme ID et ses photos de visage appropriées. Le serveur du cloud stocke les données dans la base de données du cloud, dans le même temps le serveur procédera à la création du modèle qui se sert pour entrainer le modèle à base d'apprentissage approfondie. Une fois le modèle créé, le serveur du cloud le convertit en un modèle adéquat pour le mobile à l'aide du framework Tensorflow Lite pour que les utilisateurs mobiles puissent l'utiliser. Après cela, le serveur du cloud envoie ce modèle au mobile pour l'utiliser dans une future authentification comme le montre la Figure 3.10.

f) Calcul de la distance euclidienne sous chiffrement homomorphe

L'équation principale de la distance euclidienne entre deux vecteurs est représentée dans l'Équation 3.8

$$D^2 = \sum_{i=1}^{m} (VC_i - VC'_i)^2 \; 2$$

Équation 3.8

Ou *VC* est le vecteur de caractéristiques généré par l'entrainement de l'objet *i* et le *VC'* est le vecteur de caractéristiques issue de la phase de test l'objet *i*. Le calcul de la distance euclidienne chiffrée D^2 est défini comme suit dans l'Équation 3.9

$$D^2 = \sum_{i=1}^{m} VC_i^2 + \sum_{i=1}^{m} VC'^2_i - 2(\sum_{i=1}^{m} VC_i . VC'_i)$$

Équation 3.9

Ce processus est exécuté par la coopération d'utilisateur mobile et le serveur cloud comme mentionnée dans l'étape 3 du système d'authentification proposé. A cet effet, l'utilisateur mobile chiffre le vecteur *VC* et calcule la somme du VC^2 et les transmet au serveur du cloud afin que ce dernier puisse calculer la distance sous les données chiffrées. Une fois que la distance est calculée, le résultat est une valeur chiffrée qui sera déchiffrée uniquement par l'utilisateur. A ce niveau-là, le serveur du cloud ajoutera une valeur aléatoire *x* à la distance chiffrée pour la protéger. Une fois cette distance déchiffrée et renvoyée vers le serveur du cloud, ce dernier soustrait la valeur ajoutée pour avoir la valeur exacte de la distance afin de pouvoir la comparer au seuil *n*, pour enfin décider de l'accès ou non au cloud et bénéficier de ses services.

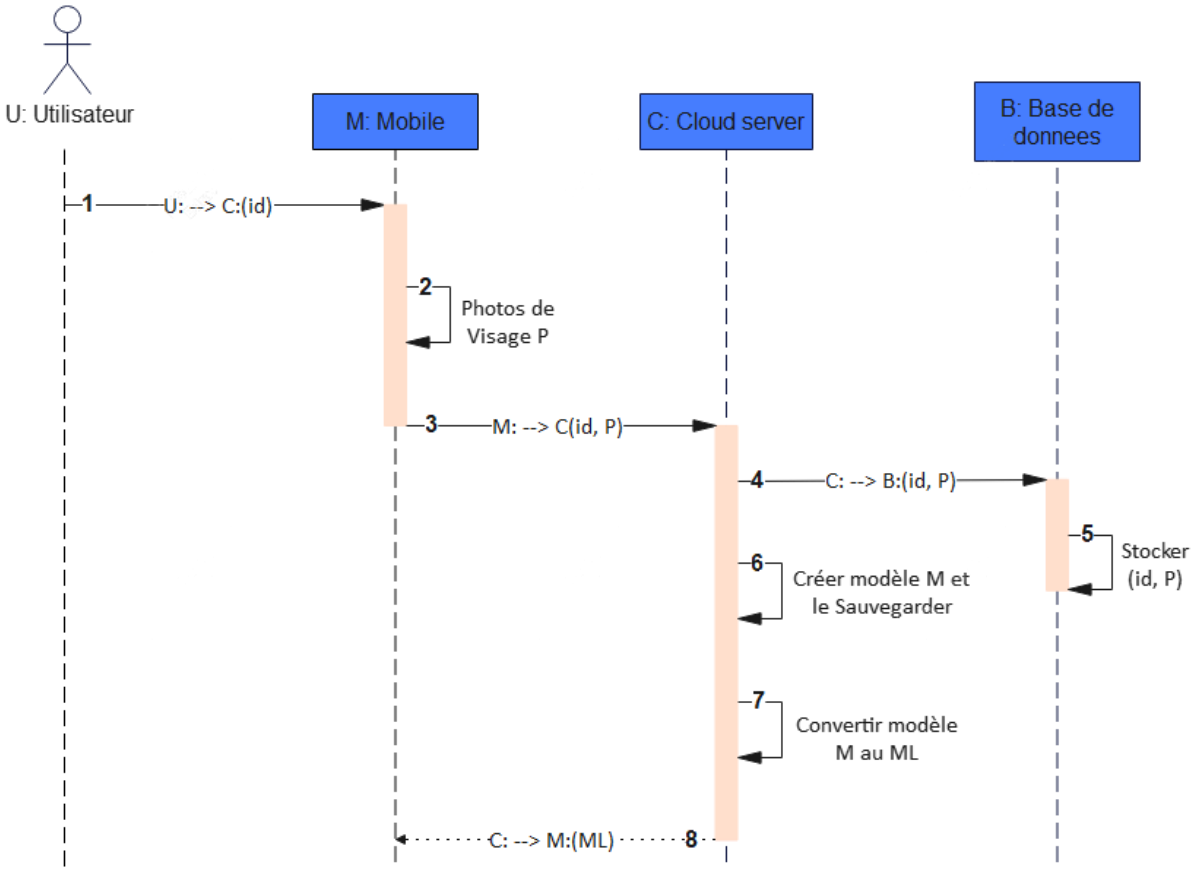

Figure 3.10 Le diagramme séquentiel de la phase d'enregistrement.

La procédure de cette étape est comme suit :

1- L'utilisateur introduit son identifiant *ID* et envoie une demande d'enregistrement auprès du mobile. *U : --> C : (id).*
2- Le mobile prend des photos de visage de cet utilisateur *P*.
3- Le mobile transfèrera la requête d'enregistrement au serveur cloud qui contient l'*ID* et les photos de visage de l'utilisateur. *M : --> C : (id, P).*
4- Une fois la demande reçue par le serveur cloud, il envoie les données de l'utilisateur à la base de données pour le stockage. *C : --> B : (id, P).*
5- Dans cette phase toutes les données sont enregistrées au sein de la base de données.
6- Le serveur cloud créera le modèle *M*, et cela pour entrainer le modèle à l'aide de la base de données qui est basée sur l'apprentissage approfondie.
7- Le modèle créé est converti vers un modèle compatible *M'* aux utilisateurs mobiles.

8- Le serveur cloud envoie le modèle converti *M'* à l'utilisateur mobile afin que ce dernier puisse l'utiliser pour l'authentification. *C : --> M : (M').*

g) L'étape d'authentification

Le déroulement de ce scénario est comme suit (Figure 3.11) :

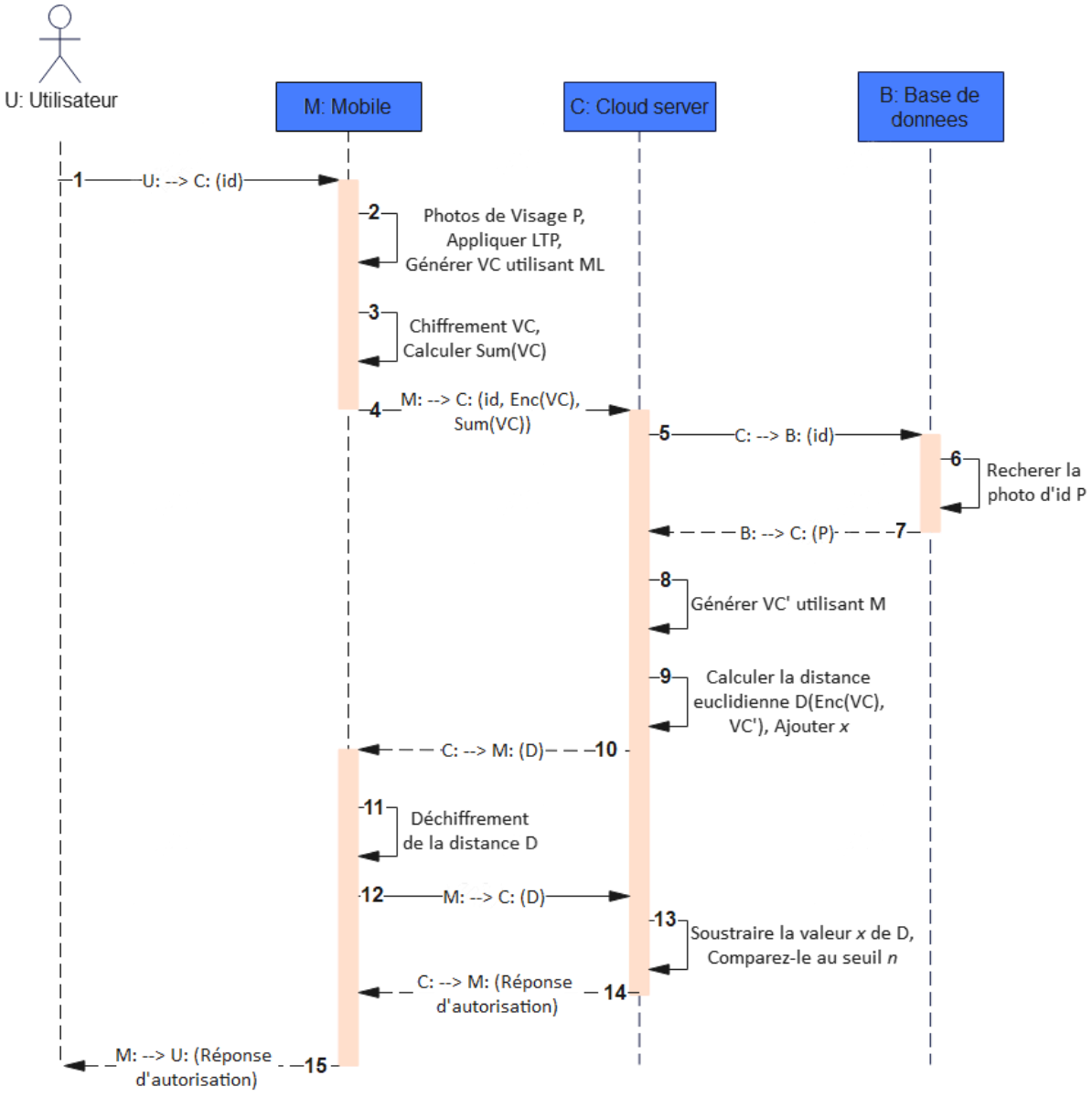

Figure 3.11 Le diagramme séquentiel de la phase d'authentification.

