



république Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

**Université des Sciences et de la Technologie Houari Boumediene**

**Faculté d'Informatique  
Département Systèmes Informatique**

Mémoire de Master

**Spécialité  
Sécurité des Systèmes Informatiques (SSI)**

## **Thème**

---

**Conception et mise en œuvre d'un outil de contrôle parental pour la surveillance et de contrôle des média sociaux  
– cas WhatsApp –**

---

**Sujet Proposé par :**

Mr BERBAR Ahmed

**Présenté par :**

BOUKHEMIA Abdelrafik

FAHAM Billel

**Soutenu le : 29/06/2025**

**Devant le jury composé de:**

Mme BOUYAKOUB Samia  
Mme CHIKHAOUI Amina

Présidente  
Membre

Binôme N° : 013 / 2025

# Remerciement

Nous commençons par exprimer notre plus profonde gratitude et nos louanges à Allah, pour Sa grâce, Sa miséricorde et la force qu'Il nous a accordées pour l'achèvement de ce travail.

Nos sincères remerciements vont ensuite à notre estimé encadrant, Monsieur Ahmed BERBAR, pour sa patience, ses conseils précieux et son soutien constant qui ont été d'une aide inestimable tout au long de ce parcours.

Nous remercions également chaleureusement les membres du jury pour avoir bien voulu consacrer leur temps et leur expertise à l'évaluation de ce mémoire.

Enfin, nous ne saurions oublier de remercier toutes les personnes qui, de près ou de loin, ont apporté leur contribution et leur soutien à la réalisation de ce projet.

## Abstract

This thesis analyzes the Android environment and WhatsApp's functionality to develop a parental control solution. It addresses the data access challenges posed by Android's security measures and WhatsApp's encryption, rendering traditional non-rooted monitoring methods ineffective. The proposed solution leverages WhatsApp's "Linked Devices" feature for integrated and secure monitoring. The client-server architecture is detailed, including the target application on the child's device, a central server, and a parental dashboard. Features encompass access to messages, call history, audio/video recordings, contacts, shared media, app usage time, location, contact/group blocking, WhatsApp access blocking, and keyword-based alerts. This work demonstrates the technical feasibility of an ethical and reliable monitoring tool without requiring rooting, offering enhanced protection against digital risks for children.

**Keywords:** Android, WhatsApp, Parental Control, Data Monitoring

## Résumé

Ce mémoire explore l'environnement Android et le fonctionnement de WhatsApp pour développer une solution de contrôle parental. Il analyse les défis d'accès aux données imposés par les mesures de sécurité d'Android et par le chiffrement de WhatsApp, rendant inefficaces les méthodes traditionnelles de surveillance sans root. La solution proposée exploite la fonctionnalité "Appareils connectés" de WhatsApp pour un monitoring intégré et sécurisé. L'architecture client-serveur est détaillée, incluant l'application cible sur le téléphone de l'enfant, un serveur central, et un tableau de bord parental. Les fonctionnalités couvrent l'accès aux messages, à l'historique des appels, aux enregistrements audio/vidéo, aux contacts, aux médias échangés, au temps passé sur l'application, à la localisation, au blocage de contacts/groupes, au blocage de l'accès à WhatsApp, et aux alertes par mots-clés. Ce travail démontre la faisabilité technique d'un outil de surveillance éthique et fiable sans nécessiter de root, offrant une protection accrue contre les risques numériques pour les enfants.

**Mots Clés :** Android, WhatsApp, Contrôle Parental, Surveillance des Données

# Table des matières

<b>Table des figures</b>	<b>i</b>
<b>Liste des tableaux</b>	<b>iii</b>
<b>Nomenclature</b>	<b>iv</b>
<b>Introduction Générale</b>	<b>1</b>
<b>1 Étude de l'environnement Android</b>	<b>4</b>
Introduction . . . . .	4
1.1 Histoire du système d'exploitation Android . . . . .	4
1.2 Architecture de la plate-forme Android . . . . .	5
1.2.1 Noyau Linux (Kernel) . . . . .	6
1.2.2 Couche d'abstraction matérielle (HAL) . . . . .	7
1.2.3 Environnement d'exécution Android (ART) . . . . .	8
1.2.4 Bibliothèques C/C++ natives . . . . .	9
1.2.5 Framework de l'API Java . . . . .	9
1.2.6 Applis système . . . . .	10
1.3 Gestion de la Mémoire sous Android . . . . .	10
1.3.1 Type de mémoire dans Android . . . . .	10
1.3.2 Stratégies d'allocation de mémoire . . . . .	11
1.3.3 Pages de mémoire dans Android . . . . .	11
1.3.4 Garbage Collection dans Android . . . . .	12
1.3.5 Mécanisme de gestion de la mémoire faible . . . . .	13
1.3.6 Défis de la gestion de la mémoire dans Android . . . . .	13
1.4 Gestion des Disques sous Android . . . . .	15
1.4.1 Architecture de stockage Android . . . . .	15
1.4.2 Hiérarchie du système de fichiers . . . . .	15
1.4.3 Types de stockage dans Android . . . . .	16

---

TABLE DES MATIÈRES

---

1.5	Open source . . . . .	18
1.5.1	Qu'est-ce que l'Open Source? . . . . .	18
1.5.2	Types de licences Open Source . . . . .	18
1.5.3	Licences Open Source utilisé par Android . . . . .	19
1.5.4	Avantages de l'Open Source . . . . .	19
1.5.5	Inconvénients de l'Open Source . . . . .	20
1.6	Principales caractéristiques d'Android . . . . .	20
1.7	Android os et la sécurité . . . . .	21
1.7.1	Fonctions de sécurité d'Android . . . . .	21
1.7.2	Défis liés à la sécurité d'Android . . . . .	23
	Conclusion . . . . .	25
<b>2</b>	<b>Les Applications de Messagerie Instantanée : Un aperçu complet avec un focus sur WhatsApp</b>	<b>26</b>
	Introduction . . . . .	26
2.1	Applications de messagerie instantanée . . . . .	26
2.1.1	Introduction aux applications de messagerie instantanée . . . . .	26
2.1.2	Caractéristiques des Applications de Messagerie Instantanée . . . . .	27
2.1.3	Applications de Messagerie Instantanée Populaires . . . . .	28
2.2	WhatsApp . . . . .	30
2.2.1	Introduction à WhatsApp . . . . .	30
2.2.2	Histoire de WhatsApp . . . . .	30
2.2.3	Caractéristiques de WhatsApp . . . . .	31
2.2.4	Popularité . . . . .	31
2.2.5	Architecture technique de WhatsApp . . . . .	32
2.2.6	Sécurité et confidentialité dans WhatsApp . . . . .	40
2.2.7	Défis et impact mondial de WhatsApp . . . . .	44
	Conclusion . . . . .	47
<b>3</b>	<b>Étude des solutions existantes</b>	<b>48</b>
	Introduction . . . . .	48
3.1	WhatsApp est-il sûr pour les enfants ? . . . . .	48
3.2	Principales caractéristiques des applications de contrôle parental . . . . .	50
3.3	Applications populaires de contrôle parental pour WhatsApp . . . . .	51
3.3.1	Bark . . . . .	51
3.3.2	mSpy . . . . .	52
3.3.3	FamiSafe . . . . .	52

3.3.4	Qustodio . . . . .	52
3.4	Défis et limites . . . . .	53
	Conclusion . . . . .	54
<b>4</b>	<b>Étude conceptuelle</b>	<b>55</b>
	Introduction . . . . .	55
4.1	Objectif . . . . .	55
4.2	Défis liés à la sécurité d'Android . . . . .	56
4.2.1	Accès restreint aux données applicatives (/data/data) . . . . .	56
4.2.2	Fonctionnalité “Paramètres restreints” . . . . .	56
4.3	Prérequis pour le monitoring de WhatsApp . . . . .	56
4.4	Root Android . . . . .	57
4.4.1	Définition du routage . . . . .	57
4.4.2	Avantages . . . . .	57
4.4.3	Risques induits par le routage . . . . .	58
4.5	Techniques actuelles de monitoring sans root . . . . .	59
4.5.1	Mise en miroir des notifications . . . . .	59
4.5.2	Services d'accessibilité (Lecture d'écran) . . . . .	60
4.5.3	Mise en miroir / Enregistrement d'écran . . . . .	60
4.5.4	Enregistrement de frappes (Keylogging) . . . . .	60
4.5.5	Liaison avec WhatsApp Web . . . . .	61
4.6	Limites des approches existantes . . . . .	61
4.7	Solution proposée . . . . .	62
4.7.1	Introduction . . . . .	62
4.7.2	Architecture . . . . .	62
4.7.3	Composants . . . . .	63
4.7.4	Modélisation de la solution . . . . .	64
4.7.5	Algorithmes de scraping . . . . .	70
4.7.6	Fonctionnalités . . . . .	71
4.8	Justification du choix . . . . .	73
	Conclusion . . . . .	73
<b>5</b>	<b>Implémentation</b>	<b>74</b>
	Introduction . . . . .	74
5.1	Environnement de Travail . . . . .	74
5.1.1	Langages de programmation . . . . .	74
5.1.2	Frameworks utilisés . . . . .	75

*TABLE DES MATIÈRES*

---

5.1.3	Base de données . . . . .	77
5.1.4	Environnements de développement . . . . .	78
5.1.5	Outils . . . . .	78
5.2	Fonctionnalités Principales . . . . .	79
5.2.1	Côté enfant (Application Android) . . . . .	79
5.2.2	Côté parent (Dashboard Web) . . . . .	80
	Conclusion . . . . .	80
	<b>Conclusion Générale</b>	<b>81</b>
<b>A</b>	<b>Historique des versions d'Android</b>	<b>A</b>
<b>B</b>	<b>Interfaces de la solution</b>	<b>F</b>
	<b>Bibliographie</b>	<b>P</b>

# Table des figures

1.1	Part de marchés des systèmes d'exploitation mobile depuis 2009 [1] . . . . .	5
1.2	Pile logiciel Android [4] . . . . .	6
1.3	Architecture GKI [5] . . . . .	7
1.4	Types de mémoire [15] . . . . .	10
2.1	Les applications de messagerie les plus utilisées dans le monde en 2024 [52]	32
2.2	Diagramme de l'architecture de WhatsApp [55] . . . . .	32
2.3	Synchronisation multi-appareils de WhatsApp [62] . . . . .	39
2.4	Chiffrement de bout en bout de WhatsApp [63] . . . . .	40
4.1	Architecture de la solution . . . . .	62
4.2	Diagramme de cas d'utilisation - Acteur "Parent" . . . . .	65
4.3	Diagramme de cas d'utilisation - Acteur "Enfant" . . . . .	66
4.4	Diagramme de séquence - Inscription Parent . . . . .	67
4.5	Diagramme de séquence - Inscription Enfant . . . . .	68
4.6	Diagramme des classes . . . . .	69
5.1	Flux de communication entre le navigateur et le serveur . . . . .	76
5.2	Interfaces d'inscription et de connexion - Android . . . . .	79
5.3	Interfaces de connexion et d'inscription - Web . . . . .	80
A.1	Versions d'Android 2008-2025 . . . . .	A
B.1	Autorisations requises I . . . . .	F
B.2	Autorisations requises II . . . . .	G
B.3	Intefraces Android . . . . .	H
B.4	Page d'accueil du tableau de bord . . . . .	I
B.5	Tableau de bord - Enfant sélectionné . . . . .	J
B.6	Tableau de bord - Notifications . . . . .	J
B.7	Tableau de bord - Contacts . . . . .	K

*TABLE DES FIGURES*

---

B.8 Tableau de bord - Discussions . . . . .	K
B.9 Tableau de bord - Dossiers . . . . .	L
B.10 Tableau de bord - Plannings . . . . .	L
B.11 Tableau de bord - Vidoes . . . . .	M
B.12 Tableau de bord - Voix . . . . .	M
B.13 Tableau de bord - Mots Clés . . . . .	N
B.14 Tableau de bord - Temps d'écean . . . . .	N
B.15 Tableau de bord - Localisation . . . . .	O

# Liste des tableaux

1.1	Répertoires Principaux du Système de Fichiers Android . . . . .	16
A.1	Les nouvelles fonctionnalités des dernières versions d'Android . . . . .	E

# Nomenclature

## Abréviations

ACID	Atomicité, Cohérence, Isolation, Durabilité
ACK	Android Common Kernel
AES	Advanced Encryption Standard
AIM	America Online Instant Messenger
AOSP	Android Open Source Project
AOT	Ahead-of-Time
API	Application Programming Interface
APNS	Apple Push Notification Service
ART	Android Runtime
BBM	BlackBerry Messenger
BDD	Base de Données
CCPA	California Consumer Privacy Act
CDN	Content Delivery Network
DRY	Don't Repeat Yourself
FCM	Firebase Cloud Messaging
GC	Garbage Collector
GDPR	General Data Protection Regulation
GIF	Graphics Interchange Format
GKI	Generic Kernel Image
GNU GPL	Licence publique générale GNU

HAL	Hardware Abstraction Layer
HTC	High Tech Computer Corporation
HTML	HyperText Markup Language
HTTP	Hypertext Transfer Protocol
IA	Intelligence artificielle
ICQ	I Seek You
IRC	Internet Relay Chat
KMI	Kernel Module Interface
kswapd	Kernel Swap Daemon
LGPL	Lesser General Public License
LMK	Low Memory Killer
LRU	Least Recently Used
LTS	Long Term Support
MAC	Mandatory Access Control
OS	Operating System
MITM	Man-In-The-Middle
MLD	Modèle logique de Données
NLP	Natural Language Processing
ORM	Object-Relational Mapping
OTA	Over The Air
PIN	Personal Identification Number
RAM	Random Access Memory
SD	Secure Digital
SGBDR	Système de gestion de bases de données relationnelles
SGBD	Système de gestion de base de données
SMS	Short Message Service
SQL	Structured Query Language

*NOMENCLATURE*

---

S RTP	Secure Real-time Transport Protocol
TEE	Trusted Execution Environment
UID	User Identifier
UI	User Interface
UML	Unified Modeling Language
URL	Uniform Resource Locator
XMPP	Extensible Messaging and Presence Protocol

# Introduction Générale

L'évolution des systèmes d'exploitation mobiles a connu des transformations significatives au cours des deux dernières décennies, passant de simples plateformes limitées à des environnements extrêmement sophistiqués où la communication, le travail collaboratif et la sécurisation des données jouent un rôle majeur. À l'origine conçus pour des téléphones disposant de fonctionnalités de base, ces systèmes constituent aujourd'hui le socle de milliards d'appareils connectés à l'échelle du globe. Parmi eux, Android s'impose comme la plate-forme mobile dominante, grâce à son ouverture, sa flexibilité ainsi que la richesse de son écosystème applicatif. Développé par Google, Android repose sur une architecture moderne, un noyau Linux adapté à la mobilité, ainsi qu'un modèle de sécurité éprouvé. Il bénéficie ainsi du soutien d'une vaste communauté de développeurs et de constructeurs, favorisant l'innovation ainsi que la personnalisation du système pour répondre à des besoins spécifiques.

Parallèlement à l'évolution des systèmes d'exploitation, les applications de messagerie instantanée ont révolutionné la manière dont les personnes communiquent et partagent des informations à l'ère du numérique. Parmi elles, WhatsApp occupe une place centrale. Avec plus de deux milliards d'utilisateurs à travers le monde, elle s'impose comme un outil majeur du quotidien, offrant des fonctionnalités de messagerie texte, vocale, vidéo ainsi que des mécanismes de sécurité de bout en bout garantissant la confidentialité des échanges. Néanmoins, malgré la popularité de ces outils, ils soulèvent des enjeux cruciaux liés à la protection des plus jeunes et à la maîtrise de leur usage. L'absence de mécanismes adaptés de contrôle parental devient ainsi une préoccupation majeure, particulièrement au regard de la sensibilité des informations échangées ainsi que de l'exposition des enfants à des contenus potentiellement dangereux.

C'est dans ce contexte que s'inscrit ce mémoire. Il propose d'analyser en profondeur l'environnement Android ainsi que le fonctionnement technique de WhatsApp, en détaillant leurs mécanismes essentiels — de la gestion de la mémoire à la couche de sécurité — tout en abordant la problématique du contrôle parental appliqué à WhatsApp. Ce tra-

vail repose sur une étude détaillée des technologies, des contraintes ainsi que des enjeux liés à la surveillance parentale, tout en gardant à l'esprit l'équilibre délicat à atteindre entre surveillance, respect de la vie privée et protection des enfants.

Pour atteindre cet objectif, le mémoire est structuré en cinq chapitres :

→ ***Chapitre 1 : Étude de l'environnement Android***

Ce chapitre détaille l'architecture du système d'exploitation Android ainsi que ses mécanismes de gestion de la mémoire, du stockage des données et de la couche de sécurité. Il aborde également l'impact de la nature open source d'Android ainsi que la manière dont elle influe sur la personnalisation du système, tout en détaillant les mécanismes de protection intégrés.

→ ***Chapitre 2 : Les applications de messagerie instantanée : Focus sur WhatsApp***

Ce chapitre propose une exploration détaillée du paysage des applications de messagerie instantanée ainsi qu'une étude approfondie de WhatsApp. Il analyse son architecture technique, ses mécanismes de chiffrement ainsi que ses caractéristiques spécifiques ayant contribué à son succès mondial.