1- L'utilisateur introduit son identifiant *ID* et envoie une demande d'authentification auprès du mobile. *U : --> C : (id).*

2- Le mobile prend une photo du visage de l'utilisateur, après, le processus de traitement de la photo par l'application du LTP est entamé. Une fois le traitement terminé, se fait alors la génération du vecteur de caractéristiques *VC* par l'utilisation du modèle *M'*.
3- L'utilisateur mobile génère la clé publique et la clé privée, puis le *VC* est chiffré par la clé publique. Enfin, le mobile calcule la somme du *VC (sum(VC)).*
4- La requête d'authentification *ID, Enc(VC) et sum(VC)* est transférée vers le serveur cloud.
   M : --> C : (id, Enc(VC), sum(VC)).
5- Le serveur cloud envoie une demande de photo de visage associée à cet *ID. C : --> B : (id).*
6- Obtention de la photo de visage demandée par le serveur cloud.
7- La réponse à la requête de la demande de la photo de visage associée à l'*ID. B : --> C : (P).*
8- Le serveur du cloud traite la photo par l'application du LTP, puis il procédera à la génération du vecteur de caractéristiques *VC'* en utilisant le modèle *M* généré dans la phase d'entrainement.
9- Le processus de calcul de la distance euclidienne *D* entre le *VC* et le *VC'* est activé, le résultat est une valeur chiffrée parce que le *VC* est chiffrée. Afin de protéger cette distance une fois qu'elle serait déchiffrée, on ajoute une valeur *x* à la distance chiffrée.
10- Une requête de déchiffrement de la distance est envoyée à l'utilisateur mobile. *C : --> M : (D).*
11- L'utilisateur mobile déchiffre la distance à l'aide de la clé privée.
12- La réponse au déchiffrement de la distance est envoyée au serveur cloud. *M : --> C : (D).*
13- La soustraction de la valeur ajoutée *x* afin de la comparer au seuil n pour accorder ou non l'autorisation à l'utilisateur.
14- Le serveur cloud envoie la réponse d'authentification au mobile. *C : --> M : (réponse d'autorisation).*
15- La requête de réponse est transférée à l'utilisateur. *M : --> U : (réponse d'autorisation).*

L'évaluation et les tests de ce travail (Zeroual et al., 2021) sont faites avec des données chiffrées et non-chiffrées sur cinq bases de données. Les résultats obtenus sont très satisfaisants.

3.4 Conclusion

L'authentification dans le Mobile Cloud Computing est une tâche importante et complexe. Les chercheurs dans ce domaine ont proposé des solutions pour sécuriser et préserver les données lors de l'authentification. A partir de l'analyse des failles de ces systèmes, nous avons pu suggérer des

solutions comme nous l'avons expliqué précédemment en utilisant l'authentification par la reconnaissance faciale en se basant sur l'apprentissage profond utilisant les réseaux de neurones convolutifs a deux modèles séquentiels.

Ce qui concerne le traitement des images, l'utilisation de LTP s'avère efficace lors de l'entrainement du modèle. Le processus de l'authentification est exécuté sous des données chiffrées à l'aide de chiffrement partiellement homomorphe (PHE) qui s'avère performant et léger (non gourmand). Les résultats obtenus dans ces travaux sont discutés dans le prochain chapitre « expérimentation et discussion ».

Chapitre 4 - Expérimentation et discussion

4.1 Introduction

Pour la validation des solutions proposées, nous avons besoin d'effectuer des évaluations. Dans ce chapitre nous allons présenter les outils et le langage utilisés lors de l'implémentation des modèles proposés, ainsi que les bases de données utilisées. Ensuite, nous allons analyser les résultats obtenus qui seront suivis par une étude comparative avec des solutions précédentes. Pour conclure ce chapitre nous allons synthétiser les résultats obtenus.

4.2 Matériels et logiciels utilisés

Cette section détaillera le matériel et le langage utilisés dans les solutions proposées. L'implémentation des solutions est faite sous Python à l'aide des bibliothèques telles que Keras and Tensorflow pour résoudre les problèmes d'apprentissage automatique à l'aide de techniques modernes d'apprentissage en profondeur. Il fournit des abstractions fondamentales et des blocs de construction pour développer et commercialiser rapidement des applications d'apprentissage automatique. Concernant le côté sécurité, la bibliothèque Python-Paillier est utilisée pour permettre une implémentation d'un système de chiffrement Paillier qui est un système de chiffrement homomorphe à clé publique. Les caractéristiques de la machine utilisée sont : Intel(R) Core (TM) i7-10510U CPU @ 1.80GHz 2.30 GHz et de 12 GB de RAM sous Windows 10.

4.3 Les base de données

Concernant les bases de données, nous avons utilisé dans les deux premières solutions proposées (Zeroual et al., 2019, 2018) la base de donnée de visages FEI et dans le travail (Zeroual et al., 2021) la base de données de visages ORL (The ORL Database of Faces, 2001) , la base de données de visages Yale (The Yale Face Database, 2001), la base de données de visages Extneded Yale (Extended Yale Face Database, 2005), la base de données de visages Georgia Tech (Georgia Tech Face Database, 2000) et la base de données de visages FEI (Thomaz, 2006).

a) Base de données de visages ORL

Cette base contient 40 personnes. Chaque personne possède 10(dix) images de visage comme le montre la Figure 4.1. Les images ont été capturées à différents moments, avec divers éclairages, expressions et structures faciales.

Figure 4.1 Echantillons de la base de données ORL (Zeroual et al., 2021).

b) Base de données de visages Yale

La base de données de visages Yale contient 15(quinze) personnes, chaque personne possède 11(onze) images avec des expressions faciales différentes : heureux, avec et sans lunettes, normal, etc. illustré dans la Figure 4.2.

Figure 4.2 Echantillons de la base de données Yale (Zeroual et al., 2021).

c) Base de données de visages Extneded Yale

Nous avons utilisé une version d'image recadrée de la base de données Extended Yale, qui contient environ 2470 images de visage prises sous 9 poses 64 environnements d'éclairage. Chaque individu a environ 65 images de visage illustrées dans la Figure 4.3.

Figure 4.3 Echantillons de la base de données Extended Yale (Zeroual et al., 2021).

d) Base de données de visages Georgia Tech

La base de données de visages Georgia Tech comprend 750 images de visage de 50 individus, comme le montre la Figure 4.4, chaque individu a 15 images comprenant diverses expressions faciales avec et sans visage incliné.

Figure 4.4 Echantillons de la base de données Georgia Tech (Zeroual et al., 2021).

e) Base de données de visages FEI

La base de données de visages FEI contient 2800 images de visages de 200 personnes. Chaque individu a 14 images de visage. Toutes les images ont été prises à différentes positions avec une échelle différente. La base de données contient 100 hommes et 100 femmes, comme illustré dans la Figure 4.5.

Figure 4.5 Echantillons de la base de données FEI (Zeroual et al., 2021).

4.4 Les résultats obtenus

4.4.1 L'évaluation de la solution 1

Dans ce travail nous avons proposé un modèle d'authentification profond utilisant la reconnaissance faciale biométrique basée sur DeepCNN dans MCC. Le modèle proposé utilise la caméra frontale d'un appareil mobile pour prendre une photo de l'utilisateur et l'envoi au cloud pour le calcul (extraction de caractéristiques à l'aide de DeepCNN). En raison de l'énorme volume de données et des calculs complexes dans l'authentification profond, nous proposons d'allouer le processus de l'entrainement au niveau du cloud.

Au début, toutes les images sont redimensionnées en 28x28 pixels et envoyées dans le cloud. Ensuite, comme nous l'avons mentionné, tout le processus se fait dans le cloud. La base de données est divisée en deux parties, la première contient les images d'entraînement environ 80 % de la base de données (11 images par personne, soit 2200 images pour entrainer notre modèle) et la seconde contient les images de test environ 20 % de la base de données (3 images par personne, soit 600 pour tester notre réseau).

La Figure 4.6 montre la précision et la perte de l'entrainement et de la validation du modèle proposé.

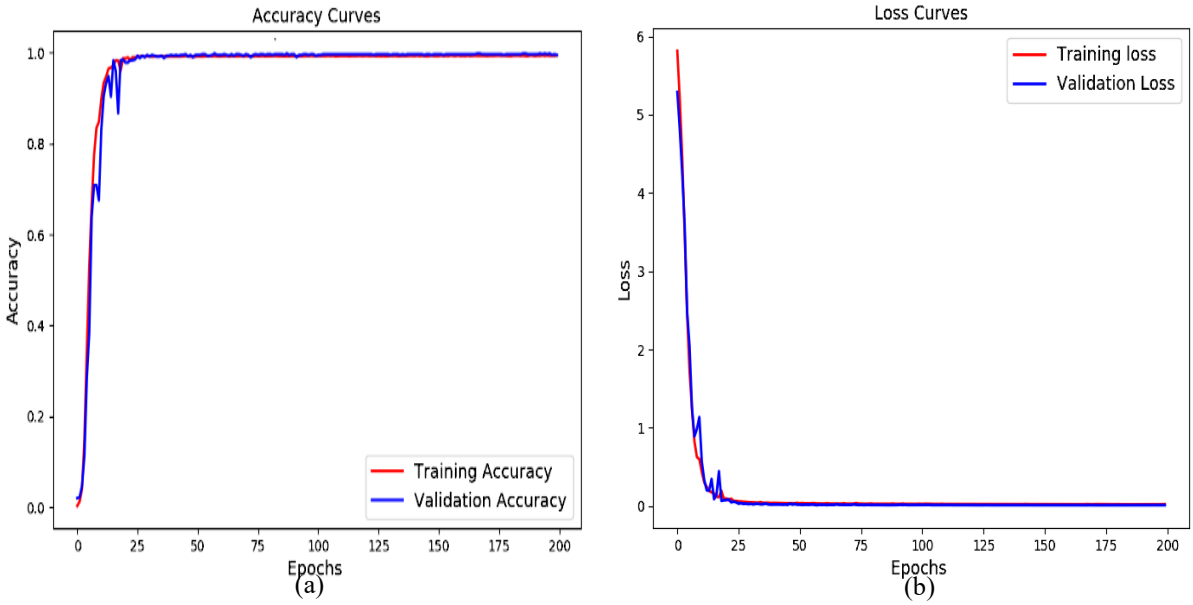

Figure 4.6 (a) La métrique précision du DeepCNN. (b) Loss du DeepCNN (Zeroual et al., 2018).

Après l'entraînement du modèle, nous avons atteint un taux de 99,50 % de précision et un taux de 0,01 % de perte, ce qui est un bon résultat dans une durée égale à 20 minutes et 36 secondes. Nous pouvons obtenir ce résultat en moins de temps sur un cloud en raison de ses ressources puissantes, c'est pourquoi nous ne pouvons pas utiliser d'appareils mobiles, après cela, nous avons testé ce modèle (600 images à tester) pour l'authentification. Nous ajoutons quelques fausses images sur 10 images pour tester si le DeepCNN proposé fonctionne et est performant, la Figure 4.7 présente les performances de classification.

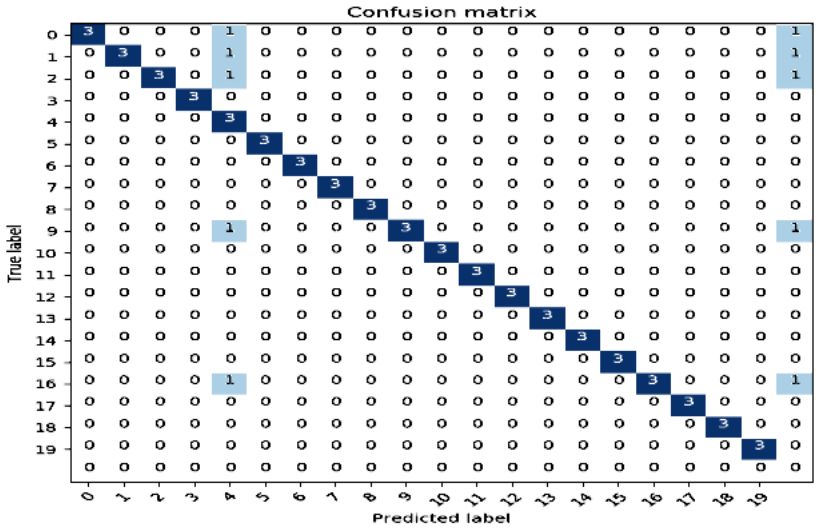

Figure 4.7 Les performances de la classification (Zeroual et al., 2018).

La Figure 4.7 est une partie des données de test, nous devrions avoir 200 classes. En analysant la matrice de confusion, toutes les images correctes sont correctement prédites en lisant cette matrice en diagonale et toutes les images négatives situées en dehors de la diagonale sont prédites incorrectement, dans ce cas, le système rejettera ces personnes et le considéreront comme des imposteurs. C'est ce qui confirme que le DeepCNN proposé fonctionne bien.

4.4.2 L'évaluation de la solution 2

Nous avons proposé dans ce travail d'utiliser l'outil d'apprentissage en profondeur pour mobile "Tensorflow lite" pour faire la reconnaissance sur mobile sans avoir besoin du cloud ou de ressources informatiques et pour éviter que les utilisateurs envoient leurs images à chaque fois.

Plusieurs expérimentations ont été faites sur notre travail basé sur le modèle VggNet pré-entraîné. La première consiste à figer toutes les couches de l'architecture VggNet sauf la dernière. Nous avons obtenu une précision de 99,33 % avec une perte égale à 0,67 % comme indiqué dans la Figure 4.8.

Les Figure 4.9 montre la précision et la perte du modèle VggNet avec les deux dernières couches non gelées. Nous avons atteint un taux de 99,83 % de précision avec une perte égale à 0,17 %. Après cela, toutes les couches sont gelées sauf les trois dernières couches. Le taux de précision et de perte s'est amélioré pour atteindre 100 % de précision et 0 % de perte, comme indiqué dans Figure 4.10.

Pour confirmer le dernier résultat obtenu, nous avons laissé les quatre trois dernières couches sans les figer. Après la phase d'entrainement, nous avons atteint un taux de 100 % de précision avec 0 % de perte comme illustré dans la Figure 4.11. C'est le même résultat obtenu avec trois couches non gelées. De plus, tous les autres paramètres sont les mêmes que ceux utilisés dans le travail qui a été fait dans (Zeroual et al., 2018).

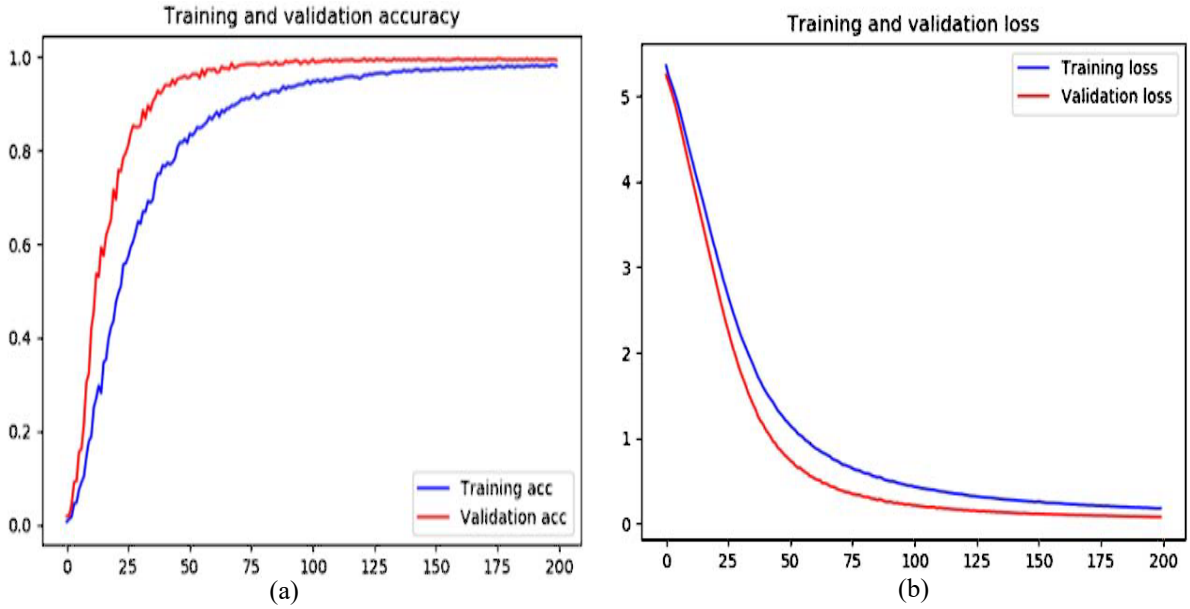

Figure 4.8 (a) La précision de VggNet avec une seule couche non gelée. (b) Loss de VggNet avec une seule couche non gelée (Zeroual et al., 2019).

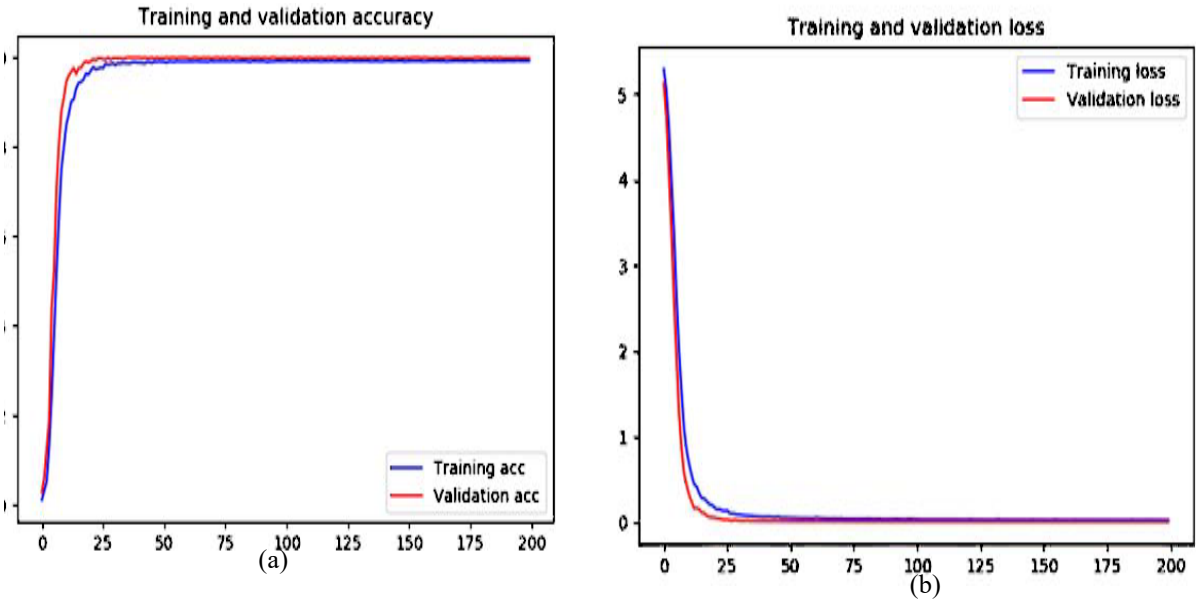

Figure 4.9 (a) La précision de VggNet avec deux couches non gelées. (b) Loss de VggNet avec deux couches non gelées (Zeroual et al., 2019).

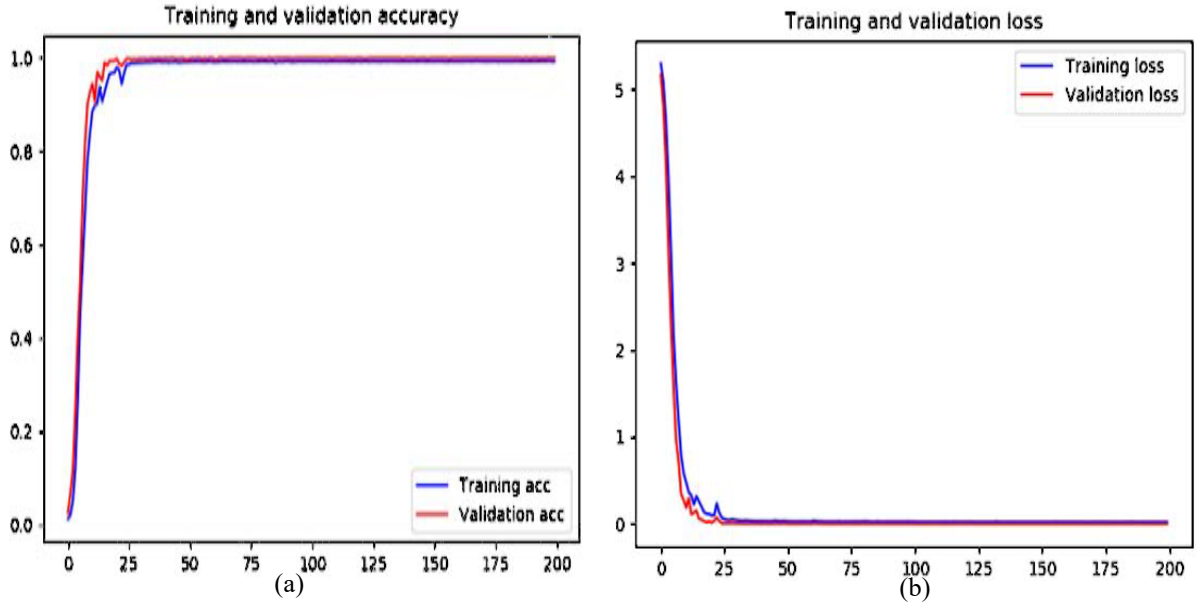

Figure 4.10 (a) La précision de VggNet avec trois couches non gelées. (b) Loss de VggNet avec trois couches non gelées (Zeroual et al., 2019).

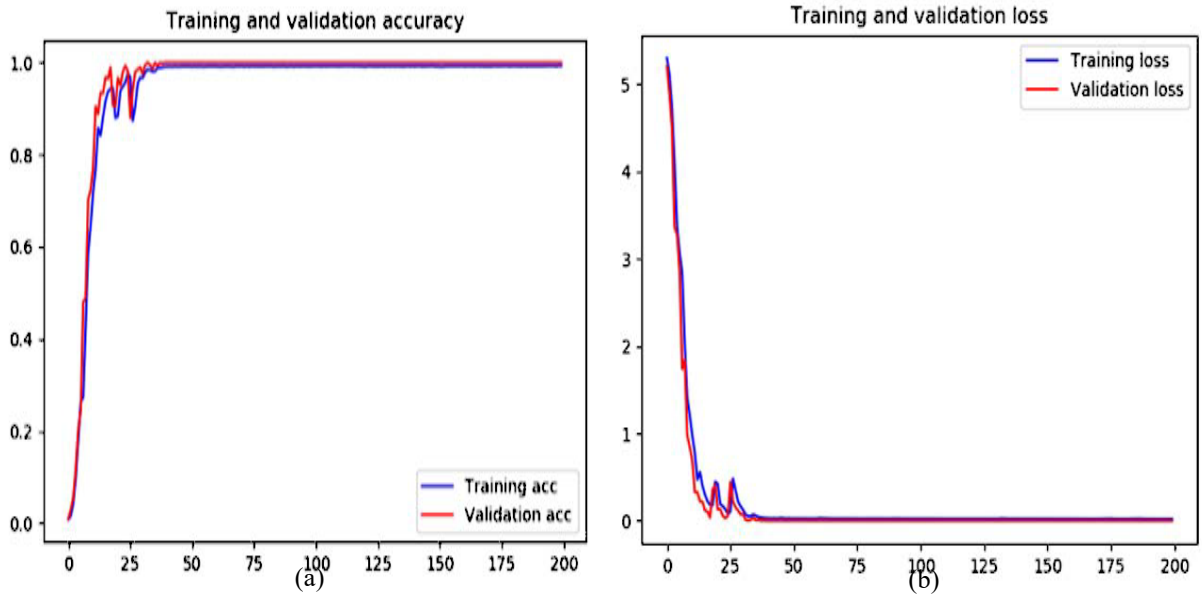

Figure 4.11 (a) La précision de VggNet avec quatre couches non gelées. (b) Loss de VggNet avec quatre couches non gelées (Zeroual et al., 2019).