→ ***Chapitre 3 : Étude des solutions existantes de contrôle parental***

Ce chapitre recense les solutions disponibles à ce jour, en détaillant leurs caractéristiques, leurs avantages ainsi que leurs limites. Il met en évidence les contraintes spécifiques à l'environnement Android ainsi qu'à la surveillance des échanges réalisés via WhatsApp.

→ ***Chapitre 4 : Étude conceptuelle de la solution proposée***

Ce chapitre détaille la solution envisagée pour répondre à la problématique du contrôle parental. Il précise son architecture générale, ses composants ainsi que les méthodes employées (incluant le scraping ainsi que l'automatisation) pour garantir une surveillance précise, sécurisée et respectueuse de la vie privée.

→ ***Chapitre 5 : Implémentation de la solution*** Ce dernier chapitre fournit une description détaillée de la mise en place du projet proposé. Il présente l'environnement de travail utilisé (langages de programmation, frameworks, outils), ainsi que le fonctionnement détaillé des principales fonctionnalités implémentées côté parent et côté enfant.

Ce travail de recherche vise à démontrer l'importance de concevoir des solutions de contrôle parental spécifiques à l'environnement Android, tout en garantissant un équi-

## *INTRODUCTION GÉNÉRALE*

---

libre entre la protection des mineurs, le respect de la vie privée ainsi que la sécurité des échanges numériques. Il fournit ainsi des perspectives nouvelles pour accompagner les évolutions futures des usages du mobile, tout en répondant aux enjeux cruciaux de la société connectée moderne.

# Chapitre 1

## Étude de l'environnement Android

### Introduction

Le système d'exploitation mobile Android, développé par Google, domine le marché mondial des smartphones et tablettes [1]. Son adoption massive par les fabricants et les utilisateurs s'explique par sa nature open-source, sa flexibilité et son vaste écosystème d'applications.

Ce chapitre introductif offre une analyse complète de l'environnement Android, explorant son histoire, son architecture logicielle, ses versions marquantes, ses caractéristiques clés, sans oublier les enjeux liés à la sécurité. Cette exploration fournira une base solide pour la compréhension et l'appréciation des chapitres suivants.

### 1.1 Histoire du système d'exploitation Android

Android Inc. a été fondée en 2003 à Palo Alto, en Californie, par des pionniers de la technologie tels que Rich Miner, Nick Sears, Chris White et Andy Rubin. À l'origine, l'objectif de cette petite start-up était de révolutionner le système d'exploitation des appareils photo numériques. L'idée était d'améliorer la gestion du stockage des images afin de permettre aux utilisateurs de profiter d'une plus grande flexibilité et de ne plus être limités par la taille de leurs cartes de stockage. Cependant, malgré l'innovation de cette idée, celle-ci n'a pas vraiment pris son essor, contraignant l'équipe à repenser sa stratégie. C'est dans un contexte d'expansion du secteur de la téléphonie mobile qu'Android Inc. a proposé une plateforme de système d'exploitation gratuit, s'opposant ainsi aux pratiques des géants de l'industrie. Cette approche innovante a incité Google à acquérir Android en 2005, marquant le début d'un système d'exploitation mobile open source accessible à tous [2].

En septembre 2008, le premier smartphone sous Android, le T-Mobile G1 (également connu sous le nom de HTC Dream), a été lancé. Il fonctionnait sous Android 1.0, qui présentait déjà les caractéristiques de la stratégie de Google pour son système d'exploitation. Ce modèle intégrait divers produits et services de l'entreprise, tels que Google Maps, YouTube, ainsi qu'un navigateur HTML (avant Chrome) utilisant les services de recherche de Google. [3]

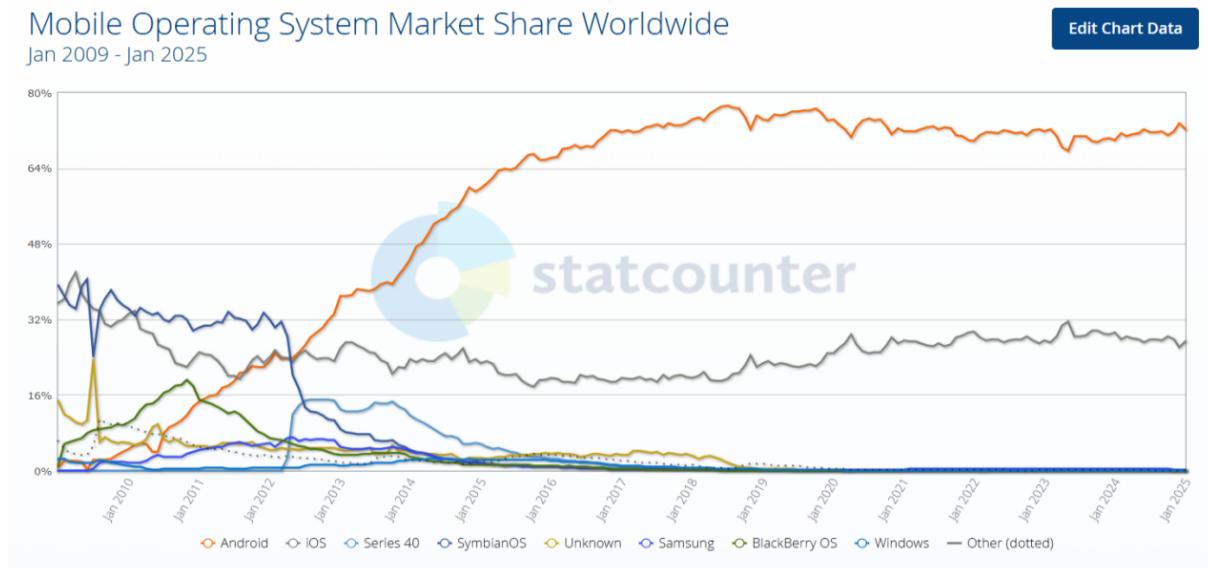


Figure 1.1: Part de marchés des systèmes d'exploitation mobile depuis 2009 [1]

En analysant la figure 1.1, il apparaît clairement qu'Android conserve une position dominante sur le marché des systèmes d'exploitation mobiles et assure constamment une part importante du marché mondial, souvent comprise entre 70 et 80% grâce à sa présence sur les appareils de toutes les catégories de prix, du budget au haut de gamme [1].

## 1.2 Architecture de la plate-forme Android

Android est une plateforme logicielle open source basée sur Linux, conçue pour une grande variété d'appareils. Son architecture s'organise en couches, chaque couche fournissant des services et des API aux couches supérieures. La Figure 1.2 illustre les principaux composants qui constituent la plateforme Android. Grâce à cette structure modulaire, les développeurs peuvent créer des applications riches et performantes en s'appuyant sur les fonctionnalités offertes par la plateforme [4].

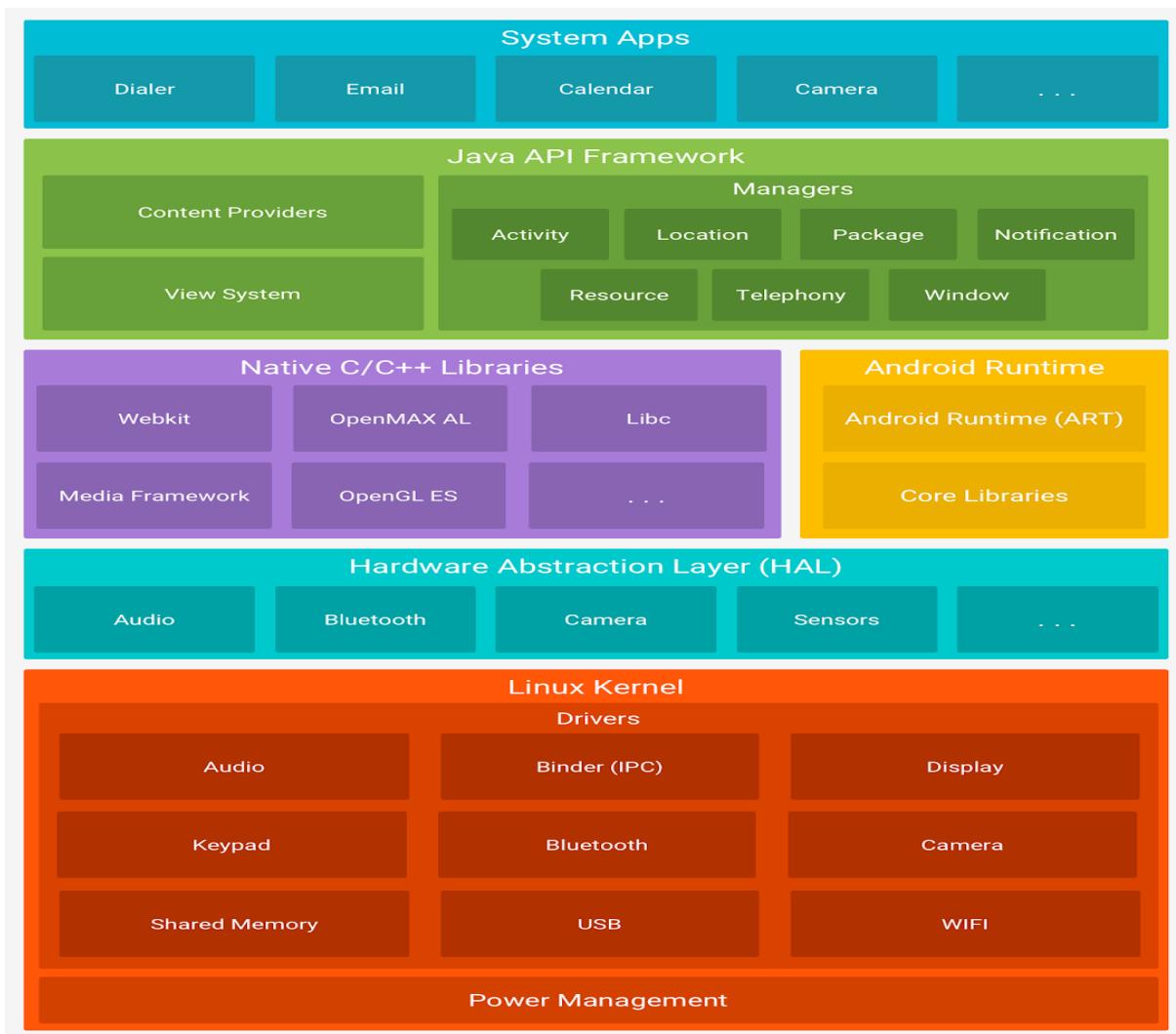


Figure 1.2: Pile logiciel Android [4]

### 1.2.1 Noyau Linux (Kernel)

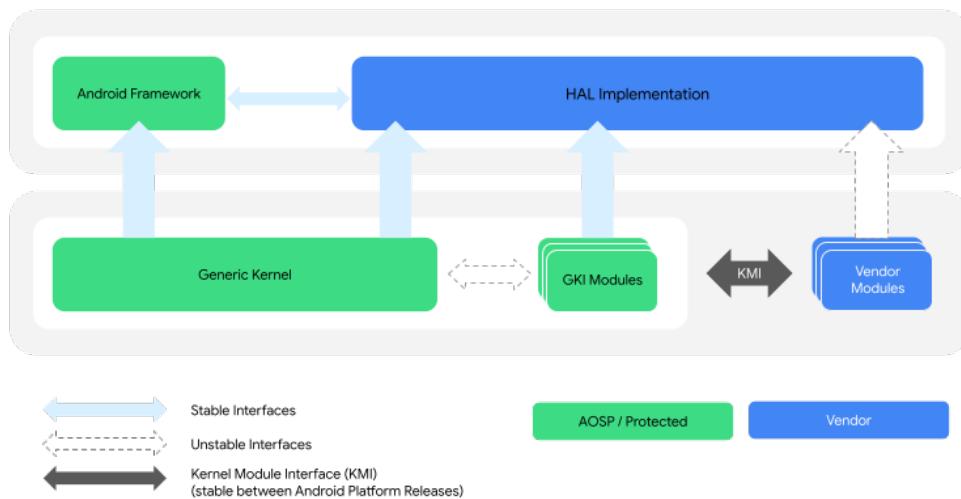
Au cœur de l'architecture Android se trouve le noyau Linux. Il assure les fonctions de base du système d'exploitation, telles que la gestion de la mémoire, des processus, des périphériques et du système de fichiers. Android utilise une version adaptée du noyau Linux, optimisée pour les appareils mobiles, notamment en termes de consommation d'énergie et d'utilisation de la mémoire [4].

Cette adaptation du noyau Linux pour les appareils mobiles consiste à intégrer de correctifs propres à Android dans des noyaux Linux à long terme (LTS) appelés désormais, après modification, noyaux GKI [5].

Les noyaux GKI jouent un rôle essentiel dans la modularité d'Android, en assurant la séparation entre le code du noyau générique, indépendant du matériel, et les modules

spécifiques au matériel, appelés modules fournisseurs. Cette séparation facilite la maintenance et les mises à jour du système d'exploitation, tout en permettant aux fabricants de matériel d'intégrer leurs propres optimisations [5].

L'interaction entre le noyau GKI et les modules fournisseurs se fait par le biais de l'interface de module noyau (KMI). Cette interface, composée de listes de symboles, définit les données et les fonctions globales nécessaires aux modules fournisseurs pour interagir avec le noyau (voir figure 1.3) [5].



**Figure 1.3:** Architecture GKI [5]

L'utilisation du noyau Linux, et de son adaptation à travers les ACKs et les GKIs, offre plusieurs avantages :

- **Sécurité** : Android profite des mécanismes de sécurité éprouvés du noyau Linux, tels que la gestion des permissions et l'isolation des processus.
- **Portabilité** : La compatibilité du noyau Linux avec une large gamme de processeurs et de périphériques permet à Android d'être déployé sur une multitude d'appareils.

### 1.2.2 Couche d'abstraction matérielle (HAL)

La couche d'abstraction matérielle (HAL) fournit une interface standard entre le framework d'applications Android et le matériel de l'appareil. Elle permet aux développeurs d'accéder aux fonctionnalités matérielles, telles que la caméra, le Bluetooth ou les capteurs, sans avoir à se soucier des spécificités de chaque appareil [6]. La HAL est composée de modules, chacun implémentant une interface pour un type de composant matériel spécifique. Lorsqu'une application utilise une API du framework pour accéder au matériel,

le système Android charge le module HAL correspondant pour interagir avec le périphérique [4].

### **1.2.3 Environnement d'exécution Android (ART)**

L'environnement d'exécution Android (ART) est la machine virtuelle qui exécute les applications Android. Il transforme le code des applications, écrit en Java/Kotlin, en instructions que le processeur peut comprendre et exécuter. ART a apporté un lot d'améliorations significatives en termes de performances, d'efficacité et de compatibilité [7].

#### **1.2.3.1 Amélioration des performances**

ART utilise une compilation Ahead-of-Time (AOT), ce qui signifie que le code de l'application est compilé en code machine natif lors de l'installation. Cette compilation AOT est essentielle pour des performances plus fluides et des lancements d'applications plus rapides, car le processeur n'a plus besoin de traduire le code à chaque utilisation. Cela réduit considérablement le temps d'exécution des applications et améliore l'expérience utilisateur [8].

#### **1.2.3.2 Gestion optimisée de la mémoire**

ART intègre un ramasse-miette (garbage collector). Ce mécanisme, un système de nettoyage de la mémoire, permet de libérer la mémoire occupée par les objets non utilisés de manière plus efficace, réduisant ainsi la fragmentation de la mémoire et améliorant la stabilité du système. Le garbage collector d'ART utilise un système de collecte "mark-and-sweep" concurrent, ce qui signifie qu'il peut fonctionner en arrière-plan sans interrompre l'exécution de l'application. Cela contribue à une expérience utilisateur plus fluide et à une meilleure réactivité des applications [9].

#### **1.2.3.3 Prise en charge des architectures 64 bits**

ART a été conçu pour prendre en charge les architectures 64 bits, qui offrent des performances accrues et une capacité de mémoire supérieure par rapport aux architectures 32 bits. Cette compatibilité a permis à Android de s'adapter à l'évolution du matériel et d'exploiter pleinement la puissance des processeurs modernes. Cela se traduit par des applications plus rapides et plus performantes, et la possibilité d'utiliser des applications gourmandes en ressources [7].

### 1.2.3.4 Amélioration de l'autonomie de la batterie

L'un des avantages les plus appréciables d'ART est son impact positif sur l'autonomie de la batterie. La compilation AOT d'ART contribue également à une meilleure autonomie de la batterie. En réduisant la charge de travail du processeur lors de l'exécution des applications, ART permet de consommer moins d'énergie [8].

### 1.2.3.5 Débogage avec ART

ART offre également des améliorations significatives en matière de débogage. Il propose un meilleur support pour le débogage du code natif, ce qui facilite le développement et le débogage des applications Android [7].

## 1.2.4 Bibliothèques C/C++ natives

Les bibliothèques natives sont des ensembles de code écrit en C/C++ qui fournissent des fonctionnalités spécifiques aux applications Android. Elles sont accessibles via le framework d'applications et permettent d'interagir avec le matériel (OpenGL ES pour les graphismes, Media Framework pour le multimédia) ou de fournir des services clés (SQLite pour les bases de données, OpenSSL pour la cryptographie) [4].

## 1.2.5 Framework de l'API Java

Le framework d'applications fournit aux développeurs un ensemble de services et d'API pour créer des applications Android. Il simplifie la réutilisation des composants et services système, permettant aux développeurs de se concentrer sur la logique métier de leurs applications [4].