Le Tableau 4.1 ci-dessous explique et résume les résultats obtenus avec le modèle proposé.

Tableau 4.1 La relation entre couches, précision et temps d'exécution.

Nombre de couches gelées	1	3	4	5
Précision	99.33%	99.83 %	100 %	100 %
Temps d'exécution	4h10m	4 h28m	5h26m	6h36m

D'après les résultats présentés dans le Tableau 4.1, nous pouvons conclure qu'il existe une relation de corrélation directe entre le nombre de couches, la précision et le temps d'exécution.

4.4.3 L'évaluation de la solution 3

L'approche proposée pour l'authentification des utilisateurs dans un environnement Mobile Cloud sous un cryptage homomorphe à l'aide de LTP est testée avec DeepCNN sur cinq ensembles de données

comme suit : The ORL Database of Faces, Yale Face Database, Extended Yale Face database Extended Yale Face database, GeorgiaTech Base de données de visages, base de données de visages FEI.

L'architecture DeepCNN utilisée pour l'extraction de caractéristiques est la même utilisée dans notre travail précédent (Zeroual et al., 2018). Elle contient deux couches convolutives, deux couches de Max-pooling et une couche Flatten chargée de générer les vecteurs de caractéristiques d'un individu. L'architecture se compose également de deux modèles séquentiels, tous les deux symétriques en termes de couches et de paramètres. Toutes les bases de données sont divisées en deux parties, 80 % pour l'entrainement et 20 % pour les tests. Cela signifie que les images de test sont prises en compte à la demande de l'utilisateur. Nous appliquons le classificateur K-Nearest Neighborhood pour compléter le processus de classification. De plus, nous comparons le taux de reconnaissance des tests utilisant DeepCNN, LTP-DeepCNN et l'évaluation sous données chiffrées avec chiffrement homomorphe.

À partir du Tableau 4.2, nous observons que le taux de précision est acceptable sur toutes les bases de données lorsque nous utilisons uniquement DeepCNN avec un seul modèle séquentiel. C'est parce que nous n'avons pas utilisé LTP pour générer les images positives et négatives. En revanche, nous notons que lorsque LTP-DeepCNN est utilisé, le taux de précision surpasse celui de DeepCNN pour quatre des cinq bases de données. Nous notons également que le taux de précision dans la base de données de Yale (The Yale Face Database, 2001) est égal à 93,93 % en utilisant les deux méthodes. Cela est dû à la petite taille de la base de données, qui contient 165 images de visage de 15 individus. La Figure 4.12 illustre la perte de l'entrainement et la précision de tous les ensembles de données. Nos résultats suggèrent que la combinaison de LTP avec DeepCNN avec deux modèles séquentiels donne de meilleurs résultats plutôt que d'utiliser uniquement DeepCNN.

Tableau 4.2 Les metriques pour différents ensembles de données utilisant DeepCNN et LTP-DeepCNN.

Base de données	**LTP-DeepCNN**				**DeepCNN**
	Précision	**Exactitude**	**Rappelle**	**F1-score**	**Précision**
ORL	100%	100%	98.75%	99.37%	97.50%
Yale	93.93%	96.88%	93.93%	95.38%	93.93%
Extended Yale	99.18%	100%	97.97%	98.97%	94.72%
Georgia Tech	99.33%	99.33%	99.33%	99.33%	98.75%
FEI	98.21%	99.82%	96.79%	98.28%	93.39%

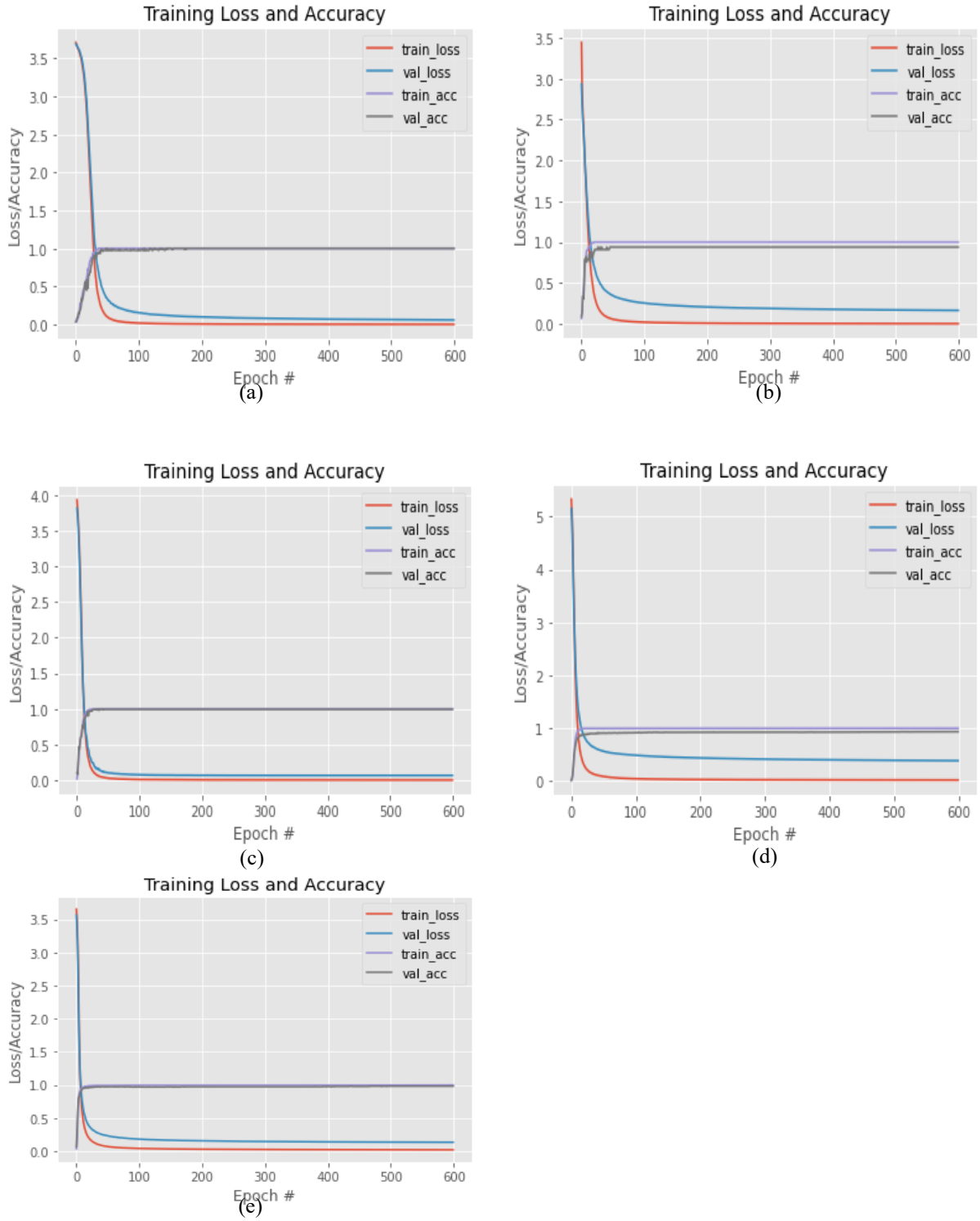

Figure 4.12 Précision, loss, précision de validation et loss de validation à l'aide de LTP-DeepCNN : (a) base de données ORL, (b) base de données Yale, (c) base de données Yale étendue, (d) base de données Georgie Tech, (e) base de données FEI (Zeroual et al., 2021).

Les coûts techniques tels que le temps d'exécution et la consommation de mémoire sont primordiaux car les appareils mobiles disposent de ressources limitées. D'après le Tableau 4.3, nous constatons que le temps de chiffrement du vecteur de caractéristiques avec une taille égale à 512 bits est supérieur au temps de déchiffrement. Le déchiffrement à l'aide de l'algorithme Pailier est plus rapide que RSA. De plus, l'approche proposée ne consomme pas beaucoup de mémoire, ce qui la rend adaptée aux appareils mobiles.

Tableau 4.3 Coûts techniques (Temps et Mémoire).

	Chiffrement	**Déchiffrement**
Durée moyenne (ms)	187.4	2.9
Mémoire (MB)	69.9	61.3
Taille du vecteur (bits)	512	
Temps de reconnaissance (s)	3.12	

L'approche proposée est également évaluée sous des données chiffrées. Tous les vecteurs de caractéristiques de l'utilisateur mobile émis en appliquant le LTP-DeepCNN sont chiffrés et envoyés au serveur d'authentification sur le Cloud pour authentification. Le serveur d'authentification calcule la distance euclidienne sous chiffrement homomorphe et la compare au seuil *n* pour l'autorisation. Nous avons calculé un taux de reconnaissance sous données chiffrées comme indiqué dans le Tableau 4.4 sur toutes les bases de données.

Tableau 4.4 Le taux de reconnaissance sous des données chiffrées.

Bases de données	**Taux de reconnaissance**
ORL	98.75%
Yale	90.90%
Extended Yale	98.78%
Georgia Tech	98.66%
FEI	98.03%

Les résultats font état de taux de précision raisonnables pour toutes les bases de données. On note cependant une petite baisse des taux de précision due au procédé de chiffrement. Cela rend l'approche proposée plus robuste et moins sensible.

4.5 Discussion

Dans cette section nous discuterons les résultats obtenus et cela en les comparant à ceux réalisés lors des travaux antérieurs.

Dans notre travail (Zeroual et al., 2018), Nous avons obtenu un taux de précision qui est égal à 99.50% pendant une durée égale à 20m et 36s. Ces résultats sont significatifs, en utilisant notre propre architecture basée sur le DeepCNN qui a été réalisé à partir de zéro pour s'authentifier au cloud à partir des appareils mobiles à base de reconnaissance faciale. Le problème de cette proposition est que pour chaque authentification, l'utilisateur doit envoyer son image de visage au cloud en clair, ce qui le rend vulnérable.

Cela nous a induit de proposer une autre méthode (Zeroual et al., 2019), qui utilise le système Tensorflow Lite pour que l'utilisateur puisse utiliser le modèle issu de la phase de l'entrainement dans l'appareil mobile sans le besoin d'envoyer l'image de visage en clair. Après plusieurs tentatives d'évaluation nous avons pu améliorer le taux de précision.

Tableau 4.5 La comparaison entre nos travaux.

	(Zeroual et al., 2018)	(Zeroual et al., 2019)
La précision	99.50%	100%
Le temps d'exécution	20m36s	5h26m

Le Tableau 4.5 montre la comparaison entre le modèle proposé (Zeroual et al., 2019) et notre précédent travail (Zeroual et al., 2018). À partir de ce tableau, nous observons que le taux de précision dans (Zeroual et al., 2018) atteint 99,50 % et la précision du modèle proposé atteint 100 %, en raison de la profondeur de VggNet (comme nous l'avons dit précédemment, la contrainte de nombre de couches est responsable des caractéristiques spécifiques). Quant au temps d'exécution, nous remarquons que dans notre travail antérieur, il est inférieur à celui du présent travail. Cette différence est toujours causée par le nombre de couches, mais nous considérons que cette différence n'est pas un problème lorsque nous utilisons le cloud pour l'entrainement en raison de ses puissantes ressources. En peut dire que ce travail surpasse le travail précédent en termes de précision et de sécurité en utilisant VggNet et Tensorflow lite.

D'après l'analyse des insuffisances des travaux précédents cités dans le Tableau 3.1, nous avons suggéré une nouvelle approche qui vise à augmenter le taux de reconnaissance, diminuer le temps d'exécution et préserver les données transmises lors de l'authentification. Les résultats obtenus dans ce travail sont très satisfaisants et sont mentionnés dans le Tableau 4.4 et le Tableau 4.5.

Tableau 4.6 Les précisions de la classification sur différentes bases de données avec CLTP, CLBP et LTP-DeepCNN.

Bases de données	CLBP	CLTP	LTP-DeepCNN
ORL	97.98%	98.52%	100%
Yale	77.20%	80.47%	93.93%
Extended Yale	/	/	99.18%
Georgia Tech	91.40%	91.63%	99.33%
FEI	75.48%	76.38%	98.21%

Le Tableau 4.6 présente nos résultats sur les performances de l'approche proposée par rapport à celles existantes, y compris CLBP et CLTP (Yee et al., 2019). Dans la base de données ORL, la précision obtenue avec LTP-DeepCNN est égale à 100 %, ce qui est supérieur à l'utilisation de CLBP et CLTP. Dans le deuxième ensemble de données de Yale, la précision de classification de 93,93 % a été obtenue dans notre méthode proposée, ce qui est meilleur que CLBP et CLTP. La précision obtenue sur la base de données Georgia Tech est de 99,33%, donc toujours supérieure aux travaux précédents. Enfin, une précision significative obtenue en utilisant LTP DeepCNN sur l de données FEI, qui est de 98,21 %.

De plus, nous avons mené une étude comparative entre notre approche d'authentification LTP-DeepCNN sous chiffrement homomorphe dans un environnement Mobile Cloud et des travaux antérieurs (Hu et al., 2020; Wang et al., 2019). Les résultats sont présentés dans le Tableau 4.7.

Tableau 4.7 La comparaison entre l'approche proposée et les travaux connexes.

Méthodes	Bases de données	Taux reconnaissance	Temps de reconnaissance (s)
(Hu et al., 2020)	ORL	92.50%	9.5
Approche proposée	ORL	98.75%	3.12
(Wang et al., 2019)	Extended Yale	95.44%	/
Approche proposée	Extended Yale	98.78%	/

En analysant ces résultats, on remarque que le taux de reconnaissance, en utilisant l'approche proposée, dépasse le taux de reconnaissance cité dans les travaux (Hu et al., 2020; Wang et al., 2019), concernant le processus de temps de reconnaissance, il est égal à 3,12s, ce qui est supérieur au temps de reconnaissance de (Hu et al., 2020) (9,5 s).

Nous constatons que l'approche proposée fonctionne mieux que les approches connexes.

4.6 Conclusion

Dans ce chapitre nous avons présenté les outils utilisés lors de l'implémentation des solutions proposées, ainsi que les bases de données employées lors des tests effectués pour la validation de notre approche. Ensuite, nous avons présenté les résultats obtenus d'après des évaluations des solutions de notre approche, enfin, une étude comparative entre notre approche et les travaux connexes a montré que les modèles proposés concernant l'authentification dans le Mobile Cloud Computing utilisant la reconnaissance faciale à base de l'apprentissage profond sous des données chiffrées, s'avèrent mieux adapté.

Conclusion générale et perspectives

De nos jours la technologie du Mobile Cloud Computing est devenue presque primordiale, cela est due à la limitation des ressources des appareils mobiles. Cette technologie est la combinaison de deux technologies : le Mobile Computing et le Cloud Computing afin que les utilisateurs mobiles puissent bénéficier des services offerts par le Cloud que ce soit le stockage ou l'exécution des taches lourdes. La croissance des utilisateurs qui utilisent le MCC a créé plusieurs défis tels que la décharge de travail et la sécurité.

Dans cette thèse, on s'est concentré sur l'aspect sécurité, spécialement la confidentialité des données des utilisateurs lors de l'authentification, afin que les utilisateurs mobiles puissent s'authentifier en toute sécurité et protéger ainsi leurs données.

D'après une analyse profonde des travaux connexes, l'intégration de la biométrie dans l'authentification dans l'environnement du MCC nous a motivés pour proposer une approche afin de sécuriser l'authentification au Cloud basé sur la reconnaissance faciale issue de l'apprentissage profond sous des données chiffrées.

Notre contribution est composée de deux parties, la première concernant la reconnaissance faciale à base de l'apprentissage profond, l'autre est une proposition d'utiliser LTP pour le traitement des images faciales de chaque personne deux images (positives et négatives). Puisque chaque utilisateur a deux images de visage après l'application du LTP. Cela aussi nous a motivés à proposer une architecture de réseau de neurones convolutifs profonds avec deux modèle séquentiels, le premier est pour l'image positive et le deuxième pour l'image négative, combinée en parallèle à la dernière couche pour mieux extraire les caractéristiques de l'image. Cela nous a menés à un taux de précision plus élevé lors de l'entrainement comparé aux autres méthodes tels que CLBP, CLTP, LBP sur cinq bases de données. L'utilisation du framework Tensorflow Lite nous a permis d'utiliser le modèle issu de la phase d'entrainement dans les appareils mobiles. Son entrainement est localisé au niveau Cloud.

La deuxième partie concerne la phase d'authentification. L'utilisateur mobile utilise le modèle converti pour extraire le vecteur de caractéristiques. Ensuite, ce vecteur est chiffré avec la méthode de chiffrement partiellement homomorphe (PHE) pour préserver la confidentialité des données des utilisateurs, puis il est envoyé au cloud afin de s'authentifie au Cloud et cela en le comparant au vecteur

chiffré avec le vecteur clair situé au cloud en se basant sur la distance euclidienne sous des données chiffrées qui autorisent ou non l'accès au cloud.

L'étude comparative nous a permis de valider notre contribution. Cette comparaison a révélé un taux de précision remarquable amélioré qui dépasse les propositions antérieures avec un temps d'exécution inférieur des temps des modèles antérieurs proposés.

Perspectives

Dans ce travail nous avons traité l'une des facettes de la sécurité, le travail proposé traitera l'authentification faciale à base de l'apprentissage profond en utilisant les réseaux de neurones convolutifs (CNN) sous des données chiffrées. Lors de l'authentification dans le cloud, ce dernier n'a aucune information sur l'utilisateur car les données sont chiffrées. Grâce au chiffrement homomorphe, le cloud peut faire des opérations sur ses données chiffrées sans avoir besoin de les déchiffrer. Les résultats obtenus sont significatifs.

Pour améliorer l'approche proposée, nous suggérons d'utiliser dans les futurs travaux, Generative Adversarial Network (GAN) au lieu des CNNs, et cela pour éviter les attaques de Fake Images. Le principe de GAN est de détecter les images fakes qui peuvent être utilisées pour accéder au système par des imposteur.

D'autre part, l'apparition du *Blockchain* et son utilisation dans nombreux domaines nous a permettre de penser à l'intégrer dans l'environnement du Mobile Cloud avec les techniques de l'apprentissage automatique pour mieux sécuriser notre système d'une manière efficace et spécialement pour protéger le système contre l'attaque *man in the middle*.

Production scientifique

- Zeroual, A., Amroune, M., Derdour, M., & Bentahar, A. (2021). Lightweight deep learning model to secure authentication in Mobile Cloud Computing. In Journal of King Saud University - Computer and Information Sciences. Elsevier BV. https://doi.org/10.1016/j.jksuci.2021.09.016.
- Zeroual, A., Amroune, M., Derdour, M., Meraoumia, A., & Bentahar, A. (2018). Deep authentication model in Mobile Cloud Computing. In 2018 3rd International Conference on Pattern Analysis and Intelligent Systems (PAIS). https://doi.org/10.1109/pais.2018.8598508.
- Zeroual, A., Derdour, M., Amroune, M., & Bentahar, A. (2019). Using a Fine-Tuning Method for a Deep Authentication in Mobile Cloud Computing Based on Tensorflow Lite Framework. In 2019 International Conference on Networking and Advanced Systems (ICNAS). https://doi.org/10.1109/icnas.2019.8807440.
- Bentahar, A., Meraoumia, A., Bendjenna, H., Chitroub, S., & Zeroual, A. (2019). Biometric Cryptosystems: Towards a Light and Precise Remote Authentication. In Recent Advances in Computer Science and Communications (Vol. 13). Bentham Science Publishers Ltd. https://doi.org/10.2174/2666255813666191223115223.
- Bentahar, A., Meraoumia, A., Bendjenna, H., & Zeroual, A. (2018). IoT Securing System using Fuzzy Commitment for DCT-based Fingerprint Recognition. In 2018 3rd International Conference on Pattern Analysis and Intelligent Systems (PAIS). IEEE. https://doi.org/10.1109/pais.2018.8598511.
- Bentahar, A., Meraoumia, A., Bendjenna, H., Chitroub, S., & Zeroual, A. (2018). Biometric Cryptosystem Scheme for Internet of Things using Fuzzy Commitment principle. In 2018 International Conference on Signal, Image, Vision and their Applications (SIVA). IEEE. https://doi.org/10.1109/siva.2018.8660993.
- Bentahar, A., Meraoumia, A., Bendjenna, H., Chitroub, S., & Zeroual, A. (2019).Securing Remote Authentication Using Fuzzy Commitment and Fuzzy Vault International Conference on Pattern Analysis and Recognition 2019-10 (ICPAR 2019). https://icpar2019.sciencesconf.org/.

- Bentahar, A., Meraoumia, A., Bendjenna, H., Chitroub, S., & Zeroual, A. (2020). Fuzzy ExtractorBased Key Agreement for Internet of Things. In 020 1st International Conference on Communications, Control Systems and Signal Processing (CCSSP). IEEE. https://doi.org/10.1109/ccssp49278.2020.9151574.
- Bentahar, A., Meraoumia, A., Bendjenna, H., Chitroub, S., & Zeroual, A. (2021). EigenFingerprints-Based Remote Authentication Cryptosystem. In 2021 International Conference on Recent Advances in Mathematics and Informatics (ICRAMI). IEEE. https://doi.org/10.1109/icrami52622.2021.9585979.

Activités scientifiques

- Programme Nationale Exceptionnel (PNE) au Royaume-Uni 2019/2020.

Bibliographie

Fan, X., Cao, J., & Mao, H. 2011. A survey of mobile cloud computing. *zTE Communications*, *9*(1), 4-8.

Ackley, D.H., Hinton, G.E., Sejnowski, T.J., 1985. A learning algorithm for boltzmann machines. Cogn. Sci. 9, 147–169. https://doi.org/10.1016/S0364-0213(85)80012-4

Al Rassan, I., Alshaher, H., 2014. Securing Mobile Cloud Computing Using Biometric Authentication (SMCBA). Proc. - 2014 Int. Conf. Comput. Sci. Comput. Intell. CSCI 2014 1, 157–161. https://doi.org/10.1109/CSCI.2014.33

Ali, H., 2020. Epc Aware Cloud computing.

Amin, M.A., Bakar, K.B.A., Al-Hashimi, H., 2013. A review of mobile cloud computing architecture and challenges to enterprise users. 2013 7th IEEE GCC Conf. Exhib. GCC 2013 240–244. https://doi.org/10.1109/IEEEGCC.2013.6705783

Andersen-Hoppe, E., Rathgeb, C., Busch, C., 2017. Combining multiple iris texture features for unconstrained recognition in visible wavelengths. Proc. - 2017 5th Int. Work. Biometrics Forensics, IWBF 2017. https://doi.org/10.1109/IWBF.2017.7935090

Anthony, G., Greg, H., Tshilidzi, M., 2007. Classification of Images Using Support Vector Machines.