Parmi les composants clés du framework d'applications, on trouve :

- **Système de vues** : Un ensemble de composants graphiques pour créer l'interface utilisateur des applications (boutons, listes, zones de texte, etc.) [10].
- **Gestionnaire de ressources** : Permet d'accéder aux ressources de l'application, telles que les images, les chaînes de texte et les fichiers de mise en page [11].
- **Gestionnaire de notifications** : Permet aux applications d'afficher des notifications à l'utilisateur [12].
- **Gestionnaire d'activités** : Gère le cycle de vie des activités (écrans) d'une application [13].
- **Fournisseurs de contenu** : Permettent aux applications de partager des données entre elles [14].

### 1.2.6 Applis système

Les applications sont la couche supérieure de l'architecture Android. Ce sont les programmes que les utilisateurs installent et utilisent sur leurs appareils. Elles peuvent être préinstallées (applications système) ou téléchargées depuis le Google Play Store. Les applications système, telles que l'application Téléphone, Contacts ou Messagerie, fournissent des fonctionnalités de base aux utilisateurs et aux développeurs. Les développeurs peuvent accéder à ces fonctionnalités via les API du framework d'applications, ce qui leur évite de les recréer [4].

## 1.3 Gestion de la Mémoire sous Android

La gestion de la mémoire est un aspect essentiel du développement d'Android, car elle garantit que les applications s'exécutent efficacement et ne consomment pas trop de ressources système. Le système de gestion de la mémoire d'Android est conçu pour optimiser l'utilisation des ressources limitées sur les appareils mobiles, qui disposent souvent d'une mémoire réduite par rapport aux systèmes de bureau.

### 1.3.1 Type de mémoire dans Android

Les appareils Android utilisent trois types de mémoire principaux : la **RAM**, la **zRAM** et le **stockage** comme illustré dans la Figure 1.4. Chaque type a une fonction spécifique dans la gestion des données et l'amélioration des performances de l'appareil [15] :

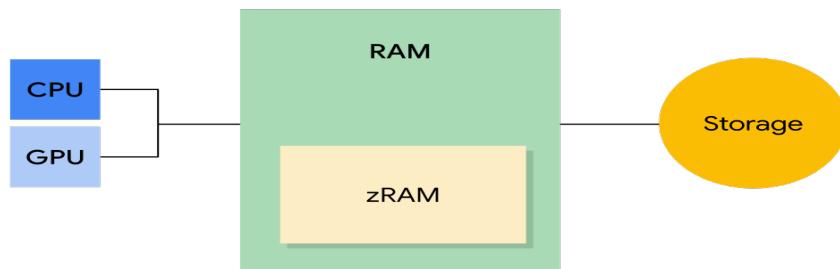


Figure 1.4: Types de mémoire [15]

- **La RAM** est le type de mémoire le plus rapide, mais sa taille est généralement limitée. Les appareils haut de gamme disposent généralement des plus grandes quantités de RAM.
- **La zRAM** est une partition de la RAM utilisée pour l'espace d'échange. Tout est compressé lorsqu'il est placé dans la zRAM, puis décompressé lorsqu'il est copié hors de la zRAM. La taille de cette partie de la RAM augmente ou diminue au

fur et à mesure que des pages sont placées dans la zRAM ou en sont retirées. Les fabricants d'appareils peuvent fixer la taille maximale.

- **Le stockage** conserve toutes les données persistantes, comme le système de fichiers et le code de l'application. Contrairement à la RAM et à la zRAM, le stockage offre une capacité beaucoup plus importante. Il est important de noter qu'Android n'utilise pas le stockage pour l'espace swap, contrairement à d'autres systèmes Linux. Il se concentre plutôt sur la conservation efficace des données utilisateur et système. Une bonne gestion du stockage est essentielle pour maintenir les performances de l'appareil et garantir un espace suffisant pour les données des utilisateurs et des applications.

### 1.3.2 Stratégies d'allocation de mémoire

Android utilise un système d'allocation dynamique de la mémoire pour gérer la mémoire entre les processus, garantissant ainsi une utilisation efficace des ressources limitées. ART emploie des techniques de pagination et de mappage de la mémoire (mmap), où la mémoire modifiée par une application reste résidente dans la RAM et ne peut pas être paginée. Chaque processus d'application est initié par le processus Zygote, qui précharge le code du cadre partagé afin de réduire l'utilisation de la mémoire par les applications. Le système hiérarchise l'allocation de la mémoire en fonction de l'importance du processus, les applications d'avant-plan recevant une priorité plus élevée, tandis que les processus d'arrière-plan peuvent être interrompus pour libérer de la mémoire dans les situations où les ressources sont faibles [16].

### 1.3.3 Pages de mémoire dans Android

Dans Android, la mémoire est divisée en blocs de taille fixe appelés pages, d'une taille typique de 4 Ko. Ces pages constituent la plus petite unité de gestion de la mémoire et sont classées comme **libres (free)** ou **utilisées (used)**. Les pages libres représentent la RAM inutilisée, tandis que les pages utilisées sont activement utilisées par le système et sont classées dans des types spécifiques en fonction de leur objectif et de leur comportement, comme suit [15] :

- **Pages mises en cache** : elles stockent des données qui peuvent être rapidement réutilisées, telles que les ressources de l'application ou les fichiers récemment consultés. Les pages mises en cache améliorent les performances en réduisant le besoin de recharger les données.
- **Pages partagés** : elles sont utilisées pour partager des ressources communes, telles

que les bibliothèques ou le code de l'application, entre plusieurs processus. Cela minimise la redondance et optimise l'utilisation de la mémoire.

- **Pages anonymes** : elles sont privées pour un processus et stockent généralement des données telles que des variables spécifiques à l'application ou des objets d'exécution. Elles ne sont pas soutenues par des fichiers et sont créées dynamiquement pendant l'exécution.

En classant les pages de mémoire en trois catégories, Android garantit une utilisation efficace de la mémoire, réduit la redondance et maintient des performances fluides même dans les situations où la mémoire est faible.

### 1.3.4 Garbage Collection dans Android

Le Garbage Collection (GC) dans Android est un processus de gestion automatique de la mémoire utilisé par les systèmes d'exécution et ART. Ce mécanisme identifie et récupère la mémoire qui n'est plus utilisée par les applications, assurant ainsi une gestion efficace de la mémoire et empêchant les fuites de mémoire qui pourraient dégrader les performances de l'application ou entraîner des plantages. Dans un environnement de mémoire gérée comme ART, le système garde une trace de chaque allocation de mémoire. Lorsqu'il détermine qu'un morceau de mémoire n'est plus utilisé, il libère cette mémoire dans le tas, sans intervention du programmeur. Les principaux objectifs du garbage collection sont de trouver les objets de données auxquels on ne pourra plus accéder à l'avenir et de récupérer les ressources utilisées par ces objets [16].

#### 1.3.4.1 Le tas générational

Android utilise une stratégie de tas générational pour le GC, qui divise la mémoire en différentes régions en fonction de la durée de vie prévue des objets. Cette stratégie comprend généralement les éléments suivants [16] :

- **Jeune génération** : où les nouveaux objets sont alloués. La plupart des objets ont une durée de vie courte et sont rapidement collectés dans cette région.
- **Ancienne génération** : les objets qui ont survécu à plusieurs collectes dans la jeune génération sont promus dans cette région, où ils sont censés avoir une durée de vie plus longue.

#### 1.3.4.2 Avantages du tas générational

- **Efficacité** : En se concentrant sur la jeune génération, où la plupart des objets ont une durée de vie courte, le GC peut être effectué plus efficacement, ce qui réduit

les frais généraux.

- **Réduction des temps de pause** : Cette approche réduit la durée des pauses, qui peuvent perturber l'expérience de l'utilisateur.
- **Amélioration des performances** : Le GC générationnel permet de réduire la fragmentation et d'optimiser l'allocation de la mémoire, ce qui est particulièrement important pour les appareils dont les ressources sont limitées.

### 1.3.5 Mécanisme de gestion de la mémoire faible

Android utilise plusieurs mécanismes pour gérer efficacement les situations de faible mémoire. Ces mécanismes sont basés sur le noyau Linux et sont conçus pour garantir la stabilité et les performances du système, même en cas de pression sur la mémoire. Deux composants clés de la gestion de la mémoire faible d'Android sont le Kernel Swap Daemon (kswapd) et le Low Memory Killer (LMK) [15].

#### 1.3.5.1 Kernel Swap Daemon

Le kswapd est un processus du noyau Linux chargé de gérer la mémoire en récupérant les pages de mémoire inutilisées. Il opère en [15] :

- Identifiant les pages de mémoire qui ne sont plus utilisées activement.
- Echangeant ou libérant ces pages pour faire de la place à de nouvelles allocations.

#### 1.3.5.2 Low Memory Killer

Le LMK est un mécanisme critique spécifique à Android qui fonctionne lorsque le système est soumis à une forte pression de mémoire. Il fonctionne en [15] :

- Surveillant l'état de la mémoire du système par l'intermédiaire du démon Low Memory Killer Daemon (lmkd).
- Terminer les processus en fonction de leur priorité et de leur importance pour l'utilisateur.
- Utilisation d'une stratégie LRU (Least Recently Used) pour déterminer les processus à terminer, afin de s'assurer que les applications les plus essentielles restent actives.

### 1.3.6 Défis de la gestion de la mémoire dans Android

La gestion de la mémoire dans Android présente plusieurs défis que les développeurs doivent relever pour garantir des performances optimales de l'application et l'expérience de l'utilisateur. Voici quelques-uns des principaux défis :

### 1.3.6.1 Les fuites de mémoire

Les fuites de mémoire constituent un problème important dans le développement d'Android. Elles se produisent lorsque des objets sont conservés en mémoire alors qu'ils ne sont plus nécessaires, ce qui empêche le GC d'en récupérer. Cela peut entraîner une augmentation de la consommation de mémoire et un ralentissement des performances de l'application, voire des plantages [17]. Les causes courantes des fuites de mémoire sont les suivantes :

- **Rétention de ressources** : Les instances d'objets tels que les bitmaps et les flux de fichiers, une fois utilisés, ne sont pas explicitement libérées, bloquant inutilement la mémoire.
- **Maintien de références** : Des références d'objets (par exemple via des classes internes, des variables statiques ou des écouteurs d'événements) persistent après que ces objets ne sont plus nécessaires, empêchant leur récupération par le GC.

### 1.3.6.2 Ressources mémoire limitées

Les appareils Android ont souvent une mémoire vive limitée, en particulier les modèles bas de gamme. Le système d'exploitation conserve les applications en mémoire pour permettre des changements rapides, ce qui peut conduire à une très faible quantité de mémoire libre disponible pour de nouveaux processus. Cette mémoire limitée peut entraîner une dégradation des performances et une probabilité accrue de plantage des applications en raison de l'épuisement de la mémoire [15].

### 1.3.6.3 Garbage Collection overhead

Bien qu'Android utilise la fonction automatique garbage collection pour gérer la mémoire, le processus peut entraîner une surcharge. Des cycles fréquents de GC peuvent provoquer des pauses notables dans les performances de l'application, en particulier si l'application alloue et désalloue la mémoire de manière inefficace. Les développeurs doivent comprendre le fonctionnement du garbage collector afin de minimiser son impact sur les performances [18].

Une gestion efficace de la mémoire est essentielle pour développer des applications Android performantes. En comprenant l'architecture de la mémoire d'Android, en reconnaissant les défis et en mettant en œuvre les meilleures pratiques, les développeurs peuvent créer des applications non seulement efficaces, mais qui offrent une expérience utilisateur transparente. Alors qu'Android continue d'évoluer, rester informé sur les techniques et les outils de gestion de la mémoire restera essentiel pour les professionnels du secteur.

## 1.4 Gestion des Disques sous Android

La gestion du stockage dans Android est un aspect critique du système d'exploitation qui assure un traitement et une organisation efficaces des données sur les appareils mobiles. Avec la quantité croissante de données générées par les applications et les utilisateurs, une gestion efficace du stockage devient essentielle pour maintenir les performances de l'appareil et l'expérience de l'utilisateur.

### 1.4.1 Architecture de stockage Android

L'architecture de stockage d'Android offre une approche flexible et sécurisée pour la gestion des données sur les appareils mobiles, s'appuyant sur une hiérarchie inspirée du système de fichiers Linux. Elle répond aux exigences opérationnelles du système et aux attentes des utilisateurs en matière de sécurité et d'accessibilité. Android propose plusieurs options de stockage, telles que le stockage interne sécurisé, le stockage externe partagé, ainsi que des mécanismes pour gérer les préférences de l'utilisateur et les bases de données. Cette variété permet une gestion efficace des données tout en préservant l'expérience utilisateur et la sécurité des applications.

### 1.4.2 Hiérarchie du système de fichiers

La hiérarchie du système de fichiers d'Android est organisée de manière à refléter à la fois les exigences opérationnelles du système et les besoins des utilisateurs. Le système de fichiers racine (« / ») est le répertoire de premier niveau, sous lequel se trouvent plusieurs répertoires importants, notamment :

Répertoire	Fonction
/system	Contient les fichiers du système d'exploitation Android (en lecture seule). Ce répertoire inclut les fichiers système essentiels et les bibliothèques nécessaires au fonctionnement de l'appareil.
/boot	Contient le noyau et l'initial ramdisk (initrd), essentiels pour le démarrage de l'appareil. Cette partition est cruciale pour le processus de démarrage et est généralement en lecture seule.
/data	Stocke les données des applications et de l'utilisateur (par exemple, fichiers privés des applications, bases de données, préférences partagées). C'est l'emplacement principal pour les données des applications et les paramètres utilisateur.

/storage	Point de montage pour le stockage externe/interne (par exemple, /storage/emulated). Ce répertoire offre un accès au stockage interne et externe, permettant aux applications de lire et d'écrire des données.
/dev	Fichiers de périphériques (par exemple, interfaces matérielles). Il contient des nœuds de périphériques représentant les composants matériels, facilitant la communication entre le système d'exploitation et le matériel.
/proc	Système de fichiers virtuel pour les informations système et de processus. Il fournit un mécanisme permettant au noyau d'envoyer des informations aux processus et aux processus d'envoyer des informations au noyau.
/cache	Fichiers temporaires du système (par exemple, mises à jour OTA). Ce répertoire stocke des données mises en cache pour accélérer l'accès aux informations fréquemment utilisées.
/vendor	Fichiers spécifiques au fournisseur (par exemple, pilotes matériels). Il contient des fichiers fournis par le fabricant de l'appareil, y compris des pilotes propriétaires et des configurations.
/mnt	Points de montage temporaires pour le stockage externe ou les partages réseau. Ce répertoire est utilisé pour monter des systèmes de fichiers, tels que des cartes SD ou des partages réseau, pendant le fonctionnement de l'appareil.

**Tableau 1.1:** Répertoires Principaux du Système de Fichiers Android

### 1.4.3 Types de stockage dans Android

Android offre une variété d'options de stockage pour répondre à différents cas d'utilisation, ce qui permet aux développeurs de choisir la méthode la plus appropriée pour les besoins en données de leur application. Voici un aperçu des principaux types de stockage disponibles dans Android [19] :

#### 1.4.3.1 Stockage interne

Le stockage interne dans Android est spécifique à l'application, permettant uniquement à l'application créée d'accéder à ses fichiers, ce qui renforce la sécurité et est idéal pour stocker des données sensibles. Il est particulièrement utile pour enregistrer les informations

d'identification des utilisateurs et les fichiers de configuration, comme le montrent les applications bancaires qui stockent les informations de connexion pour empêcher les accès non autorisés et réduire les risques de violation des données.

#### 1.4.3.2 Stockage externe

Le stockage externe dans Android est un stockage partagé accessible par plusieurs applications, y compris les cartes SD et le stockage intégré. Il est idéal pour les contenus multimédias (photos, vidéos, téléchargements) que les utilisateurs souhaitent partager ou auxquels ils veulent accéder à travers différentes applications.

#### 1.4.3.3 Préférences partagées

Les préférences partagées sont une méthode légère pour stocker de petites quantités de données dans des paires clé-valeur, idéale pour enregistrer les paramètres de l'utilisateur et les configurations d'applications simples. Elles sont couramment utilisées pour stocker les préférences de l'utilisateur, telles que les choix de thèmes et les paramètres de notification, ainsi que des données spécifiques telles que le dernier niveau joué ou les paramètres sonores dans les jeux. Cette approche permet aux développeurs de gérer efficacement les données et d'améliorer la personnalisation et la convivialité des applications.

#### 1.4.3.4 Bases de données

Android utilise des bases de données SQLite pour le stockage de données structurées, ce qui le rend adapté aux applications qui gèrent des ensembles de données relationnelles complexes. Cette méthode est particulièrement efficace pour les opérations de données étendues dans les plateformes de commerce électronique et les applications de médias sociaux. En utilisant SQLite, les développeurs peuvent interroger, mettre à jour et organiser les données de manière efficace, ce qui permet de créer des applications robustes et réactives capables de gérer de gros volumes d'informations.

#### 1.4.3.5 Stockage cloud

Des services comme Google Drive, Dropbox et OneDrive offrent un stockage distant accessible via Internet. Ce type de stockage permet aux utilisateurs de synchroniser leurs données sur plusieurs appareils et de libérer de l'espace sur leur appareil.