Arel, I., Rose, D., Karnowski, T., 2010. Deep machine learning-A new frontier in artificial intelligence research. IEEE Comput. Intell. Mag. 5, 13–18. https://doi.org/10.1109/MCI.2010.938364

Arulkumaran, K., Deisenroth, M.P., Brundage, M., Bharath, A.A., 2017. Deep reinforcement learning: A brief survey. IEEE Signal Process. Mag. 34, 26–38. https://doi.org/10.1109/MSP.2017.2743240

Attneave, F., B., M., Hebb, D.O., 1950. The Organization of Behavior; A Neuropsychological Theory. Am. J. Psychol. 63, 633. https://doi.org/10.2307/1418888

Barca, C., Barca, C., Cucu, C., Gavriloaia, M.R., Vizireanu, R., Fratu, O. and Halunga, S., 2016, June. A virtual cloud computing provider for mobile devices. In *2016 8th International Conference on*

Electronics, Computers and Artificial Intelligence (ECAI) (pp. 1-4). IEEE.. https://doi.org/10.1109/ECAI.2016.7861184

Berg, E.J., 1929. Heaviside's Operational Calculus as Applied to Engineering and Physics. University of California: McGraw-Hill book Company.

Bifulco, R., Brunner, M., Canonico, R., Mir, F., 2012. Scalability of a Mobile Cloud Management System. Proc. first Ed. MCC Work. Mob. cloud Comput. - MCC '12. https://doi.org/10.1145/2342509

Bishop, C.M., 2013. Pattern recognition and machine learning. Springer, New York.

Borchani, H., Varando, G., Bielza, C., Larrañaga, P., 2015. A survey on multi-output regression. Wiley Interdiscip. Rev. Data Min. Knowl. Discov. 5, 216–233. https://doi.org/10.1002/WIDM.1157

Bowyer, K., Ortiz, E., 2015. Iris recognition: does template ageing really exist? Biometric Technol. Today 2015, 5–8. https://doi.org/10.1016/S0969-4765(15)30156-9

Bowyer, K.W., Hollingsworth, K., Flynn, P.J., 2008. Image understanding for iris biometrics: A survey. Comput. Vis. Image Underst. 110, 281–307. https://doi.org/10.1016/J.CVIU.2007.08.005

Brown, N., Sandholm, T., 2019. Superhuman AI for multiplayer poker. Science (80-.). 365, 885–890. https://doi.org/10.1126/SCIENCE.AAY2400/SUPPL_FILE/AAY2400_DATA_FILE_S1.ZIP

Brownlee, J., 2018. Better deep learning: train faster, reduce overfitting, and make better predictions. Machine Learning Mastery.

Brownlee, J., 2016. Supervised and Unsupervised Machine Learning Algorithms Understand Mach. Learn. Algorithms.

Chang, R.S., Gao, J., Gruhn, V., He, J., Roussos, G., Tsai, W.T., 2013. Mobile cloud computing research - Issues, challenges, and needs. Proc. - 2013 IEEE 7th Int. Symp. Serv. Syst. Eng. SOSE 2013 442–453. https://doi.org/10.1109/SOSE.2013.96

Chang, T.K., 2014. A secure operational model for mobile payments. Sci. World J. 2014. https://doi.org/10.1155/2014/626243

Chih-Ching, H., Chin-Hsing, K., Daisuke, M., Yukio, T., 2019. Advances in Mechanism and Machine

Science 73, 1491–1498. https://doi.org/10.1007/978-3-030-20131-9

Chow, R., Jakobsson, M., Masuoka, R., Molina, J., Niu, Y., Shi, E., Song, Z., 2010. Authentication in the clouds: A framework and its application to mobile users. Proc. ACM Conf. Comput. Commun. Secur. 1–6. https://doi.org/10.1145/1866835.1866837

Climent, J., Hexsel, R.A., 2012. IRIS RECOGNITION USING ADABOOST AND LEVENSHTEIN DISTANCES. http://dx.doi.org/10.1142/S0218001412660012 26. https://doi.org/10.1142/S0218001412660012

CUDA Spotlight: GPU-Accelerated Deep Neural Networks | NVIDIA Developer Blog, 2014. URL https://developer.nvidia.com/blog/cuda-spotlight-gpu-accelerated-deep-neural-networks/

Dai, W., Chen, H., Wang, W., Chen, X., 2013. RMORM: A framework of multi-objective optimization resource management in clouds. Proc. - 2013 IEEE 9th World Congr. Serv. Serv. 2013 488–494. https://doi.org/10.1109/SERVICES.2013.85

Daugman, J., 2016. Information theory and the iriscode. IEEE Trans. Inf. Forensics Secur. 11, 400–409. https://doi.org/10.1109/TIFS.2015.2500196

Daugman, J., Downing, C., 2016. Searching for doppelgängers: Assessing the universality of the IrisCode impostors distribution. IET Biometrics 5, 65–75. https://doi.org/10.1049/IET-BMT.2015.0071

De, D., 2016. Mobile cloud computing: architectures, algorithms and applications. CRC Press.

De Silva, V., Roche, J., Kondoz, A., 2018. Robust fusion of LiDAR and wide-angle camera data for autonomous mobile robots. Sensors 18, 2730.

Derawi, M.O., Yang, B., Busch, C., 2011. Fingerprint recognition with embedded cameras on mobile phones, in: International Conference on Security and Privacy in Mobile Information and Communication Systems. Springer, pp. 136–147.

Dinh, H.T., Lee, C., Niyato, D., Wang, P., 2013. A survey of mobile cloud computing: Architecture, applications, and approaches. Wirel. Commun. Mob. Comput. 13, 1587–1611. https://doi.org/10.1002/WCM.1203

Donald, A.C., Arockiam, L., 2014. Securing Data with Authentication in Mobile Cloud Environment: Methods, Models and Issues. Int. J. Comput. Appl. 94.

ElGamal, T., 1985. A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Trans. Inf. theory 31, 469–472.

Extended Yale Face Database, 2005. No Title.

Fernando, N., Loke, S.W., Rahayu, W., 2013. Mobile cloud computing: A survey. Futur. Gener. Comput. Syst. 29, 84–106. https://doi.org/10.1016/J.FUTURE.2012.05.023

Gai, K., Li, S., 2012. Towards cloud computing: A literature review on cloud computing and its development trends. Proc. - 2012 4th Int. Conf. Multimed. Secur. MINES 2012 142–146. https://doi.org/10.1109/MINES.2012.240

Gai, K., Qiu, L., Zhao, H., Qiu, M., 2020. Cost-Aware Multimedia Data Allocation for Heterogeneous Memory Using Genetic Algorithm in Cloud Computing. IEEE Trans. Cloud Comput. 8, 1212–1222. https://doi.org/10.1109/TCC.2016.2594172

Gai, K., Qiu, M., Sun, X., 2018. A survey on FinTech. J. Netw. Comput. Appl. 103, 262–273. https://doi.org/10.1016/J.JNCA.2017.10.011

Gai, K., Qiu, M., Zhao, H., Tao, L., Zong, Z., 2016. Dynamic energy-aware cloudlet-based mobile cloud computing model for green computing. J. Netw. Comput. Appl. 59, 46–54. https://doi.org/10.1016/J.JNCA.2015.05.016

Ge, Y., Zhang, Y., Qiu, Q., Lu, Y.H., 2012. A game theoretic resource allocation for overall energy minimization in mobile cloud computing system. Proc. Int. Symp. Low Power Electron. Des. 279–284. https://doi.org/10.1145/2333660.2333724

Gentry, C., 2009. Fully homomorphic encryption using ideal lattices, in: Proceedings of the Forty-First Annual ACM Symposium on Theory of Computing. pp. 169–178.

Georgia Tech Face Database, 2000. No Title.

Géron, A., 2017. Hands-on machine learning with scikit-learn and tensorflow: Concepts. Tools, Tech. to build Intell. Syst.

Ghatak, A., 2017. Machine Learning with R. Mach. Learn. with R 1–210. https://doi.org/10.1007/978-981-10-6808-9

Gonzalez, R.C., Woods, R.E., Masters, B.R., 2009. Digital image processing.

Graves, A., 2012. Supervised Sequence Labelling with Recurrent Neural Networks. Studies in Computational Intelligence 385. https://doi.org/10.1007/978-3-642-24797-2

Grother, P.J., Matey, J.R., Tabassi, E., Quinn, G.W., Chumakov, M., 2013. IREX VI - Temporal Stability of Iris Recognition Accuracy. https://doi.org/10.6028/NIST.IR.7948

Grzonkowski, S., Corcoran, P.M., Coughlin, T., 2011. Security analysis of authentication protocols for next-generation mobile and CE cloud services. Dig. Tech. Pap. - IEEE Int. Conf. Consum. Electron. 83–87. https://doi.org/10.1109/ICCE-BERLIN.2011.6031855

Hahnloser, R.H.R., Sarpeshkar, R., Mahowald, M.A., Douglas, R.J., Seung, H.S., 2000. Digital selection and analogue amplification coexist in a cortex-inspired silicon circuit. Nature 405, 947–951.

He, K., Zhang, X., Ren, S., Sun, J., 2016. Deep residual learning for image recognition. Proc. IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit. 2016-December, 770–778. https://doi.org/10.1109/CVPR.2016.90

Heaton, J., 2015. Artificial intelligence for humans. Incorporated.

Hemanth, D.J., Estrela, V.V., 2017. Deep learning for image processing applications. IOS Press.

Hewitt, C., Amanatidis, T., Politis, I., Sarkar, A., 2019. Assessing public perception of self-driving cars: The autonomous vehicle acceptance model. Int. Conf. Intell. User Interfaces, Proc. IUI Part F147615, 518–527. https://doi.org/10.1145/3301275.3302268

Hinton, G., Sejnowski, T., 1999. Unsupervised learning: foundations of neural computation.

Hinton, G.E., Osindero, S., Teh, Y.-W., 2006. A fast learning algorithm for deep belief nets. Neural Comput. 18, 1527–1554.

Hsueh, S.C., Lin, J.Y., Lin, M.Y., 2011. Secure cloud storage for convenient data archive of smart phones. Proc. Int. Symp. Consum. Electron. ISCE 156–161.

https://doi.org/10.1109/ISCE.2011.5973804

Hu, J., Li, J., Nawaz, S.A., Lin, Q., 2020. Research on Encrypted Face Recognition Algorithm Based on New Combined Chaotic Map and Neural Network, in: Innovation in Medicine and Healthcare. Springer, pp. 105–115. https://doi.org/10.1007/978-981-15-5852-8_10

Huang, D., Zhou, Z., Xu, L., Xing, T., Zhong, Y., 2011. Secure data processing framework for mobile cloud computing. 2011 IEEE Conf. Comput. Commun. Work. INFOCOM WKSHPS 2011 614–618. https://doi.org/10.1109/INFCOMW.2011.5928886

Huerta-Canepa, G., Lee, D., 2010. A virtual cloud computing provider for mobile devices. Proc. 1st ACM Work. Mob. Cloud Comput. Serv. Soc. Networks Beyond, MCS'10, Co-located with ACM MobiSys 2010. https://doi.org/10.1145/1810931.1810937

Iliadis, L., Papadopoulos, H., Jayne, C., 2013. Engineering applications of neural networks: 14th International Conference, EANN 2013 Halkidiki, Greece, September 13-16, 2013 Proceedings, Part I. Commun. Comput. Inf. Sci. 383 CCIS. https://doi.org/10.1007/978-3-642-41013-0

Jager, T., 2012. The generic composite residuosity problem, in: Black-Box Models of Computation in Cryptology. Springer, pp. 49–56.

Jain, A.K., Ross, A.A., Nandakumar, K., 2011. Introduction to Biometrics. Introd. to Biometrics. https://doi.org/10.1007/978-0-387-77326-1

Judd, J.S., 1990. Neural Network Design and the Complexity of Learning. Neural Netw. Des. Complex. Learn. https://doi.org/10.7551/MITPRESS/4932.001.0001

Kakaletsis, E., Tzelepi, M., Kaplanoglou, P.I., Symeonidis, C., Nikolaidis, N., Tefas, A., Pitas, I., 2019. Semantic Map Annotation Through UAV Video Analysis Using Deep Learning Models in ROS. Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics) 11296 LNCS, 328–340. https://doi.org/10.1007/978-3-030-05716-9_27

Kalra, N., Paddock, S.M., 2016. Driving to safety: How many miles of driving would it take to demonstrate autonomous vehicle reliability? Transp. Res. Part A Policy Pract. 94, 182–193. https://doi.org/10.1016/J.TRA.2016.09.010

Kamath, U., Choppella, K., n.d. Mastering Java machine learning : mastering and implementing

advanced techniques in machine learning.

Kilinc, C., Booth, T., Andersson, K., 2012. Walldroid: Cloud assisted virtualized application specific firewalls for the android os, in: 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications. IEEE, pp. 877–883.

Kiumarsi, B., Vamvoudakis, K.G., Modares, H., Lewis, F.L., 2018. Optimal and Autonomous Control Using Reinforcement Learning: A Survey. IEEE Trans. Neural Networks Learn. Syst. 29, 2042–2062. https://doi.org/10.1109/TNNLS.2017.2773458

Kotevska, O., Lbath, A., Bouzefrane, S., 2016. Toward a real-time framework in cloudlet-based architecture. Tsinghua Sci. Technol. 21, 80–88. https://doi.org/10.1109/TST.2016.7399285

Kothari, S.C., Oh, H., 1993. Neural Networks for Pattern Recognition. Adv. Comput. 37, 119–166. https://doi.org/10.1016/S0065-2458(08)60404-0

KRONFELD, P.C., 1962. The Gross Anatomy and Embryology of the Eye. Veg. Physiol. Biochem. 1–62. https://doi.org/10.1016/B978-1-4832-3090-0.50007-1

Kumar, A., Pilli, E.S., 2012. University wide M-learning using cloud environment. Proc. - 2012 Int. Symp. Cloud Serv. Comput. ISCOS 2012 118–123. https://doi.org/10.1109/ISCOS.2012.26

Kumar, D.R., ManjupPriya, S., 2014. Cloud based M-Healthcare emergency using SPOC. 2013 5th Int. Conf. Adv. Comput. ICoAC 2013 286–292. https://doi.org/10.1109/ICOAC.2013.6921965

Kurzweil, R., Jaroch, D., 1992. The age of intelligent machines. Viking.

LeCun, Y., Bengio, Y., Hinton, G., 2015. Deep learning. Nature 521, 436–444.

LeCun, Y., Bottou, L., Bengio, Y., Haffner, P., 1998. Gradient-based learning applied to document recognition. Proc. IEEE 86, 2278–2323. https://doi.org/10.1109/5.726791

Lee, J., 2017. A survey of robot learning from demonstrations for Human-Robot Collaboration.

Lewis, G., Echeverría, S., Simanta, S., Bradshaw, B., Root, J., 2014. Tactical cloudlets: Moving cloud computing to the edge. Proc. - IEEE Mil. Commun. Conf. MILCOM 1440–1446. https://doi.org/10.1109/MILCOM.2014.238

Li, H., Sun, L., Zhu, H., Lu, X., Cheng, X., 2014. Achieving privacy preservation in WiFi fingerprint-

based localization. Proc. - IEEE INFOCOM 2337–2345. https://doi.org/10.1109/INFOCOM.2014.6848178

Li, X., Autran, G., 2009. Implementing an mobile agent platform for M-commerce. Proc. - Int. Comput. Softw. Appl. Conf. 2, 40–45. https://doi.org/10.1109/COMPSAC.2009.112

Liu, D., Zhang, H., Polycarpou, M., Alippi, C., He, H., 2011. Advances in Neural Networks--ISNN 2011: 8th International Symposium on Neural Networks, ISNN 2011, Guilin, China, May 29--June 1, 2011, Prodceedings. Springer Science & Business Media.

Liu, H., Wang, L., 2018. Gesture recognition for human-robot collaboration: A review. Int. J. Ind. Ergon. 68, 355–367. https://doi.org/10.1016/J.ERGON.2017.02.004

Luong, A., Gerbush, M., Waters, B., Grauman, K., 2013. Reconstructing a fragmented face from a cryptographic identification protocol, in: 2013 IEEE Workshop on Applications of Computer Vision (WACV). IEEE, pp. 238–245. https://doi.org/10.1109/WACV.2013.6475024

Ma, Y., Wu, L., Gu, X., He, J., Yang, Z., 2017. A Secure Face-Verification Scheme Based on Homomorphic Encryption and Deep Neural Networks. IEEE Access 5, 16532–16538. https://doi.org/10.1109/ACCESS.2017.2737544

Maio, D., Maltoni, D., Cappelli, R., Wayman, J.L., Jain, A.K., 2002. FVC2002: Second fingerprint verification competition. Proc. - Int. Conf. Pattern Recognit. 16, 811–814. https://doi.org/10.1109/ICPR.2002.1048144

Marr, D., 1970. A theory for cerebral neocortex. Proc. R. Soc. London. Ser. B. Biol. Sci. 176, 161–234. https://doi.org/10.1098/RSPB.1970.0040

Matin, A., Mahmud, F., Zuhori, S.T., Sen, B., 2017. Human iris as a biometric for identity verification. ICECTE 2016 - 2nd Int. Conf. Electr. Comput. Telecommun. Eng. https://doi.org/10.1109/ICECTE.2016.7879610

McCulloch, W.S., Pitts, W., 1943. A logical calculus of the ideas immanent in nervous activity. Bull. Math. Biophys. 5, 115–133.

Michels, J., Saxena, A., Ng, A.Y., 2005. High speed obstacle avoidance using monocular vision and reinforcement learning, in: Proceedings of the 22nd International Conference on Machine

Learning. pp. 593–600.

Mohiuddin, K., Islam, A., Alam, A., Ali, A., 2012. 24X7X365: Mobile cloud access. ACM Int. Conf. Proceeding Ser. 544–551. https://doi.org/10.1145/2381716.2381820

Mousavi, S.S., Schukat, M., Howley, E., 2016. Deep Reinforcement Learning: An Overview. Lect. Notes Networks Syst. 16, 426–440. https://doi.org/10.1007/978-3-319-56991-8_32

Muganda, L., Standley, E., 2009. Automated Cars Prophesied by William Branham. Xulon Press, Incorporated.

Muller, U., Ben, J., Cosatto, E., Flepp, B., Cun, Y.L., 2006. Off-road obstacle avoidance through end-to-end learning, in: Advances in Neural Information Processing Systems. Citeseer, pp. 739–746.

Nader, R., 2011. Unsafe at any speed: the designed-in dangers of the American automobile. 1965. Am. J. Public Health 101, 254–256. https://doi.org/10.2105/AJPH.101.2.254

Nassar, M., Wehbe, N., Bouna, B. Al, 2016. K-NN Classification under Homomorphic Encryption: Application on a Labeled Eigen Faces Dataset, in: 2016 IEEE Intl Conference on Computational Science and Engineering (CSE) and IEEE Intl Conference on Embedded and Ubiquitous Computing (EUC) and 15th Intl Symposium on Distributed Computing and Applications for Business Engineering (DCABES). IEEE, pp. 546–552. https://doi.org/10.1109/CSE-EUC-DCABES.2016.239

Nath, R., 2009. Philosophy of artificial intelligence : a critique of the mechanistic theory of mind. Universal-Publishers.

Nielsen, M.A., 2015. Neural Networks and Deep Learning. Determination Press.

Ojha, V.K., Abraham, A., Snášel, V., 2017. Metaheuristic design of feedforward neural networks: A review of two decades of research. Eng. Appl. Artif. Intell. 60, 97–116.

Osadchy, M., Pinkas, B., Jarrous, A., Moskovich, B., 2010. SCiFI - A System for Secure Face Identification, in: 2010 IEEE Symposium on Security and Privacy. IEEE, pp. 239–254. https://doi.org/10.1109/SP.2010.39

Paillier, P., 1999. Public-Key Cryptosystems Based on Composite Degree Residuosity Classes, in:

Advances in Cryptology — EUROCRYPT '99. Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 223–238. https://doi.org/10.1007/3-540-48910-X_16

Pan, S.J., Yang, Q., 2009. A survey on transfer learning. IEEE Trans. Knowl. Data Eng. 22, 1345–1359.

Patterson, J., Gibson, A., 2017. Deep learning: A practitioner's approach. " O'Reilly Media, Inc."

Pavlus, J., 2016. Computers Now Recognize Patterns Better Than Humans Can. Sci. Am.

Picek, R., Grcic, M., 2013. Evaluation of the potential use of m-learning in higher education. Proc. Int. Conf. Inf. Technol. Interfaces, ITI 63–68. https://doi.org/10.2498/ITI.2013.0583

Planche, B., Andres, E., Safari, an O.M.C., 2019. Hands-On Computer Vision with TensorFlow 2. Pucket Publisher.

Poonguzhal, N., Ezhilarasa, M., 2015. Identification Based on Iris Geometric Features. J. Appl. Sci. 15, 792–799. https://doi.org/10.3923/JAS.2015.792.799

Qiu, M., Ming, Z., Li, J., Gai, K., Zong, Z., 2015. Phase-Change Memory Optimization for Green Cloud with Genetic Algorithm. IEEE Trans. Comput. 64, 3528–3540. https://doi.org/10.1109/TC.2015.2409857

Rapaka, S., Kumar, P.R., 2018. Efficient approach for non-ideal iris segmentation using improved particle swarm optimisation-based multilevel thresholding and geodesic active contours. IET Image Process. 12, 1721–1729. https://doi.org/10.1049/IET-IPR.2016.0917

Rivest, R.L., Adleman, L., Dertouzos, M.L., 1978. On data banks and privacy homomorphisms. Found. Secur. Comput. 4, 169–180.

Roche, J., 2020. Multimodal machine learning for intelligent mobility. Loughborough University. https://doi.org/10.26174/THESIS.LBORO.12245483.V1

Romanuke, V. V, 2017. Appropriate Number of Standard 2× 2 Max Pooling Layers and Their Allocation in Convolutional Neural Networks for Diverse and Heterogeneous Datasets. Inf. Technol. Manag. Sci. 20.

Rosenblatt, F., 1959. A probabilistic model for visual perception. Acta Psychol. (Amst). 15, 296–297.

Rosenblatt, F., 1958. The Design of an Intelligent Automaton. U.S. Off. Nav. Res. 6, 7.

Sahib, S.M., Sri, P., Sahib, M., 2014. Perspectives of Mobile Cloud Computing: Architecture, Applications and Issues. Int. J. Comput. Appl. 101, 975–8887.

Samuel, A.L., 1959. Some Studies in Machine Learning Using the Game of Checkers. IBM J. Res. Dev. 3, 210–229. https://doi.org/10.1147/RD.33.0210

Satyanarayanan, M., Bahl, P., Cáceres, R., Davies, N., 2009. The case for VM-based cloudlets in mobile computing. IEEE Pervasive Comput. 8, 14–23. https://doi.org/10.1109/MPRV.2009.82

Scherer, D., Müller, A., Behnke, S., 2010. Evaluation of pooling operations in convolutional architectures for object recognition, in: International Conference on Artificial Neural Networks. Springer, pp. 92–101.