Le système de gestion du stockage d'Android est conçu pour équilibrer la flexibilité, la sécurité et la facilité d'utilisation. Grâce à des fonctionnalités telles que le gestionnaire de stockage, le stockage délimité et la prise en charge de différents types de stockage,

Android permet aux utilisateurs et aux développeurs de gérer efficacement les données tout en préservant la confidentialité et les performances.

## 1.5 Open source

### 1.5.1 Qu'est-ce que l'Open Source ?

Un logiciel open source est un logiciel dont le code source est accessible au public. Cela signifie que n'importe qui peut consulter, modifier et distribuer le code. L'open source repose sur des principes de collaboration, de transparence et de liberté. Il est important de noter que l'open source ne signifie pas "gratuit". Les logiciels open source peuvent être distribués gratuitement, mais ils peuvent aussi être vendus commercialement. Ce qui définit l'open source, c'est la liberté d'accès au code source et la possibilité de le modifier et de le redistribuer selon les termes d'une licence open source. Ces licences définissent les droits et les obligations des utilisateurs du logiciel, notamment en ce qui concerne la modification et la redistribution du code [20].

Les implications de l'open source sont nombreuses :

- **Collaboration** : L'open source encourage la collaboration entre développeurs du monde entier, ce qui peut accélérer le développement et l'amélioration du logiciel.
- **Transparence** : Le code source étant accessible, les utilisateurs peuvent vérifier le fonctionnement du logiciel et identifier d'éventuels problèmes de sécurité.
- **Liberté** : Les utilisateurs sont libres d'utiliser, modifier et distribuer le logiciel comme bon leur semble, sans restriction de licence (sous réserve des termes de la licence open source).

### 1.5.2 Types de licences Open Source

Il existe plus de 80 variantes de licences de logiciels libres, mais elles se classent généralement dans l'une des deux catégories principales suivantes [21] :

#### 1.5.2.1 Licences permissives

Les licences open source permissives permettent aux utilisateurs d'utiliser, de modifier et de distribuer des logiciels avec un minimum de restrictions, sans exiger que les travaux dérivés restent open source. Parmi les exemples, on peut citer la licence Apache 2.0, qui autorise la modification et la redistribution à des fins commerciales moyennant une attribution appropriée, la licence MIT et qui n'exige que l'attribution aux auteurs originaux.

Ces licences sont particulièrement populaires dans les projets commerciaux de logiciels libres en raison de leur flexibilité et de leur facilité d'utilisation [22].

#### 1.5.2.2 Licences copyleft

Les licences Copyleft exigent que tout travail dérivé soit distribué sous la même licence, ce qui garantit que le logiciel reste libre et ouvert. La licence publique générale GNU (GPL) exige que les modifications soient également soumises à la licence GPL, tandis que la licence publique générale amoindrie (LGPL) offre une approche plus permissive, souvent utilisée pour les bibliothèques, autorisant l'intégration avec des logiciels propriétaires sous certaines conditions. Ce cadre de licence favorise le partage et l'amélioration continus au sein de la communauté des logiciels libres [23].

#### 1.5.3 Licences Open Source utilisé par Android

Android est basé sur un noyau Linux, formant la fondation technique de la plateforme. Une grande partie d'Android est développée au sein de l'Android Open Source Project (AOSP), dirigé par Google, qui fournit le code source sous la licence Apache 2.0. Cette licence permet aux développeurs d'utiliser, modifier et distribuer le code librement, y compris à des fins commerciales. Cependant, Android n'est pas complètement open source et utilise plusieurs licences, dont :

- **Licence Apache 2.0** : Majoritairement appliquée à AOSP, elle autorise l'utilisation et la distribution, même pour des usages propriétaires [24].
- **Licence GNU GPL** : S'applique à certains composants, comme le noyau Linux, exigeant que les dérivés soient également distribués sous GPL [23].
- **Autres licences** : Comprend des composants sous d'autres licences open source comme MIT ou BSD [25].

Cette diversité de licences confère à Android la flexibilité nécessaire pour intégrer des éléments propriétaires, ce qui le qualifie de "partiellement open source".

#### 1.5.4 Avantages de l'Open Source

- **Flexibilité** : La possibilité de modifier le code source permet aux fabricants de personnaliser Android pour leurs appareils et aux développeurs de créer des applications innovantes.
- **Communauté** : La communauté open source contribue au développement et à l'amélioration d'Android en signalant des bugs, en proposant des correctifs et en développant de nouvelles fonctionnalités.

- **Coût** : L'utilisation d'une base open source peut réduire les coûts de développement pour les fabricants d'appareils.

### 1.5.5 Inconvénients de l'Open Source

- **Fragmentation** : La liberté de modification du code source peut entraîner une fragmentation de l'écosystème Android, avec des versions différentes du système d'exploitation sur différents appareils. Cela peut compliquer le développement d'applications et la maintenance du système. Par exemple, les applications peuvent ne pas fonctionner correctement sur toutes les versions d'Android, et les mises à jour de sécurité peuvent être déployées de manière inégale.
- **Sécurité** : La disponibilité du code source peut faciliter l'identification de failles de sécurité par des personnes malveillantes. En rendant le code accessible à tous, y compris aux pirates, l'open source peut potentiellement augmenter la surface d'attaque et exposer le système à des vulnérabilités.
- **Dépendance à Google** : Malgré la base open source, Android reste fortement dépendant des services Google, ce qui peut poser des problèmes de confidentialité et de liberté pour les utilisateurs.

## 1.6 Principales caractéristiques d'Android

- **Interface utilisateur personnalisable** : Android offre des options de personnalisation étendues aux fabricants d'appareils et aux utilisateurs. Les fabricants peuvent créer des interfaces utilisateur personnalisées (UI skins) et les utilisateurs peuvent personnaliser leurs appareils avec des widgets, des thèmes et des fonds d'écran.
- **Écosystème d'applications** : Android donne accès au Google Play Store, un vaste marché où les utilisateurs peuvent télécharger et installer des applications à des fins diverses : productivité, divertissement, éducation, jeux, etc.
- **Notifications** : Le système de notification d'Android permet aux applications d'envoyer des mises à jour et des alertes aux utilisateurs, leur fournissant des informations pertinentes sans qu'ils aient besoin d'ouvrir l'application.
- **Connectivité** : Les appareils Android prennent en charge diverses options de connectivité, telles que Wi-Fi, Bluetooth, NFC et données mobiles, ce qui permet aux utilisateurs de rester connectés à l'internet et à d'autres appareils.
- **Intégration avec les services Google** : Android s'intègre étroitement à l'écosystème de Google, notamment à des services tels que Google Search, Google Maps,

Gmail, Google Drive et bien d'autres, ce qui améliore l'expérience globale de l'utilisateur.

- **Contrôle gestuel** : Android 10 a également introduit des fonctions de contrôle gestuel, telles que le balayage du bord gauche ou droit de l'écran pour revenir en arrière, ce qui rend la navigation plus intuitive et plus pratique.

## 1.7 Android os et la sécurité

Android est doté d'un cadre de sécurité solide conçu pour protéger les données des utilisateurs et garantir l'utilisation sûre des applications. Grâce à des fonctionnalités telles que Google Play Protect, des mises à jour de sécurité régulières et un modèle d'autorisation rigoureux, Android offre une protection efficace contre les menaces potentielles. Toutefois, malgré ces atouts considérables, la plateforme n'est pas exempte de défis. La nature fragmentée de l'écosystème Android, caractérisée par la diversité des fabricants d'appareils et des niveaux de prise en charge des mises à jour, crée des vulnérabilités qui peuvent être exploitées par des acteurs malveillants. De plus, les utilisateurs ont souvent du mal à distinguer les applications sûres des applications nuisibles, en particulier lorsqu'ils les téléchargent à partir de sources tierces. Alors que le paysage des cybermenaces continue d'évoluer, l'équilibre entre les impressionnantes fonctions de sécurité d'Android et les vulnérabilités inhérentes reste un défi permanent pour les développeurs comme pour les utilisateurs.

Ci-dessous, vous trouverez une variété de fonctions de sécurité disponibles sur les appareils Android, ainsi que plusieurs défis communs en matière de sécurité Android.

### 1.7.1 Fonctions de sécurité d'Android

#### 1.7.1.1 Bac à sable d'application

Android tire parti de la protection Linux basée sur l'utilisateur pour identifier et isoler les ressources des applications. Pour ce faire, Android attribue à chaque application un identifiant unique (UID) et l'exécute dans son propre processus. Android utilise cet identifiant pour mettre en place un bac à sable applicatif au niveau du noyau [26].

#### 1.7.1.2 Signature d'application

La signature des applications permet aux développeurs d'identifier l'auteur de l'application et de mettre à jour leur application sans créer d'interfaces et d'autorisations

compliquées. Chaque application fonctionnant sur la plateforme Android doit être signée par le développeur [27].

#### **1.7.1.3 Authentication**

Android utilise le concept de clés cryptographiques liées à l'authentification de l'utilisateur qui nécessite un stockage des clés cryptographiques et des authentificateurs du fournisseur de services et de l'utilisateur. Sur les appareils équipés d'un capteur d'empreintes digitales, les utilisateurs peuvent enregistrer une ou plusieurs empreintes digitales et les utiliser pour déverrouiller l'appareil et effectuer d'autres tâches. Le sous-système Gatekeeper effectue l'authentification du modèle de l'appareil ou du mot de passe dans un environnement d'exécution de confiance (TEE). Android 9 et les versions ultérieures incluent la confirmation protégée, qui permet aux utilisateurs de confirmer formellement les transactions critiques, telles que les paiements [28].

#### **1.7.1.4 Biométrie**

Android 9 et les versions ultérieures comprennent une API BiometricPrompt que les développeurs d'applications peuvent utiliser pour intégrer l'authentification biométrique dans leurs applications de manière agnostique en termes d'appareils et de modalités. Seule la biométrie forte peut être intégrée à BiometricPrompt [29].

#### **1.7.1.5 Chiffrement**

Une fois qu'un appareil est crypté, toutes les données créées par l'utilisateur sont automatiquement cryptées avant d'être enregistrées sur le disque et toutes les lectures décryptent automatiquement les données avant de les renvoyer au processus d'appel. Le cryptage garantit que même si une partie non autorisée tente d'accéder aux données, elle ne peut pas les lire [30].

#### **1.7.1.6 Keystore**

Android propose une base de données matérielle qui permet de générer des clés, d'importer et d'exporter des clés asymétriques, d'importer des clés symétriques brutes, de chiffrer et de déchiffrer des données asymétriques avec des modes de remplissage appropriés, et bien plus encore [31].

### 1.7.1.7 Linux à sécurité améliorée

Dans le cadre du modèle de sécurité Android, Android utilise Security-Enhanced Linux (SELinux) pour appliquer le contrôle d'accès obligatoire (MAC) à tous les processus, même ceux qui s'exécutent avec les priviléges de l'utilisateur principal ou du superutilisateur (capacités Linux) [32].

### 1.7.1.8 Trusty Trusted Execution Environment (TEE)

Trusty est un système d'exploitation (OS) sécurisé qui fournit un environnement d'exécution de confiance (TEE) pour Android. Le système d'exploitation Trusty fonctionne sur le même processeur que le système d'exploitation Android, mais Trusty est isolé du reste du système à la fois par le matériel et le logiciel [33].

### 1.7.1.9 Démarrage vérifié

Verified Boot s'efforce de garantir que tout le code exécuté provient d'une source fiable (généralement les équipementiers), et non d'un attaquant ou d'une corruption. Il établit une chaîne de confiance complète, allant d'une racine de confiance protégée par le matériel au chargeur d'amorçage, à la partition d'amorçage et aux autres partitions vérifiées [34].

## 1.7.2 Défis liés à la sécurité d'Android

### 1.7.2.1 Rooting

Autoriser un appareil Android à installer une application infectée par un logiciel malveillant permet à ce code malveillant de contourner la plupart des mécanismes de sécurité intégrés au système. Cependant, si vous rootez votre appareil pour contourner la couche de restrictions d'Android, vous mettez également de côté les mécanismes de sécurité qui protègent votre système contre les codes malveillants que vous n'avez pas autorisés à s'exécuter sur votre appareil. Les appareils Android sont donc plus susceptibles d'être infectés par des cyberattaques basées sur Internet et de propager ces infections sur les réseaux d'entreprise auxquels ils se connectent [35].

### 1.7.2.2 App Permissions

Bien qu'Android dispose d'un système de permissions robuste, les applications peuvent encore demander des permissions qui peuvent être confuses ou perçues comme risquées par les utilisateurs. Cela peut conduire les utilisateurs à ne pas installer une application ou à accorder des autorisations alors que le créateur de l'autorisation n'a pas été installé [36].

### 1.7.2.3 Insecure Apps

Une autre menace pour la sécurité des appareils Android provient de la nature ouverte du processus de soumission d'applications sur Google Play : les applications ne sont pas livrées avec un code malveillant, mais utilisent une conception logicielle non sécurisée. Lorsque les développeurs laissent des failles de sécurité dans leur code, les pirates ou les logiciels malveillants peuvent les exploiter pour compromettre votre appareil. Le code malveillant utilise les autorisations que vous avez accordées à l'application non sécurisée pour contourner la sécurité de votre appareil, à la manière dont des voleurs dérobent les cartes-clés d'employés involontaires dans les films [35].

### 1.7.2.4 Google Play Malware

L'un des principaux risques de sécurité dans l'écosystème Android est le risque de téléchargement d'applications de la boutique Google Play contenant des logiciels malveillants. Google permet aux développeurs d'ajouter facilement leurs applications à son magasin d'applications, ce qui crée une vaste sélection d'applications pour les utilisateurs d'Android. Toutefois, le manque de rigueur de la boutique permet aux programmeurs de télécharger plus facilement sur Google Play des applications contenant des codes malveillants. Ces applications malveillantes peuvent se faire passer pour n'importe quoi, des jeux aux utilitaires antivirus Android [35].

### 1.7.2.5 Nayure Open Source

Le code source ouvert d'Android permet un examen approfondi par les développeurs et les attaquants potentiels, ce qui peut conduire à la découverte et à l'exploitation de vulnérabilités. Cette ouverture contribue également à la fragmentation de l'écosystème, car les différents fabricants modifient le système d'exploitation pour l'adapter à leurs appareils, ce qui donne lieu à un large éventail de configurations matérielles et logicielles [24].

### 1.7.2.6 Fragmentation de versions

La fragmentation complique le processus de diffusion des mises à jour de sécurité dans les délais impartis sur tous les appareils. Les fabricants d'appareils et les opérateurs sont responsables de la mise en œuvre et de la distribution de ces mises à jour, ce qui peut entraîner des retards et des incohérences. Certains appareils plus anciens peuvent rester vulnérables à des risques de sécurité pendant de longues périodes [35].

## Conclusion

Ce premier chapitre a jeté les bases essentielles à notre étude en explorant en profondeur l'environnement Android : son histoire, son architecture, ses composants clés, son modèle open source, l'évolution de ses récentes versions et ses caractéristiques. Un regard attentif a été porté sur la sécurité, enjeu crucial pour une application de contrôle parental.

Forts de cette compréhension d'Android, nous abordons le cœur de notre sujet : les applications de messagerie instantanée. Le chapitre suivant se concentrera sur une analyse détaillée de ces applications, avec un focus sur WhatsApp, plateforme de communication mondiale majeure.

# Chapitre 2

## Les Applications de Messagerie Instantanée : Un aperçu complet avec un focus sur WhatsApp

### Introduction

La messagerie instantanée a transformé notre manière de communiquer, proposant une alternative rapide et pratique aux appels téléphoniques et aux SMS traditionnels. Des applications telles que WhatsApp, Telegram et Signal sont désormais des outils incontournables de notre quotidien. Elles nous permettent d'échanger des messages, des photos, des vidéos, mais aussi d'effectuer des appels vocaux et vidéo en temps réel. Cette analyse approfondie des applications de messagerie instantanée examine leur évolution, leurs caractéristiques techniques et leur impact sur la société, en mettant particulièrement l'accent sur WhatsApp, l'une des applications les plus populaires au monde.

### 2.1 Applications de messagerie instantanée

#### 2.1.1 Introduction aux applications de messagerie instantanée

##### 2.1.1.1 Définition

La messagerie instantanée désigne une forme de communication textuelle dans laquelle deux ou plusieurs personnes échangent des messages en temps réel ou de manière asynchrone par le biais d'applications logicielles dédiées ou de plates-formes de chat intégrées. Ces applications permettent aux utilisateurs d'envoyer du texte, du multimédia et même

des fichiers sur l'internet, ce qui permet une communication transparente entre les différents appareils [37].

### **2.1.1.2 Évolution**

L'évolution de la messagerie instantanée a été remarquable, passant d'une communication textuelle de base à des plateformes riches en fonctionnalités. Les premières formes de messagerie instantanée ont vu le jour à la fin des années 1980 et au début des années 1990 avec l'Internet Relay Chat (IRC) [38], qui permettait de communiquer en temps réel au sein d'un groupe. Au milieu des années 1990, ICQ est devenu l'une des premières messageries instantanées commercialisées, suivi par d'autres services comme AOL Instant Messenger (AIM).

Les années 2000 ont vu l'essor des plateformes de messagerie instantanée sur mobile, dont BlackBerry Messenger (BBM) est un exemple notable. L'introduction de WhatsApp en 2009 et d'autres applications comme Telegram et WeChat a révolutionné l'espace en offrant le partage multimédia, le cryptage bout en bout et la compatibilité multiplateforme. Dans le monde de l'entreprise, des outils comme Slack (2013) et Microsoft Teams (2017) ont introduit la collaboration en temps réel et l'intégration avec des outils de productivité, redéfinissant ainsi la communication sur le lieu de travail [39].