Schmidhuber, J., 2015. Deep learning in neural networks: An overview. Neural Networks 61, 85–117. https://doi.org/10.1016/J.NEUNET.2014.09.003

Schmohl, R., Baumgarten, U., 2008. A generalized context-aware architecture in heterogeneous mobile computing environments. Proc. - 4th Int. Conf. Wirel. Mob. Commun. ICWMC 2008 118–124. https://doi.org/10.1109/ICWMC.2008.59

Seneviratne, S., Seneviratne, A., Mohapatra, P., 2013. Personal cloudlets for privacy and resource efficiency in mobile in-app advertising. Proc. Int. Symp. Mob. Ad Hoc Netw. Comput. 33–39. https://doi.org/10.1145/2492348.2492356

Shen, F., n.d. A Visually Interpretable Iris Recognition System with Crypt Features.

Simanta, S., Ha, K., Lewis, G., Morris, E., Satyanarayanan, M., 2012. A Reference Architecture for Mobile Code Offload in Hostile Environments. Lect. Notes Inst. Comput. Sci. Soc. Telecommun. Eng. 110 LNICST, 274–293. https://doi.org/10.1007/978-3-642-36632-1_16

Simon, H.A., 1983. Why Should Machines Learn? Mach. Learn. 25–37. https://doi.org/10.1007/978-3-662-12405-5_2

Sivanandam, S.N., Sumathi, S., Deepa, S.N., 2006. Introduction to neural networks using MATLAB 6.0. McGraw Hill Education (India) Private Limited.

Tajouri, I., Aydi, W., Ghorbel, A., Masmoudi, N., 2017. Efficient iris texture analysis method based on Gabor ordinal measures. https://doi.org/10.1117/1.JEI.26.4.043012 26, 043012. https://doi.org/10.1117/1.JEI.26.4.043012

Tan, X., Triggs, B., 2010. Enhanced local texture feature sets for face recognition under difficult lighting conditions. IEEE Trans. image Process. 19, 1635–1650.

TensorFlow Lite | ML for Mobile and Edge Devices. URL https://www.tensorflow.org/lite

The ORL Database of Faces, 2001. No Title.

The Yale Face Database, 2001. No Title.

Thomaz, C.E., 2006. The FEI face database. URL https://fei.edu.br/~cet/facedatabase.html

Tistarelli, M., Champod, C. (Eds.), 2017. Handbook of Biometrics for Forensic Science. Advances in Computer Vision and Pattern Recognition. https://doi.org/10.1007/978-3-319-50673-9

Tiwari, A., Jain, V., 2015. Indian Iris Recognition System using Ant Colony Optimization. Int. J. Eng. Trends Technol. 21, 380–387. https://doi.org/10.14445/22315381/IJETT-V21P273

Tortora, G.J., Evans, R.L., 1986. Principles of human physiology. Harper & Row.

Tucker, A., 2004. Computer science handbook.

Vandenbroucke, K., Ferreira, D., Goncalves, J., Kostakos, V., De Moor, K., 2014. Mobile cloud storage: A contextual experience. MobileHCI 2014 - Proc. 16th ACM Int. Conf. Human-Computer Interact. with Mob. Devices Serv. 101–110. https://doi.org/10.1145/2628363.2628386

VAPNIK, V., 1963. Pattern recognition using generalized portrait method. Autom. Remote Control 24, 774–780.

Victor Roman, 2019. Unsupervised Machine Learning: Clustering Analysis | Towards Data Science.

Wang, C., Zou, P., Liu, Z., Wang, J., 2010. CS-DRM: A Cloud-Based SIM DRM Scheme for Mobile Internet. EURASIP J. Wirel. Commun. Netw. 2011 20111 2011, 1–19. https://doi.org/10.1155/2011/837209

Wang, S., Liu, Y., Dey, S., n.d. Wireless Network Aware Cloud Scheduler for Scalable Cloud Mobile

Gaming.

Wang, Y., Lin, X., Pedram, M., 2013. A nested two stage game-based optimization framework in mobile cloud computing system. Proc. - 2013 IEEE 7th Int. Symp. Serv. Syst. Eng. SOSE 2013 494–502. https://doi.org/10.1109/SOSE.2013.68

Wang, Y., Nakachi, T., 2020. A Privacy-Preserving Learning Framework for Face Recognition in Edge and Cloud Networks. IEEE Access 8, 136056–136070. https://doi.org/10.1109/ACCESS.2020.3011112

Wang, Y., Nakachi, T., Ishihara, H., 2019. Edge and Cloud-aided Secure Sparse Representation for Face Recognition, in: 2019 27th European Signal Processing Conference (EUSIPCO). IEEE, pp. 1–5. https://doi.org/10.23919/EUSIPCO.2019.8903137

Weber, R.H., Weber, R., 2010. Introduction. Internet of Things 1–22. https://doi.org/10.1007/978-3-642-11710-7_1

Weiss, N., Kost, H., Homeyer, A., 2018. Towards interactive breast tumor classification using transfer learning, in: International Conference Image Analysis and Recognition. Springer, pp. 727–736.

Wermter, S., Riloff, E., Scheler, G. (Eds.), 1996. Connectionist, Statistical and Symbolic Approaches to Learning for Natural Language Processing. Lecture Notes in Computer Science 1040. https://doi.org/10.1007/3-540-60925-3

What is mobile cloud computing? - Cloud computing news. URL https://www.ibm.com/blogs/cloud-computing/2013/06/25/mobile-cloud-computing/ (accessed 10.20.21).

What is the vanishing gradient problem? - Quora, 2015. URL https://www.quora.com/What-is-the-vanishing-gradient-problem

Wicht, B., 2017. Deep learning feature extraction for image processing thesis. Phd, Dep. Informatics, Univ. Fribg.

Wilson, H.R., Cowan, J.D., 1972. Excitatory and inhibitory interactions in localized populations of model neurons. Biophys. J. 12, 1–24.

Xiang, C., Tang, C., Cai, Y., Xu, Q., 2016. Privacy-preserving face recognition with outsourced

computation. Soft Comput. 20, 3735–3744. https://doi.org/10.1007/s00500-015-1759-5

Xu, Y., Fei, L., Zhang, D., 2015. Combining left and right palmprint images for more accurate personal identification. IEEE Trans. Image Process. 24, 549–559. https://doi.org/10.1109/TIP.2014.2380171

Yang, J., Jiang, Y., Fang, H., Jiang, Z., Zhang, H., Hao, S., 2018. Semantic Segmentation of Aerial Image Using Fully Convolutional Network, in: Chinese Conference on Image and Graphics Technologies. Springer, pp. 546–555.

YangLei, CaoJiannong, YuanYin, LiTao, HanAndy, ChanAlvin, 2013. A framework for partitioning and execution of data stream applications in mobile cloud computing. ACM SIGMETRICS Perform. Eval. Rev. 40, 23–32. https://doi.org/10.1145/2479942.2479946

Yee, S.Y., H., T., Falah, M., M., N., 2019. Performance Evaluation of Completed Local Ternary Pattern (CLTP) for Face Image Recognition. Int. J. Adv. Comput. Sci. Appl. 10. https://doi.org/10.14569/IJACSA.2019.0100446

Yu, F.R., Leung, V., 2015. Advances in mobile cloud computing systems. CRC Press.

Zafar, I., Tzanidou, G., Burton, R., Patel, N., Araujo, L., 2018. Hands-on convolutional neural networks with TensorFlow: Solve computer vision problems with modeling in TensorFlow and Python. Packt Publishing Ltd.

Zeroual, A., Amroune, M., Derdour, M., Bentahar, A., 2021. Lightweight deep learning model to secure authentication in Mobile Cloud Computing. J. King Saud Univ. - Comput. Inf. Sci. https://doi.org/10.1016/J.JKSUCI.2021.09.016

Zeroual, A., Amroune, M., Derdour, M., Meraoumia, A., Bentahar, A., 2018. Deep authentication model in Mobile Cloud Computing, in: 2018 3rd International Conference on Pattern Analysis and Intelligent Systems (PAIS). IEEE, pp. 1–4. https://doi.org/10.1109/PAIS.2018.8598508

Zeroual, A., Derdour, M., Amroune, M., Bentahar, A., 2019. Using a fine-tuning method for a deep authentication in mobile cloud computing based on Tensorflow Lite framework, in: 2019 International Conference on Networking and Advanced Systems (ICNAS). IEEE, pp. 1–5.

Zhang, C., Bengio, S., Hardt, M., Recht, B., Vinyals, O., 2021. Understanding deep learning (still)

requires rethinking generalization. Commun. ACM 64, 107–115.

Zhang, D., Lu, G., 2013. 3D biometrics: Systems and applications. 3D Biometrics Syst. Appl. 1–290. https://doi.org/10.1007/978-1-4614-7400-5

Zhang, Z., Li, S., 2016. A survey of computational offloading in mobile cloud computing. Proc. - 2016 4th IEEE Int. Conf. Mob. Cloud Comput. Serv. Eng. MobileCloud 2016 81–82. https://doi.org/10.1109/MOBILECLOUD.2016.15

Zhao, K., Jin, H., Zou, D., Chen, G., Dai, W., 2013. Feasibility of deploying biometric encryption in mobile cloud computing. Proc. - 2013 8th Annu. ChinaGrid Conf. ChinaGrid 2013 28–33. https://doi.org/10.1109/CHINAGRID.2013.10

ZhaoW., ChellappaR., J., P., RosenfeldA., 2003. Face recognition. ACM Comput. Surv. 5, V-305-V–308. https://doi.org/10.1145/954339.954342

Zhou, J., Lin, X., Dong, X., Cao, Z., 2015. PSMPA: Patient self-controllable and multi-level privacy-preserving cooperative authentication in distributed m-healthcare cloud computing system. IEEE Trans. Parallel Distrib. Syst. 26, 1693–1703. https://doi.org/10.1109/TPDS.2014.2314119

Ziegel, E.R., 2012. The Elements of Statistical Learning. http://dx.doi.org/10.1198/tech.2003.s770 45, 267–268. https://doi.org/10.1198/TECH.2003.S770

Liste des abréviations

A

Artificial Neural Network
(ANN), 53
Assistants numériques personnels
(PDA), 16

C

Cloud Computing
(CC), 16
Completed Local Bianry Patterns
CLBP, 103
Completed Local Ternary Patterns
(CLTP), 103
Convolutional Neural Network
(CNN), 55

E

Energy Efficiency Ratio
(EER), 68

F

Fully Homomorphic Encryption
(FHE), 69

I

Infrastructur As A Service
(IaaS), 16

L

l'intelligence artificiel
(IA), 45
Local Binary Pattern
(LBP), 72
Local Ternary Pattern
(LTP), 78

M

Machine Learning
(ML), 45
Mobile Cloud
(MC), 16
Mobile Cloud Computing
(MCC), 16

P

Paltform As A Service
(PaaS), 16
Partialy Homomorphic Encryption
(PHE), 79
Personal Identification Number
(PIN), 42
Principal Component Analysis
(PCA), 69

R

Rectified Linear Unit

(ReLU), 61

S

Software As A Service (SaaS), 16

SomeWhat Homomorphic Encryption (SWHE), 79

Support Vector Machine (SVM), 47

V

Virtual Private Network (VPN), 30

Z

Zero Knowledge Proof(ZKP), 32