## **2.1.2 Caractéristiques des Applications de Messagerie Instantanée**

Les applications de messagerie instantanée se distinguent par un ensemble de caractéristiques qui les rendent populaires et fonctionnelles pour les utilisateurs. Voici les principales fonctionnalités qui définissent ces plateformes [40] :

### **2.1.2.1 Messagerie en temps réel**

Les applications de messagerie instantanée permettent de communiquer instantanément avec ses contacts. Elles offrent également la possibilité d'envoyer et de recevoir des messages presque instantanément. Cela favorise des échanges fluides et dynamiques entre les utilisateurs.

### **2.1.2.2 Bots et automatisation**

De nombreuses applications intègrent des bots qui automatisent certaines interactions, facilitant les réponses instantanées aux demandes fréquentes, la gestion des réservations

ou l'assistance client. Ces systèmes améliorent l'expérience utilisateur et augmentent l'efficacité des communications.

#### **2.1.2.3 Discussions de groupe**

Les fonctionnalités de discussion de groupe permettent à plusieurs utilisateurs de converser simultanément, ce qui rend la coordination de projets ou les échanges entre amis plus simples et organisés. Ils peuvent également partager des idées, des fichiers et des informations en temps réel.

#### **2.1.2.4 Partage multimédia**

Les applications de messagerie instantanée permettent de partager facilement différents types de contenus multimédias, comme des images, des vidéos, des fichiers audio et des documents. Cette capacité d'échange enrichit les conversations et offre une meilleure expérience de communication.

#### **2.1.2.5 Appels vocaux et vidéo**

La possibilité d'effectuer des appels vocaux et vidéo directement via l'application est une caractéristique essentielle, permettant aux utilisateurs de se connecter de manière plus personnelle et interactive, sans nécessiter d'autres services ou logiciels.

#### **2.1.2.6 Cryptage**

La sécurité des données est une préoccupation majeure pour de nombreux utilisateurs. Les applications de messagerie instantanée utilisent des protocoles de cryptage pour protéger les conversations et assurer ainsi la confidentialité et la sécurité des informations échangées entre les utilisateurs.

Ces caractéristiques combinées font des applications de messagerie instantanée un outil essentiel pour la communication moderne, tant sur le plan personnel que professionnel. Elles continuent de s'adapter et d'évoluer en fonction des attentes croissantes des utilisateurs en matière de fonctionnalités et de sécurité.

### **2.1.3 Applications de Messagerie Instantanée Populaires**

Les applications de messagerie instantanée sont effectivement au cœur de la communication moderne, offrant aux utilisateurs des moyens rapides et efficaces de rester connectés. Voici une synthèse des applications les plus populaires :

### **2.1.3.1 WhatsApp**



WhatsApp est une application de messagerie instantanée de premier plan qui compte plus de 2 milliards d'utilisateurs actifs dans le monde. Elle permet aux utilisateurs d'envoyer des messages texte, de passer des appels vocaux et vidéo et de partager des fichiers multimédias, tout en prenant en charge les discussions de groupe et les mises à jour instantanées de statut. L'une des principales caractéristiques de WhatsApp est son cryptage de bout en bout, qui garantit la confidentialité et la sécurité des communications. L'application est disponible sur plusieurs plateformes, dont Android, iOS et les ordinateurs de bureau, et utilise les données Internet pour proposer une messagerie à faible coût. En outre, WhatsApp Business fournit aux entreprises des outils leur permettant de communiquer avec leurs clients par le biais d'une messagerie et d'une assistance automatisées, ce qui étend son utilisation aussi bien dans un contexte personnel que professionnel [41].

### **2.1.3.2 WeChat**



WeChat est une application polyvalente de messagerie, de médias sociaux et de paiement mobile développée par Tencent en Chine. Elle compte plus d'un milliard d'utilisateurs depuis son lancement en 2011. Elle permet aux utilisateurs d'envoyer des messages, de passer des appels, de partager des contenus multimédias et de publier des mises à jour sur Moments. WeChat se distingue par l'intégration de divers services, notamment des jeux, des achats en ligne et l'accès à des services gouvernementaux, ainsi que par la prise en charge de mini-programmes qui améliorent les fonctionnalités. WeChat Pay offre des options de paiement mobile transparentes, ce qui le rend populaire pour les transactions. Dans l'ensemble, WeChat a considérablement modifié la communication et l'interaction dans le cadre personnel et professionnel, en particulier en Chine [42].

### **2.1.3.3 Facebook Messenger**



Facebook Messenger est une application de messagerie très répandue, développée par Facebook et lancée en 2011. Elle permet une communication transparente par le biais d'appels textuels, vocaux et vidéo, et permet aux utilisateurs d'envoyer des messages multimédias, de partager des photos et des vidéos, et de participer à des discussions de groupe. Ses principales fonctionnalités sont le transfert d'argent, l'intégration avec les services Facebook et la prise en charge des chatbots. L'application propose également des éléments interactifs tels que des

autocollants et des jeux, ce qui renforce l'engagement des utilisateurs. Avec des milliards d'utilisateurs dans le monde, Messenger a transformé la communication et s'est imposé comme un outil essentiel pour communiquer avec ses amis, sa famille et ses entreprises [43].

#### **2.1.3.4 Telegram**



Telegram est une application de messagerie basée sur le cloud lancée en 2013 par Pavel Durov et connue pour sa rapidité et sa sécurité. Elle offre diverses options de communication, notamment la messagerie texte, les appels vocaux et vidéo et les chats de groupe, ainsi que la possibilité de partager des fichiers volumineux et de créer des canaux et des supergroupes pour des milliers de membres. L'application met l'accent sur la protection de la vie privée grâce à des fonctionnalités telles que le chiffrement bout en bout pour les discussions secrètes et l'autodestruction des messages. En outre, Telegram prend en charge les robots pour l'automatisation des tâches et offre une interface conviviale avec des thèmes et des autocollants personnalisables. Telegram a ainsi conquis des millions d'utilisateurs dans le monde entier, devenant une alternative populaire aux autres plateformes de messagerie [44].

## **2.2 WhatsApp**

### **2.2.1 Introduction à WhatsApp**

WhatsApp est une application de messagerie instantanée multiplateforme qui permet aux utilisateurs d'envoyer des messages texte, des messages vocaux, des images, des vidéos et de passer des appels vocaux et vidéo. Elle appartient à Meta Platforms (anciennement Facebook) et est l'une des applications de communication les plus utilisées au monde. En juin 2023, WhatsApp comptait environ 2,78 milliards d'utilisateurs actifs uniques dans le monde [45]. L'application est également populaire auprès des entreprises, WhatsApp Business connaissant une croissance significative, avec notamment 300 millions de téléchargements en 2023 [46].

### **2.2.2 Histoire de WhatsApp**

WhatsApp a été fondée en 2009 par Brian Acton et Jan Koum, tous deux anciens employés de Yahoo. L'application a d'abord été conçue comme une plateforme de partage de statuts, où les utilisateurs pouvaient afficher des mises à jour à côté de leur nom. Koum l'a baptisée « WhatsApp » pour évoquer l'expression « what's up » [47].

En 2013, l'application est passée d'un service payant à un modèle freemium, ce qui a considérablement accru sa popularité. Les premiers défis ont été les pannes de serveur et les contraintes financières, mais l'accent mis par les fondateurs sur la protection de la vie privée et l'expérience des utilisateurs a permis à l'application de prospérer. En 2014, WhatsApp a été racheté par Facebook (aujourd'hui Meta) pour 19 milliards de dollars, marquant ainsi l'une des plus grandes acquisitions technologiques de l'histoire [47].

Au fil des ans, WhatsApp a introduit plusieurs fonctionnalités, notamment les appels vocaux et vidéo, les discussions de groupe et WhatsApp Business, qui s'adresse aux utilisateurs commerciaux. Son chiffrement de bout en bout, introduit en 2016, a encore renforcé sa réputation de plateforme de messagerie sécurisée.

### **2.2.3 Caractéristiques de WhatsApp**

WhatsApp est une plateforme de messagerie puissante qui offre une grande variété de fonctionnalités répondant aux besoins de communication personnels et professionnels. Voici quelques-unes de ses fonctionnalités les plus remarquables :

- **Chiffrement de bout en bout** : Le cryptage de bout en bout, garantit que seul le destinataire prévu peut lire les messages [48].
- **Discussions de groupe** : Les discussions de groupe permettent à plusieurs utilisateurs de partager des informations, de coordonner des événements et de discuter de divers sujets en temps réel [49].
- **Partage multimédia** : Les utilisateurs peuvent facilement partager des images, des vidéos, des documents et même leur position sur WhatsApp. Cette polyvalence a rendu l'application indispensable pour la communication personnelle et professionnelle [50].
- **Appels vocaux et vidéo** : WhatsApp a dépassé le stade de la messagerie texte et propose désormais des appels vocaux et vidéo de haute qualité [51].
- **Accessibilité multiplateforme** : WhatsApp est une plateforme très polyvalente qui fonctionne de manière transparente sur plusieurs appareils, notamment les smartphones Android et iOS, ainsi que sur les ordinateurs grâce à WhatsApp Web et aux applications de bureau dédiées pour Windows et MacOs [51].

### **2.2.4 Popularité**

En avril 2024, WhatsApp continue de dominer le marché mondial des applications de messagerie avec environ deux milliards d'utilisateurs mensuels, ce qui en fait la messagerie

mobile la plus populaire au monde. Après WhatsApp, WeChat possède une base d'utilisateurs importante, en particulier en Chine, tandis que Facebook Messenger se classe troisième avec près d'un milliard d'utilisateurs, bien qu'il ait connu une baisse des téléchargements ces dernières années. Parmi les autres concurrents notables, citons Telegram, reconnu pour sa rapidité et ses fonctions de sécurité, qui séduit les utilisateurs privilégiant la confidentialité de leurs communications [52].

En conclusion, le leadership de WhatsApp sur le marché des applications de messagerie témoigne de son importance dans la communication moderne.

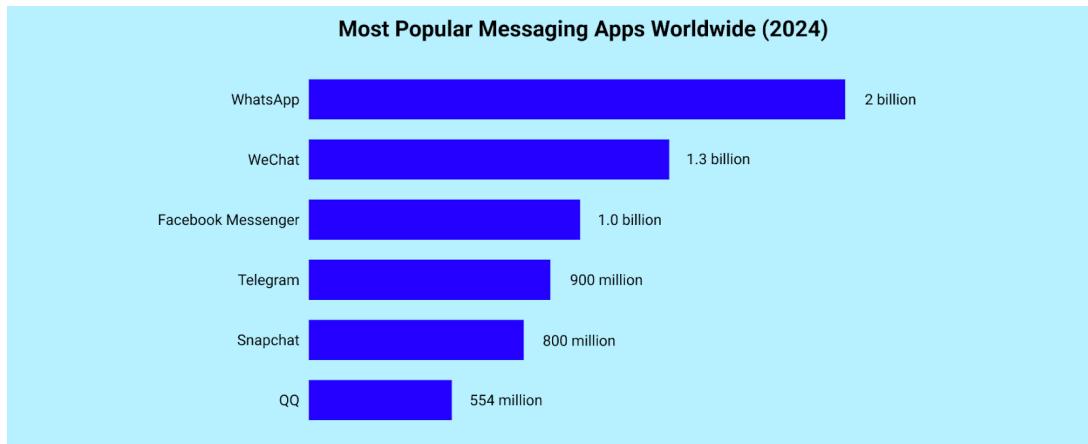


Figure 2.1: Les applications de messagerie les plus utilisées dans le monde en 2024 [52]

## 2.2.5 Architecture technique de WhatsApp

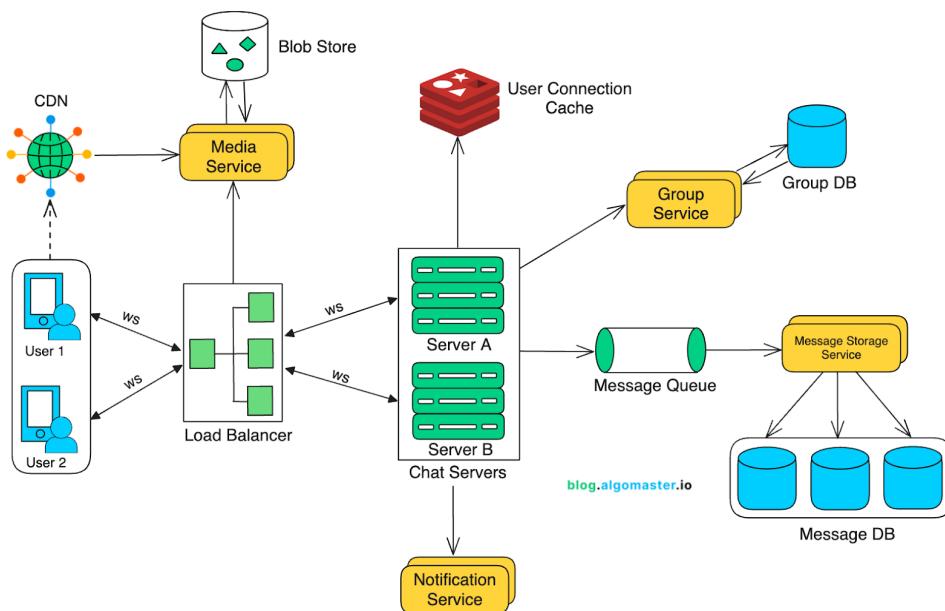


Figure 2.2: Diagramme de l'architecture de WhatsApp [55]

L'architecture de WhatsApp est conçue pour gérer des milliards d'utilisateurs tout en garantissant une messagerie en temps réel, ainsi que la sécurité et l'évolutivité. Pour ce faire, elle s'appuie sur un système complexe optimisé pour la vitesse et la fiabilité. Vous trouverez ci-dessous une vue d'ensemble de ses principaux composants architecturaux :

#### **2.2.5.1 Modèle client-serveur**

WhatsApp utilise un modèle client-serveur comme élément fondamental de son architecture. Voici comment cela fonctionne dans le contexte de WhatsApp :

→ **Côté client** : L'application WhatsApp agit comme un client sur plusieurs plateformes, notamment Android, iOS et le web :

- Elle utilise une base de données SQLite légère pour stocker les conversations localement sur l'appareil de l'utilisateur.
- WebSockets pour une connectivité persistante et en temps réel avec ses serveurs afin de faciliter l'envoi et la réception de messages de manière transparente.
- Le chiffrement bout en bout via le protocole Signal pour garantir que seuls l'expéditeur et le destinataire prévus peuvent déchiffrer les messages.
- En ce qui concerne les tâches qui ne se déroulent pas en temps réel, telles que le téléchargement de médias, WhatsApp communique avec ses serveurs via HTTP et utilise XMPP ou un protocole personnalisé pour la messagerie. Lorsqu'un utilisateur envoie un message, le client le crypte avec la clé publique du destinataire avant de l'envoyer aux serveurs de WhatsApp, qui n'agissent qu'en tant qu'intermédiaires dans le processus de communication [53].

→ **Côté serveur** : La stratégie de mise à l'échelle du côté serveur de WhatsApp est méticuleusement conçue pour gérer sa vaste base d'utilisateurs, tout en garantissant une haute disponibilité, une faible latence et des performances stables. La plateforme combine diverses technologies et principes architecturaux pour atteindre ces objectifs [54].

Principaux éléments de la stratégie de mise à l'échelle du serveur de WhatsApp :

- **Microservices** : WhatsApp utilise une architecture microservices, ce qui permet de structurer l'application comme une collection de services faiblement couplés, chacun dédié à des fonctionnalités spécifiques et communiquant par le biais d'API bien définies. Cette conception permet de dimensionner les serveurs de chat, qui gèrent de nombreuses connexions simultanées et facilitent la communication en temps réel avec une latence minimale grâce à des protocoles tels que les WebSockets, de manière indépendante en fonction de la demande, ce qui améliore l'évolutivité globale de la plateforme. En outre, la résilience de

l'architecture signifie qu'en cas de défaillance d'un service, les autres services restent opérationnels, garantissant ainsi une grande fiabilité. Les microservices permettent également de développer et de déployer rapidement de nouvelles fonctionnalités sans revoir l'ensemble du système [54].

- **Équilibrage de charge** : consiste à répartir le trafic sur plusieurs serveurs, ce qui améliore considérablement les performances et la fiabilité d'une application en évitant qu'un seul serveur ne soit submergé. WhatsApp utilise l'équilibrage de charge pour faire évoluer efficacement sa plateforme de plusieurs façons. En répartissant le trafic entre ses serveurs, l'équilibrage de la charge garantit qu'aucun serveur n'est surchargé, ce qui améliore les performances globales pour les utilisateurs. En outre, cette technique améliore la résistance de la plateforme aux pannes : si un serveur tombe en panne, les autres serveurs peuvent continuer à gérer le trafic, ce qui maintient la fiabilité globale de la plateforme [54].
- **Cache** : La mise en cache est une technique qui améliore les performances des applications en stockant les données fréquemment consultées dans des emplacements très performants tels que la mémoire ou les disques d'état solide, ce qui réduit la fréquence d'accès à la base de données. WhatsApp exploite diverses stratégies de mise en cache pour faire évoluer sa plateforme de manière efficace. Il s'agit notamment de la mise en cache en mémoire, où les données fréquemment consultées sont stockées pour une récupération rapide, et de la mise en cache sur disque pour un stockage persistant. En outre, WhatsApp utilise la mise en cache distribuée pour répartir les données sur plusieurs serveurs, ce qui améliore l'évolutivité. Un composant spécialisé de ce système de mise en cache est le cache de connexion de l'utilisateur, qui utilise des solutions rapides en mémoire comme Redis pour stocker les détails de la connexion active de chaque utilisateur, y compris le serveur de chat auquel il est lié et l'horodatage de sa dernière activité. Les clients envoient périodiquement des signaux de battement de cœur pour mettre à jour leur horodatage **last\_active**, ce qui permet à WhatsApp de gérer efficacement le statut **en ligne/hors ligne** et les fonctionnalités **last seen**. Si le temps écoulé depuis l'horodatage **last\_active** est inférieur à un seuil défini, cette configuration permet à l'application de refléter efficacement la présence de l'utilisateur en temps réel [54].
- **Service de notification** : est essentiel pour envoyer des notifications en temps réel aux utilisateurs, en particulier lorsqu'ils sont déconnectés. Lorsqu'un utilisateur est déconnecté, le serveur de chat transmet les messages entrants au service de notification, ce qui permet à l'utilisateur de recevoir des messages,

même s'il n'utilise pas l'application. Pour améliorer l'efficacité, le serveur de chat utilise une file d'attente de messages plutôt que de contacter directement le service de notification, ce qui réduit les délais potentiels. Le service est également compatible avec des fournisseurs de notifications push tels que Firebase Cloud Messaging (FCM) et Apple Push Notification Service (APNS), ce qui permet de délivrer des messages sous forme de notifications push, et ainsi d'encourager l'engagement des utilisateurs dans leurs conversations lorsqu'ils reviennent en ligne [55].

- **Service des messages :** Le service de messagerie de WhatsApp comprend trois éléments : la file d'attente des messages, le service de stockage des messages et la base de données des messages. La file d'attente des messages est un système distribué à haut débit qui conserve temporairement les messages avant qu'ils ne soient traités par le service de stockage. Ce système agit comme un intermédiaire, séparant le stockage des messages du traitement en temps réel sur les serveurs de chat, réduisant ainsi la latence et améliorant l'évolutivité de l'application. Le service de stockage des messages est chargé de stocker les messages de chat de manière fiable, de les récupérer rapidement et de les archiver efficacement. Il extrait les messages entrants de la file d'attente des messages et les enregistre dans la base de données des messages, conçue pour un débit d'écriture élevé et une récupération efficace afin de gérer le grand volume de messages typique des applications de chat en temps réel, tout en garantissant aux utilisateurs un accès transparent à leurs anciens messages [55].
- **Service de groupe :** est essentiel pour gérer toutes les fonctions liées aux groupes, comme la création de groupes, la mise à jour de leurs détails et le suivi de leurs membres. Lorsqu'un message est envoyé à une discussion de groupe, les serveurs de discussion interrogent le service Groupes pour obtenir la liste actuelle des membres du groupe. La base de données des groupes permet de stocker et de récupérer toutes les informations relatives aux groupes de discussion, y compris les identifiants, les listes de membres, les rôles des administrateurs et les paramètres [55].
- **Service de médias :** est responsable du téléchargement et de la gestion du contenu multimédia, y compris les images, les vidéos et les fichiers audio. Il stocke ces fichiers en toute sécurité dans un système de stockage blob, tout en conservant les métadonnées organisées dans une base de données distincte pour en faciliter l'accès : type de fichier, taille et horodatage de téléchargement. En déchargeant le stockage des médias des serveurs de chat principaux, le ser-

vice multimédia contribue à réduire l'utilisation de la bande passante sur ces serveurs, améliorant ainsi les performances globales de l'application [55].

- **Magasin Blob :** Le magasin Blob de WhatsApp sert de base de stockage pour les contenus multimédias de l'application de chat. On y trouve divers types de médias tels que des images, des vidéos, des fichiers audios et des documents. Il est spécialement conçu pour gérer de gros volumes de médias tout en garantissant un accès rapide, sécurisé et fiable. Le Media Store utilise généralement des solutions de stockage d'objets basées sur le cloud, telles qu'Amazon S3, Google Cloud Storage ou Azure Blob Storage, qui offrent une grande durabilité, une évolutivité et une rentabilité pour répondre aux divers besoins des utilisateurs en matière de médias [55].
- **Réseau de diffusion de contenu :** Pour minimiser la latence lors du chargement ou du téléchargement de contenu multimédia, WhatsApp utilise un réseau de diffusion de contenu (CDN) qui distribue les fichiers à des emplacements géographiquement plus proches des utilisateurs. Lorsqu'un utilisateur partage un fichier multimédia, l'application client le télécharge directement vers le CDN, ce qui garantit qu'il est stocké à proximité du destinataire prévu. Plutôt que d'envoyer le fichier lui-même, le client transmet l'URL du fichier au serveur de chat dans le cadre du message, ce qui permet aux autres utilisateurs de télécharger et d'accéder rapidement et efficacement au contenu à partir de l'emplacement CDN le plus proche. Une fois les fichiers téléchargés vers le CDN, le service média les récupère et les stocke dans un blob store pour une conservation à long terme. Cette stratégie permet de réduire efficacement la charge sur les serveurs de chat, de minimiser la latence et d'améliorer considérablement la vitesse de diffusion des médias pour les utilisateurs [55].

#### **2.2.5.2 Protocole de communication**

WhatsApp utilise une combinaison de protocoles de communication personnalisés et normalisés pour garantir la rapidité, la sécurité et la fiabilité des messages, des appels vocaux et vidéos et du partage des médias. Voici un aperçu des principaux protocoles :

##### **→ Extensible Messaging and Presence Protocol**

WhatsApp utilise le protocole XMPP pour sa messagerie, ce qui garantit une transmission efficace des messages et des informations de présence. Ce protocole prend en charge les discussions individuelles et collectives, et permet une communication décentralisée [56].

→ **Protocole WebSocket**

Les WebSockets facilitent la communication bidirectionnelle entre le client et le serveur via une connexion unique. Cela permet un transfert de données en temps réel, garantissant ainsi que les messages sont délivrés instantanément [57].

→ **Hypertext Transfer Protocol (HTTP)**

Il est utilisé pour télécharger des contenus multimédias tels que des images et des vidéos sur les serveurs de WhatsApp, ce qui permet aux utilisateurs de partager des médias en toute transparence [58].

→ **Secure Real-time Transport Protocol (SRTP)**

Ce protocole permet de crypter le contenu multimédia (comme les images et les vidéos) pendant la transmission, offrant ainsi une sécurité accrue [59].

→ **Protocol Signal**

WhatsApp utilise le protocole Signal pour le cryptage de bout en bout, ce qui signifie que seuls les destinataires prévus peuvent lire les messages. Cela renforce la confidentialité des utilisateurs et protège les communications contre toute interception [57].

#### 2.2.5.3 Gestion et synchronisation des données

→ **Bases de données côté serveur**

Mnesia est un système de base de données distribué (SGBD) intégré à l'environnement Erlang/OTP. Il est conçu pour garantir la haute disponibilité, la tolérance aux pannes et la concurrence. Il est très probable que WhatsApp, qui repose sur Erlang/OTP, ait utilisé Mnesia pour des fonctions essentielles telles que les listes de contacts, les informations sur les utilisateurs et la gestion des sessions [53].

Principaux cas d'utilisation :

- **Gestion des sessions** : Suivi de l'état en ligne/hors ligne de l'utilisateur et des connexions actives.
- **Files d'attente de messages** : Stocke temporairement les messages non délivrés pour les utilisateurs hors ligne (supprimés après délivrance).
- **Métadonnées** : Stocke les données non liées au contenu (par exemple, les horodatages, les identifiants de l'expéditeur et du destinataire, les informations sur l'acheminement des messages).

→ **Bases de données côté client**

WhatsApp utilise une base de données **SQLLite** locale, basée sur des fichiers, sur l'appareil de chaque utilisateur pour stocker les messages, les contacts et les paramètres. Cette base de données, composée de **msgstore.db** pour les messages et

de **wa.db** pour les contacts et les paramètres, est cryptée à l'aide de l'algorithme AES avec une clé de 256 bits. Les clés de chiffrement sont stockées dans les fichiers **key** et **base\_key**. La sécurité repose sur des clés spécifiques aux appareils, ce qui signifie que chaque appareil possède ses propres clés de chiffrement. Cela garantit que même si un appareil est compromis, les données chiffrées restent inaccessibles sans les clés de chiffrement correctes [60].

→ **Systèmes de secours (Backup)**

WhatsApp propose des systèmes de sauvegarde conçus pour aider les utilisateurs à protéger leur historique de chat et leurs médias. Voici les principales caractéristiques de ces systèmes de sauvegarde [61] :

a) **Sauvegardes dans le nuage :**

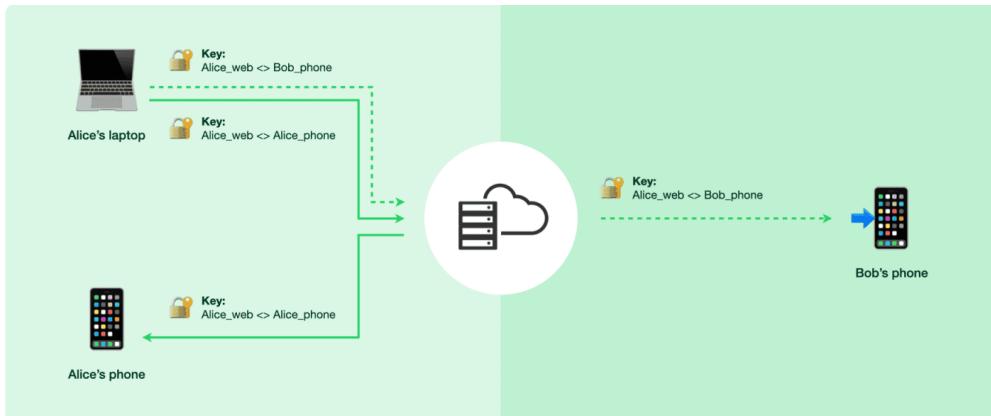
- **Google Drive** : WhatsApp offre la possibilité de sauvegarder l'historique des chats et les médias sur Google Drive. Il s'agit de la principale méthode de sauvegarde dans le nuage pour les utilisateurs d'Android.
- **iCloud** : les utilisateurs d'iOS peuvent sauvegarder leurs données WhatsApp sur iCloud. Comme Google Drive, cette option de stockage dans le nuage permet aux utilisateurs de sauvegarder leur historique de chat et leurs médias.

b) **Sauvegardes locales** : Outre les sauvegardes dans le nuage, WhatsApp prend également en charge les sauvegardes locales. Cela signifie que les utilisateurs peuvent stocker leur historique de chat et leurs médias directement sur leur appareil ou sur un support de stockage externe, tel qu'un ordinateur. Les sauvegardes locales sont souvent utilisées pour restaurer les chats sans dépendre d'une connexion internet ou si l'utilisateur ne souhaite pas stocker sa sauvegarde dans le nuage.

→ **Synchronisation des données**

La synchronisation de WhatsApp fait référence au processus transparent qui garantit que les messages, les médias et l'historique de chat restent cohérents sur plusieurs appareils. À la base, l'application utilise le téléphone comme plaque tournante pour toutes les données ; lors de l'envoi ou de la réception des messages, ils sont d'abord stockés sur le téléphone. Pour synchroniser ces données avec d'autres appareils, le téléphone doit disposer d'une connexion Internet active, ce qui lui permet d'agir comme un serveur qui relaie les messages vers et depuis les serveurs de WhatsApp, qui les répercutent ensuite en temps réel sur les appareils secondaires. Le processus de synchronisation démarre lorsque l'utilisateur définit un appareil secondaire, par exemple lors de l'ouverture de [web.whatsapp.com](http://web.whatsapp.com). Une fois connecté,

le téléphone transmet une copie cryptée de l'historique de chat récent à l'appareil lié, ce qui garantit que tous les nouveaux messages ou actions, comme les réponses ou les chats supprimés, sont instantanément reflétés sur toutes les plates-formes connectées [62].



**Figure 2.3:** Synchronisation multi-appareils de WhatsApp [62]

Le cryptage de bout en bout de WhatsApp est essentiel pour préserver la confidentialité lors de la synchronisation. Les messages sont cryptés sur le téléphone avant d'être envoyés aux serveurs de WhatsApp, puis au destinataire, ce qui garantit que les données non cryptées ne sont jamais transmises pour être stockées. Au contraire, lors de la synchronisation avec un autre appareil, le téléphone partage les messages cryptés avec l'appareil lié via un canal sécurisé, préservant ainsi la confidentialité de sa communication. Avec le déploiement de la prise en charge améliorée de plusieurs appareils, les utilisateurs peuvent désormais relier jusqu'à quatre appareils supplémentaires, tels qu'un autre téléphone, une tablette ou un ordinateur, chacun disposant de sa propre clé de cryptage liée au téléphone principal. Lorsqu'un message est envoyé, il est crypté séparément pour chaque appareil lié, ce qui permet une fonctionnalité indépendante même si le téléphone principal est hors ligne pendant une période pouvant aller jusqu'à 14 jours, car ces appareils peuvent récupérer les données sur les serveurs de WhatsApp en fonction de la dernière synchronisation. Les utilisateurs peuvent sauvegarder leurs discussions sur Google Drive sur Android ou sur iCloud sur iPhone, et ces sauvegardes sont associées au numéro de téléphone. Lorsque l'utilisateur change de téléphone ou réinstalle WhatsApp, il peut restaurer l'historique de ses discussions à partir de ces sauvegardes. Toutefois, il est important de noter que ces sauvegardes ne sont pas chiffrées de bout en bout, à moins que l'utilisateur n'opte manuellement pour une option de sauvegarde chiffrée à l'aide d'un mot de passe ou d'une clé [62].

## 2.2.6 Sécurité et confidentialité dans WhatsApp

### 2.2.6.1 Aspect sécurité

Il est essentiel de garantir la sécurité des communications, en particulier à une époque marquée par des préoccupations croissantes en matière de protection de la vie privée et par des atteintes à la protection des données. Les méthodes de vérification jouent un rôle clé dans la confirmation de l'authenticité des partenaires de communication et de l'intégrité des données partagées. Voici quelques méthodes de vérification couramment utilisées par WhatsApp pour garantir la sécurité des communications :

#### 1. Chiffrement de bout en bout

WhatsApp utilise le cryptage de bout en bout pour protéger les messages, ce qui garantit que les conversations restent privées et sécurisées tout au long de leur transmission. Ce processus de cryptage signifie que lors de l'envoi d'un message, celui-ci est crypté sur l'appareil et ne peut être décrypté que par l'appareil du destinataire. Aucun intermédiaire, y compris WhatsApp lui-même, ne peut accéder au contenu des messages [63].

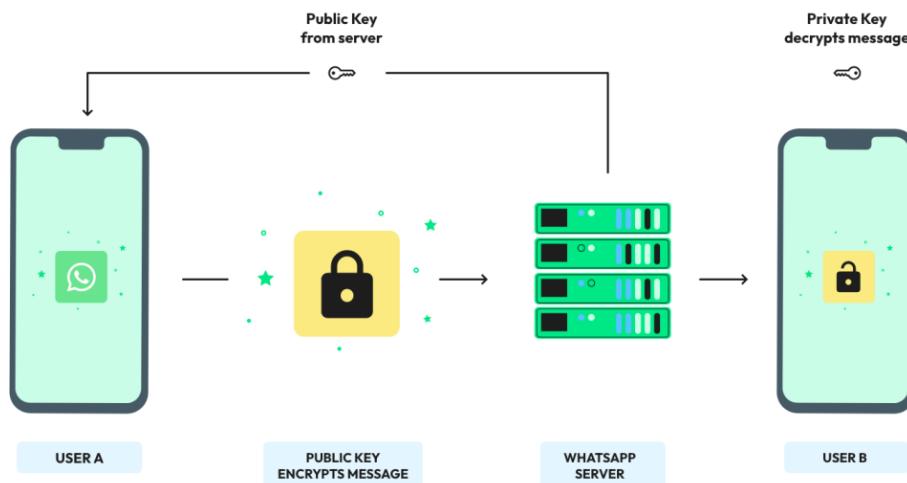


Figure 2.4: Chiffrement de bout en bout de WhatsApp [63]

Voici une explication étape par étape du cryptage de WhatsApp [63] :

- **Génération de clés** : Lors de l'installation WhatsApp pour la première fois, l'application crée une paire de clés cryptographiques pour l'appareil : une clé publique et une clé privée. La clé publique est partagée avec les autres utilisateurs, tandis que la clé privée est stockée en toute sécurité sur l'appareil et ne le quitte jamais.
- **Échange de clés** : Lors de l'entame d'une conversation avec quelqu'un sur WhatsApp, l'application échange automatiquement les clés publiques entre

les deux appareils. Cet échange de clés s'effectue de manière transparente en arrière-plan.

- **Chiffrement des messages :** Lors de l'envoi d'un message à un contact, WhatsApp le crypte sur l'appareil à l'aide de la clé publique du destinataire. Ce cryptage transforme le message en un charabia illisible (texte chiffré) avant qu'il ne soit envoyé aux serveurs de WhatsApp.
- **Relais du serveur :** Les serveurs de WhatsApp servent de relais pour ces messages cryptés. Ils reçoivent le texte chiffré et le transmettent à l'appareil du destinataire sans accéder à son contenu.
- **Décryptage du message :** Lorsqu'il reçoit le texte chiffré, l'appareil du destinataire utilise sa clé privée pour déchiffrer le message. Cette clé privée, stockée en toute sécurité sur son appareil, est la seule capable de déchiffrer le texte chiffré.
- **Affichage du message :** Une fois que l'appareil du destinataire a déchiffré le texte chiffré, il affiche le message dans sa forme originale, lisible.

En conclusion, le chiffrement bout en bout de WhatsApp préserve la confidentialité et la sécurité des messages en générant des clés cryptographiques uniques pour chaque utilisateur, ce qui permet un échange de clés automatique sans l'intervention de l'utilisateur. Cela signifie que même si les messages passent par les serveurs de WhatsApp, seul le destinataire prévu peut accéder au contenu. Ce cadre de sécurité protège les communications contre l'interception et souligne l'importance de la vie privée, ce qui permet aux utilisateurs de communiquer en toute confiance.

## 2. Vérification en deux étapes

La vérification en deux étapes est une fonction de sécurité facultative qui ajoute une couche de protection supplémentaire aux comptes WhatsApp. Les utilisateurs peuvent activer cette fonction pour définir un code PIN à six chiffres, qui leur est demandé chaque fois qu'ils enregistrent leur numéro de téléphone sur WhatsApp. Cette exigence supplémentaire permet de protéger les comptes contre les accès non autorisés, car même si quelqu'un parvient à obtenir le numéro de téléphone de l'utilisateur, il devra toujours connaître le code PIN pour terminer le processus d'enregistrement sur un nouvel appareil. En utilisant la vérification en deux étapes, les utilisateurs peuvent renforcer considérablement la sécurité de leurs comptes [64].

## 3. Verrouillage biométrique

Pour plus de sécurité, WhatsApp propose une fonction de verrouillage biométrique sur les appareils pris en charge, permettant aux utilisateurs de sécuriser l'application à l'aide de méthodes d'authentification biométriques telles que la numérisation

des empreintes digitales ou la reconnaissance faciale. Cette fonction renforce la sécurité du compte en garantissant que seul l'utilisateur autorisé peut accéder à WhatsApp, même si quelqu'un d'autre a physiquement accès à l'appareil. En activant le verrouillage biométrique, les utilisateurs peuvent avoir l'esprit tranquille en sachant que leurs conversations et informations privées restent à l'abri des regards indiscrets [64].

#### **4. Disparition des messages**

La disparition des messages est une autre fonction remarquable qui permet aux utilisateurs de maintenir un niveau de confidentialité plus élevé dans leurs conversations. Lorsqu'elle est activée, tout message envoyé dans le cadre d'une discussion disparaît automatiquement au bout d'une durée déterminée, généralement fixée à 7 jours. Ce paramètre garantit que les conversations sensibles ne s'éternisent pas, réduisant ainsi le risque d'accès non autorisé à des informations potentiellement privées. En utilisant cette fonction, les utilisateurs peuvent se sentir plus en sécurité lorsqu'ils partagent des informations qu'ils préfèrent ne pas voir sauvegardées à long terme [64].

En conclusion, WhatsApp propose un ensemble solide de fonctions de sécurité pour protéger la vie privée des utilisateurs et la sécurité des communications. Il s'agit notamment du chiffrement de bout en bout des messages et des appels, de la vérification en deux étapes, des paramètres de confidentialité personnalisables, des sauvegardes sécurisées et des outils permettant de signaler toute activité suspecte. En utilisant ces fonctions et en suivant les meilleures pratiques, les utilisateurs peuvent renforcer leur sécurité et protéger leurs informations personnelles dans le paysage numérique [64].

##### **2.2.6.2 Aspect vie privée**

La politique de confidentialité de WhatsApp décrit les pratiques de gestion des données, en mettant l'accent sur la transparence et le contrôle par l'utilisateur. Elle décrit la collecte des données personnelles et des données d'utilisation, ainsi que la manière dont ces informations sont utilisées pour améliorer les services et la sécurité. Les utilisateurs peuvent ajuster les paramètres de confidentialité, supprimer leur compte et exporter l'historique de leurs conversations. Bien que les données puissent être partagées avec des tiers et Facebook, WhatsApp garantit la sécurité grâce à un cryptage de bout en bout. Les utilisateurs peuvent accéder à leurs données et les mettre à jour, et la politique comprend un engagement à les informer des changements importants, ce qui favorise la confiance et la transparence [65].

Voici un aperçu structuré des principaux aspects [65] :

## **1. Collecte de données**

WhatsApp recueille différents types de données pour fournir ses services. Les informations relatives au compte comprennent le numéro de téléphone de l'utilisateur, son nom de profil, sa photo et son statut. En ce qui concerne les messages, bien que le contenu soit protégé par un cryptage de bout en bout, les messages non lus peuvent être temporairement stockés sur des serveurs. Les données relatives à l'appareil et à l'utilisation englobent des détails tels que le type d'appareil, le système d'exploitation, l'adresse IP, l'activité de l'application (comme les fonctions utilisées et les temps d'interaction) et les cookies pour l'analyse. Pour les contacts, si les utilisateurs l'autorisent, WhatsApp accède aux contacts pour faciliter la messagerie, ces informations étant stockées localement ou cryptées sur des serveurs. Les données de localisation ne sont collectées que si elles sont partagées par l'utilisateur ou lors de l'utilisation des fonctions de localisation en direct. Enfin, pour les utilisateurs qui ont recours à des services de paiement, WhatsApp recueille les détails de la transaction, y compris les informations relatives au paiement et à la transaction.

## **2. Utilisation des données**

WhatsApp utilise les données collectées pour améliorer l'expérience des utilisateurs et garantir la sécurité de la plateforme. Ces données sont essentielles pour les fonctionnalités de base telles que la messagerie, les appels et les discussions de groupe, ainsi que pour personnaliser les interactions avec les utilisateurs. La plateforme utilise des systèmes automatisés pour détecter les activités suspectes et se protéger contre le spam, tout en mettant en œuvre des mesures de sécurité telles que la vérification en deux étapes. WhatsApp tient les utilisateurs informés des mises à jour et des changements de politique et effectue des analyses pour améliorer le service et l'efficacité opérationnelle. Bien qu'aucune publicité directe ne soit affichée, les données peuvent être partagées avec des sociétés Meta pour une publicité plus pertinente. Dans l'ensemble, WhatsApp s'efforce de fournir un environnement de messagerie sécurisé et convivial tout en accordant la priorité à la protection de la vie privée des utilisateurs.

## **3. Partage des données**

WhatsApp partage des informations avec les sociétés Meta, y compris les numéros de téléphone, les données de transaction et les détails de l'appareil, afin d'améliorer les expériences sur les plateformes Meta, comme spécifié dans la politique de données de Meta. En outre, les services tiers avec lesquels les utilisateurs interagissent sur WhatsApp peuvent recevoir des données d'utilisateurs, telles que les numéros

de téléphone et les historiques de chat, et peuvent faire appel à des fournisseurs tiers pour l'hébergement. Pour garantir la conformité légale, WhatsApp répond aux demandes légales et prévient les préjudices conformément aux lois en vigueur. Bien que le contenu des messages cryptés ne puisse pas être divulgué, les métadonnées associées, telles que les identifiants des utilisateurs et les horodatages, peuvent être partagées.

#### **4. Droits de l'utilisateur**

WhatsApp offre aux utilisateurs des droits et des contrôles importants sur leurs données et leur vie privée, y compris la possibilité d'exporter les informations de leur compte et de supprimer leur compte, ce qui supprime leurs données de la plate-forme. L'application comprend divers paramètres de confidentialité qui permettent aux utilisateurs de gérer la visibilité de leur dernier statut, de leur photo de profil et de leurs mises à jour de statut, ainsi que de bloquer les contacts indésirables et de désactiver la synchronisation des contacts et le partage de la localisation. En outre, WhatsApp prend en charge la portabilité des données conformément à des réglementations telles que le GDPR et le CCPA, soulignant ainsi son engagement en faveur de l'autonomisation des utilisateurs et du respect de la vie privée.

La politique de confidentialité de WhatsApp met l'accent sur le contrôle de l'utilisateur et la transparence en matière de traitement des données. Elle veille à ce que les utilisateurs soient informés de la manière dont leurs informations sont utilisées et leur offre diverses options pour gérer leur vie privée. En consultant et en utilisant régulièrement les paramètres de confidentialité disponibles, les utilisateurs peuvent protéger leurs informations personnelles tout en profitant des fonctionnalités de l'application [65].

### **2.2.7 Défis et impact mondial de WhatsApp**

WhatsApp, l'une des applications de messagerie les plus utilisées au monde, a profondément modifié la façon dont les personnes communiquent. Avec plus de deux milliards d'utilisateurs, son influence est indéniable. Cependant, cette popularité entraîne également des défis significatifs et suscite des critiques.

#### **2.2.7.1 L'impact mondial de WhatsApp**

WhatsApp, qui compte plus de 2 milliards d'utilisateurs actifs dans le monde, a profondément influencé la communication personnelle, les opérations commerciales et la dynamique sociale et culturelle. Voici un aperçu de son impact mondial :

## **1. Communication personnelle**

WhatsApp a révolutionné la connectivité en rendant la messagerie instantanée accessible et abordable, en particulier dans les régions où les coûts des SMS ou des appels peuvent être prohibitifs. Grâce à sa faible consommation de données et à la gratuité des appels vocaux et vidéo, l'application a réussi à combler les lacunes en matière de communication pour des millions de personnes, permettant des interactions transparentes au-delà des grandes distances. En outre, la possibilité de partager des contenus multimédias, tels que des photos, des vidéos et des notes vocales, a enrichi la communication personnelle, la rendant plus expressive et plus engageante, et a ainsi amélioré la qualité globale des interactions entre les utilisateurs du monde entier [66].

## **2. Utilisation professionnelle**

WhatsApp est devenu un outil essentiel pour l'engagement des clients, avec plus de 50 millions d'entreprises qui utilisent la plateforme pour interagir avec leurs clients. Plus de 175 millions de personnes communiquent quotidiennement avec des comptes professionnels, ce qui souligne l'efficacité de l'application en tant que canal de communication direct qui améliore le service et la satisfaction des clients. Parallèlement, les fonctionnalités de messagerie en temps réel de WhatsApp contribuent à l'efficacité opérationnelle en rationalisant les communications internes. Cela permet d'améliorer la collaboration au sein des équipes et d'accélérer les processus de prise de décision [67].

## **3. Influence sociale et culturelle**

WhatsApp transcende les frontières culturelles, offrant aux utilisateurs une plate-forme pour partager leurs expériences, leurs traditions et leurs points de vue, favorisant ainsi l'émergence d'une communauté mondiale. Cette richesse des échanges culturels a joué un rôle important dans l'adoption massive de l'application, en particulier par les milléniaux qui apprécient la connectivité et la diversité des interactions. En outre, WhatsApp s'est avéré essentiel pour l'organisation et la mobilisation des mouvements sociaux, en permettant la diffusion rapide d'informations et en facilitant la coordination entre les militants. Sa capacité à servir d'outil de changement social souligne son influence, qui va bien au-delà de la simple communication, et met en évidence son importance dans la dynamique sociétale contemporaine [68].

En résumé, l'intégration de WhatsApp dans la vie quotidienne a modifié la façon dont les individus communiquent, les entreprises fonctionnent et les cultures interagissent. Cela a consolidé sa position d'outil essentiel à l'ère numérique.

### **2.2.7.2 Défis de WhatsApp**

WhatsApp est confronté à plusieurs défis majeurs en matière de sécurité et de protection de la vie privée. Il s'agit notamment de :

#### **1. Préoccupations en matière de protection de la vie privée**

Bien qu'il utilise un chiffrement de bout en bout grâce au protocole Signal, WhatsApp recueille de nombreuses métadonnées, y compris les interactions des utilisateurs et les informations relatives à l'appareil, ce qui pose des problèmes de protection de la vie privée. Ces données peuvent être partagées avec sa société mère, Meta (anciennement Facebook), ce qui suscite des craintes quant à la surveillance des utilisateurs et à l'utilisation abusive des données [69].

#### **2. Désinformation**

WhatsApp est souvent utilisé pour propager de fausses informations, en particulier dans des contextes politiques ou de santé publique. Des études ont montré que des messages trompeurs peuvent se propager rapidement, entraînant des conséquences graves, comme des violences physiques dans certains cas. WhatsApp a mis en place des mesures pour limiter le partage de messages fréquemment transférés afin de combattre la désinformation, mais le défi reste important [70].

#### **3. Phishing et ingénierie sociale**

WhatsApp est une cible courante pour les attaques de phishing, où les attaquants se font passer pour des contacts de confiance afin de soutirer des informations sensibles. Les utilisateurs sont souvent incités à communiquer des codes de vérification ou à cliquer sur des liens malveillants, ce qui peut compromettre leur compte [71].

#### **4. Distribution de logiciels malveillants**

WhatsApp est confronté à de sérieux problèmes de diffusion de logiciels malveillants par le biais de trois canaux principaux. Tout d'abord, les cybercriminels partagent des liens malveillants dans les messages qui peuvent infecter les appareils des utilisateurs. Ensuite, les pièces jointes nuisibles peuvent être téléchargées et exécutées à leur insu par les utilisateurs. Enfin, les vulnérabilités dans les discussions de groupe permettent au contenu malveillant de se propager rapidement si un membre le partage, ce qui augmente le risque d'une infection généralisée [71].

#### **5. Concurrence**

WhatsApp est confronté à d'importants défis concurrentiels sur le marché des applications de messagerie, principalement de la part de plateformes émergentes telles que Telegram, Signal et Discord. Ces applications proposent en effet des caractéristiques uniques telles qu'une meilleure confidentialité, des fonctionnalités de groupe

plus étendues et des intégrations transparentes avec d'autres services. Ces concurrents s'adressent souvent à des groupes démographiques spécifiques et proposent une expérience utilisateur plus personnalisable, ce qui peut attirer les utilisateurs à la recherche de solutions sur mesure. En outre, les préoccupations croissantes concernant la confidentialité des données et la concurrence des applications locales sur divers marchés internationaux compliquent encore la position de WhatsApp. Pour conserver sa pertinence, l'application doit sans cesse innover, résoudre les problèmes de confidentialité et améliorer l'engagement des utilisateurs tout en tenant compte des préférences et des besoins diversifiés de sa base mondiale d'utilisateurs [72].

Pour relever ces défis, des efforts continus sont nécessaires pour renforcer les mesures de sécurité, protéger la vie privée des utilisateurs, lutter contre la désinformation et naviguer efficacement dans le paysage concurrentiel et réglementaire.

## Conclusion

Les applications de messagerie instantanée ont révolutionné la communication, offrant une alternative rapide, pratique et accessible à tous. WhatsApp, avec son interface conviviale, ses fonctionnalités innovantes et son cryptage de bout en bout, s'est imposé comme l'une des applications les plus populaires au monde. Son impact sur la communication personnelle, les relations interpersonnelles et les interactions professionnelles est indéniable.

Malgré les défis et les critiques, WhatsApp continue d'innover et de se développer en proposant de nouvelles fonctionnalités et en s'adaptant aux besoins de ses utilisateurs. Son rôle sur les marchés émergents et son influence sociale et culturelle en font un acteur majeur de la communication mondiale. L'avenir de WhatsApp s'annonce prometteur, avec de nouvelles fonctionnalités prévues et une expansion continue de sa base d'utilisateurs. L'intégration croissante de l'intelligence artificielle dans les applications de messagerie, l'importance grandissante de la confidentialité et de la sécurité, ainsi que l'impact potentiel des technologies émergentes comme Web3 sont autant de facteurs qui façonnent l'avenir de la messagerie instantanée.

# Chapitre 3

## Étude des solutions existantes

### Introduction

Être parent à l'ère numérique présente des défis uniques en raison de l'évolution rapide de la technologie. Si les plateformes en ligne offrent de précieuses possibilités d'apprentissage et de socialisation, elles exposent également les enfants à des risques tels que les contenus inappropriés, la cyberintimidation, l'usurpation d'identité et les problèmes de protection de la vie privée. Pour relever ces défis, la mise en place de contrôles parentaux est devenue essentielle pour garantir la sécurité en ligne des enfants et promouvoir une expérience numérique saine. Des outils avancés et des applications de surveillance permettent aux parents de gérer les activités de leurs enfants, de fixer des limites de temps d'écran et de filtrer les contenus pour les aider à naviguer dans le monde numérique de manière sûre et responsable [73].

### 3.1 WhatsApp est-il sûr pour les enfants ?

Dans certaines circonstances, WhatsApp peut être un outil utile pour rester en contact avec les amis et la famille. Cependant, il présente des risques importants pour les enfants car il ne permet pas de contrôler les messages et permet aux utilisateurs d'envoyer et de recevoir des photos et des textes inappropriés, violents et sexuellement explicites. En outre, l'utilisation de WhatsApp ne nécessite pas de vérification de l'âge, ce qui soulève des inquiétudes quant à sa sécurité pour les jeunes utilisateurs. Bien que l'application puisse faciliter une communication efficace, les parents et les tuteurs doivent être conscients de ces dangers potentiels afin de prendre des décisions éclairées concernant la vie numérique de leurs enfants. Comprendre les risques associés à WhatsApp est essentiel pour les familles qui souhaitent protéger leurs proches tout en naviguant dans la complexité des interactions

en ligne [74, 75]. Voici quelques-uns des principaux risques liés à l'utilisation de WhatsApp par les enfants [75] :

- **Contenu inapproprié** : En l'absence de filtres, les utilisateurs peuvent envoyer n'importe quel type de média, y compris par le biais de la fonction « **view once** », qui permet aux photos et aux vidéos de n'être visionnées qu'une seule fois avant de disparaître. Il est donc difficile pour les parents de surveiller ou de conserver les preuves d'un contenu préjudiciable. La fonction « **disparition des messages** », qui supprime automatiquement les messages après une période donnée, peut être désactivée par les parents, mais les enfants peuvent facilement la réactiver lorsqu'ils ne sont pas surveillés. Par conséquent, certains enfants peuvent envoyer des contenus risqués ou intimes en pensant à tort qu'ils disparaîtront définitivement, sans se rendre compte qu'il est toujours possible de faire des captures d'écran.
- **Étrangers et escrocs** : Les membres d'un groupe WhatsApp peuvent facilement copier et partager des liens de discussion, ce qui permet à n'importe qui de se joindre au groupe sans autorisation préalable. Des inconnus mal intentionnés ou des escrocs peuvent ainsi s'infiltrer dans des groupes privés, entamer des conversations privées ou inviter des membres à rejoindre d'autres groupes potentiellement dangereux. En outre, les enfants qui rejoignent des groupes de discussion publics en ligne au hasard risquent d'être contactés par des personnes inconnues et potentiellement dangereuses.
- **Cyberintimidation** : Les messageries de groupe peuvent faciliter la cyberintimidation en permettant aux individus de cibler d'autres personnes au sein du groupe, ou en diffusant des images et des rumeurs inappropriées. Par exemple, un intimidateur peut partager publiquement le numéro WhatsApp d'une personne, ce qui fait que la victime reçoit une avalanche de messages blessants de la part d'inconnus. Une autre forme particulièrement préjudiciable de cyberintimidation est le « doxing », qui consiste à partager publiquement des informations personnelles sur la victime dans l'intention de lui nuire ou de la mettre dans l'embarras.
- **Addictivité** : Les parents doivent également être conscients que le chat, ainsi que l'envoi d'émoticônes et de GIF, peuvent créer une dépendance et conduire leurs enfants à passer un temps excessif sur leur téléphone.
- **Partage d'emplacement** : Les enfants peuvent partager leur position en direct avec leurs contacts. Cependant, cette fonction peut être risquée si elle est partagée avec des personnes qui ne font pas partie de leur cercle de confiance.

Bien que WhatsApp soit un outil de communication précieux, il présente certains risques pour les enfants. Pour garantir leur sécurité, les parents devraient utiliser des

applications de contrôle parental pour surveiller les activités de leurs enfants sur la plateforme. À l’ère du numérique, la sécurité en ligne des enfants doit être une priorité, d'où la nécessité de mettre en place un contrôle parental.

## **3.2 Principales caractéristiques des applications de contrôle parental**

Lorsque vous choisissez une application de contrôle parental, il est important de donner la priorité aux fonctionnalités qui protégeront l’expérience en ligne et le bien-être de vos enfants. Voici quelques caractéristiques clés à prendre en compte [76] :

- **Surveillance et gestion de l'utilisation des applications** : Les fonctions de gestion et de blocage des applications sont essentielles dans les applications de contrôle parental, car elles permettent aux parents de restreindre l'accès à certaines applications, telles que les médias sociaux et les plateformes de messagerie, qui peuvent être distrayantes ou inappropriées. Ces outils offrent souvent la possibilité de bloquer temporairement certaines applications pendant les heures d'école ou d'autres périodes désignées, ce qui contribue à favoriser la concentration et à créer un environnement plus productif pour les enfants.
- **Suivi de la localisation** : Les applications de contrôle parental offrent des fonctions de localisation et de géofencing qui permettent aux parents de surveiller l'emplacement de leur enfant en temps réel. La géolocalisation permet de créer des frontières virtuelles et d'envoyer des alertes lorsqu'un enfant entre ou sort de certaines zones, comme l'école ou la maison. Cette fonction peut contribuer à apaiser les inquiétudes des parents concernant les allées et venues de leur enfant, en particulier en cas de manque de communication, en les avertissant lorsque leur enfant entre ou sort de certaines zones.
- **Rapports d'activité** : Des journaux et des rapports détaillés donnent aux parents un aperçu de l'utilisation de l'appareil par leur enfant, y compris l'utilisation des applications, le temps passé dans chaque application et l'historique de la navigation sur le web. Ces informations permettent d'identifier des schémas ou des comportements inquiétants, ce qui permet aux parents de mieux comprendre les habitudes numériques de leur enfant et de prendre des décisions éclairées en matière de politiques et de restrictions.
- **Gestion des comptes familiaux** : Un compte familial simplifié vous permet de gérer tous les appareils et comptes de vos enfants à partir d'une interface unique, ce

qui facilite la configuration et la personnalisation des contrôles pour plusieurs utilisateurs. Ces applications sont conçues pour être conviviales et faciles à parcourir, de sorte que même les utilisateurs non initiés à la technologie peuvent configurer et gérer les contrôles rapidement et sans frustration.

Si ces fonctionnalités sont des conditions préalables fondamentales pour un contrôle parental efficace, elles jouent un rôle crucial en aidant les parents à protéger leurs enfants contre les divers dangers numériques.

### 3.3 Applications populaires de contrôle parental pour WhatsApp

Étant donné le nombre d'options disponibles, chacune offrant une gamme différente de fonctionnalités telles que la surveillance des messages textuels, le suivi de la localisation en temps réel et les restrictions d'utilisation. Pour prendre une décision éclairée, les parents doivent tenir compte de plusieurs facteurs clés, notamment la facilité d'utilisation de l'application, son prix et sa compatibilité avec l'appareil de leur enfant, afin de trouver la solution la plus adaptée à leurs besoins spécifiques [77].

Voici quelques applications de contrôle parental populaires qui peuvent aider les parents à surveiller et à assurer la sécurité de leurs enfants lorsqu'ils utilisent WhatsApp [78] :

#### 3.3.1 Bark



Bark est une application de contrôle parental qui surveille les interactions sociales sur des plateformes telles que WhatsApp, en utilisant une IA avancée pour détecter les risques tels que la cyberintimidation et les contenus explicites. Elle fournit des alertes en temps réel, permettant aux parents d'intervenir rapidement lorsqu'une activité inquiétante est identifiée. Bien que Bark excelle à alerter les parents sur les risques potentiels, son coût d'abonnement est plus élevé que celui des applications de contrôle parental de base, ce qui peut constituer un inconvénient pour certaines familles. En outre, elle se concentre moins sur la gestion du temps d'écran que d'autres solutions. Les nouveaux utilisateurs peuvent bénéficier d'une version d'essai gratuite, et le plan Bark Premium est proposé au prix de 14,00 \$ par mois et offre des fonctions complètes de surveillance et d'alerte.

### **3.3.2 mSpy**



mSpy est une application de surveillance conçue pour permettre aux parents de surveiller discrètement l'activité en ligne de leurs enfants, en particulier sur des plateformes telles que WhatsApp.

Elle excelle dans le suivi des interactions avec les SMS, les applications de messagerie et les courriels, et donne un aperçu des messages WhatsApp envoyés et reçus, ainsi que de l'accès aux fichiers multimédias échangés et aux informations de contact.

Bien que mSpy offre des fonctionnalités telles que le blocage des contenus inappropriés et une interface conviviale, il présente des limites, notamment l'absence de version gratuite, de garantie de remboursement et de contrôle parental avancé. Les prix d'abonnement sont fixés à 48,99 \$ par mois, 83,99 \$ par trimestre et 139,99 \$ par an, ce qui fait du coût un élément à prendre en considération pour les utilisateurs potentiels.

### **3.3.3 FamiSafe**



FamiSafe est une application de contrôle parental qui aide les parents à surveiller les activités en ligne de leurs enfants. Elle propose le suivi de la localisation en temps réel, le geofencing et la gestion de l'utilisation de WhatsApp, ce qui la rend idéale pour assurer la sécurité des enfants dans les environnements numériques et physiques. Ses principales fonctionnalités sont le suivi GPS, les alertes personnalisables, la gestion du temps d'écran, le filtrage de contenu, le blocage d'applications et la surveillance des médias sociaux.

L'application est facile à utiliser, prend en charge plusieurs appareils et est simple à configurer. Toutefois, certaines fonctionnalités nécessitent un abonnement et le suivi GPS continu peut réduire l'autonomie de la batterie. L'abonnement annuel coûte 59,99 \$ et prend en charge un nombre illimité d'appareils.

### **3.3.4 Qustodio**



Qustodio est une application complète de contrôle parental conçue pour aider les parents à surveiller les activités en ligne de leurs enfants, y compris les applications de messagerie populaires telles que WhatsApp. Elle permet de filtrer les contenus, de gérer le temps passé devant l'écran et d'effectuer un suivi détaillé afin de promouvoir un comportement numérique sûr. En particulier, elle suit les paramètres d'utilisation de WhatsApp tels que le temps passé, le volume de messages et les contacts, tout en offrant

la possibilité de bloquer les contenus inappropriés et de fixer des limites d'utilisation de l'application.

Cependant, si la version de base est gratuite, de nombreuses fonctionnalités, notamment la surveillance de WhatsApp, nécessitent un abonnement premium. Le processus d'installation peut également s'avérer complexe pour les utilisateurs moins avertis sur le plan technique. Les abonnements premium coûtent 99,95 \$ par an (8,33 \$/mois) pour l'abonnement complet.

En conclusion, si les applications de contrôle parental offrent des fonctionnalités intéressantes pour assurer la sécurité des enfants en ligne, leur coût élevé et le nombre limité d'options gratuites peuvent constituer un obstacle important pour de nombreuses familles. L'importance de ces outils pour la protection des jeunes utilisateurs est évidente, mais l'absence de plans abordables peut conduire les parents à chercher d'autres solutions. En fin de compte, il est essentiel pour les familles qui cherchent à protéger l'expérience numérique de leurs enfants de trouver un équilibre entre la nécessité d'un contrôle efficace et les considérations budgétaires.

### 3.4 Défis et limites

- **Exigences techniques :** Certains contrôles parentaux nécessitent le rootage (pour Android) ou le jailbreaking (pour iOS) des appareils pour accéder à des données système plus profondes, ce qui peut annuler des garanties, créer des vulnérabilités en matière de sécurité et ne pas être pratique pour tous les utilisateurs [79].
- **Nature multiplateforme de WhatsApp :** La nature multiplateforme de WhatsApp, qui est disponible sur Android, iOS et les plateformes Web, constitue un obstacle important pour les applications de contrôle parental qui cherchent à surveiller l'activité des utilisateurs. En effet, la présence généralisée de l'application sur plusieurs appareils et interfaces complique les efforts visant à mettre en œuvre des mesures de surveillance efficaces.
- **Un faux sentiment de sécurité :** Les parents peuvent développer un faux sentiment de sécurité en se fiant trop aux applications de contrôle parental, ce qui peut les amener à négliger des discussions ouvertes et importantes sur la sécurité en ligne avec leurs enfants [80].
- **Absence de contrôle parental :** WhatsApp ne dispose pas de contrôle parental intégré, ce qui peut rendre difficile pour les parents de surveiller les conversations ou d'intervenir si nécessaire. Ce manque de contrôle peut parfois conduire les enfants à utiliser la plateforme intentionnellement, sachant que leurs parents sont moins

susceptibles de surveiller leurs activités [75].

- **Les violations de données :** Un défi majeur pour les applications de contrôle parental qui traitent des informations sensibles sur les enfants, comme l'a montré le piratage de KidGuard en 2020 qui a révélé des vulnérabilités de sécurité. De tels incidents peuvent conduire à l'usurpation d'identité et à une perte de confiance entre les parents. Pour limiter ces risques, les parents doivent choisir des fournisseurs réputés ayant des pratiques de sécurité solides, donner la priorité aux applications qui utilisent le chiffrement et appliquent des politiques de confidentialité transparentes, et veiller à ce que les logiciels soient régulièrement mis à jour [81].

## Conclusion

En conclusion, si la nécessité pour les parents de surveiller l'utilisation du téléphone de leurs enfants - en particulier sur des plateformes telles que WhatsApp - n'a jamais été aussi pressante, le coût élevé des applications de contrôle parental constitue un obstacle important. De nombreux parents se sentent obligés d'investir dans ces outils pour leurs avantages et leurs fonctionnalités, mais ces abonnements peuvent être financièrement écrasants, en particulier pour les familles à revenus moyens ou faibles et pour les ménages plus nombreux confrontés à des limites en matière d'appareils. Par conséquent, ces mesures de sécurité essentielles risquent de rester hors de portée de ceux qui en ont le plus besoin.

# Chapitre 4

## Étude conceptuelle

### Introduction

La phase d'étude conceptuelle est une étape clé dans le cycle de vie d'un logiciel. Elle répond aux besoins identifiés lors de l'analyse préalable, en permettant de spécifier le système à développer et de décrire son fonctionnement. Cette étape constitue un support essentiel pour l'implémentation.

Dans ce chapitre, nous présenterons en détail la phase de conception du projet à travers notre architecture et avec l'aide de diagrammes UML.

### 4.1 Objectif

L'objectif général de ce mémoire est de répondre au besoin croissant de solutions de surveillance éthique et techniquement robustes pour les plateformes de messagerie instantanée, en se concentrant spécifiquement sur WhatsApp étant l'une des solutions les plus usitées dans le monde. Il s'agit de concevoir un système de monitoring qui permet un accès aux données de communication dans des cadres définis : protection de l'enfance, prévention des risques, tout en naviguant les complexités imposées par les mécanismes de sécurité des systèmes d'exploitation et des applications elles-mêmes. Ce mémoire vise à explorer les limites des approches actuelles et à proposer une architecture innovante.

Dans cette optique, ce chapitre se concentre sur l'analyse des défis techniques liés à l'accès aux messages WhatsApp sur la plateforme Android et sur la présentation détaillée de l'architecture de la solution proposée.

Avant de plonger dans la conception d'une solution de monitoring, il est indispensable de comprendre le contexte sécuritaire de la plateforme Android. Les évolutions constantes

de ce système d'exploitation ont un impact direct sur les possibilités d'accès aux données applicatives.

## 4.2 Défis liés à la sécurité d'Android

Android 13 (API niveau 33), ainsi que les versions suivantes, ont durci les fonctionnalités de sécurité permettant ainsi de renforcer la confidentialité des utilisateurs et la sécurité globale de la plateforme [82] au détriment de l'accessibilité des applications aux données.

### 4.2.1 Accès restreint aux données applicatives (/data/data)

Android 13 et les versions ultérieures ont maintenu et renforcé le principe de sandboxing. L'accès au répertoire de données privées d'une application (/data/data/[nom.du.paquet]), où sont stockées les informations les plus sensibles comme les bases de données et les clés, reste interdit aux autres applications sans priviléges root [83].

### 4.2.2 Fonctionnalité “Paramètres restreints”

Il s'agit d'une mesure de sécurité conçue spécifiquement pour contrer l'abus de permissions particulièrement dangereuses par des applications potentiellement malveillantes, notamment celles installées en dehors des boutiques d'applications officielles (sideloading) [84].

Les deux permissions principalement ciblées par cette restriction sont :

- **Accès aux services d'accessibilité** : En raison de leur capacité à lire l'écran et intercepter les saisies, ces services sont fréquemment détournés par des malwares pour voler des identifiants, des informations bancaires, contourner l'authentification à deux facteurs, et espionner les communications [85].
- **Accès à l'écouteur de notification** : Cette permission permet de lire le contenu de toutes les notifications [84].

## 4.3 Prérequis pour le monitoring de WhatsApp

Pour effectuer une surveillance significative des conversations WhatsApp, l'accès aux éléments suivant est indispensables [86] :

- **Base de données des messages** : Il s'agit de la base de données où WhatsApp stocke l'historique des messages, les métadonnées (horodatages, expéditeur-

destinataire), les informations de groupe, etc. Elle réside dans le stockage partagé /media/com.whatsapp/WhatsApp/databases/msgstore.db.

- **Clé de chiffrement** : La base de données msgstore.db est chiffrée pour protéger la confidentialité des messages. Elle est stockée séparément dans le répertoire privé de WhatsApp : /data/data/com.whatsapp/files/key.
- **Fichiers média** : Les fichiers multimédias échangés (images, vidéos, audio, documents) sont stockés dans le stockage partagé, dans un dossier accessible avec les nouvelles permissions média /media/com.whatsapp/WhatsApp/media/.

Les mécanismes de sécurité renforcés d'Android 13 rendent l'accès à ces données essentielles pratiquement impossible pour une application tierce. En conséquence, les solutions traditionnelles de monitoring de WhatsApp sont rendues inefficaces, et le développement d'alternatives fiables est devenu excessivement difficile.

Le principal obstacle réside dans l'accès à la clé de chiffrement. Sans cette clé, la base de données des messages msgstore.db, bien qu'accessible demeure inutilisable car chiffrée. Les mesures de sandboxing renforcées par Android interdisent l'accès direct à ce répertoire privé par une application tierce non privilégiée. Cette situation rend obsolète les approches de monitoring qui reposaient sur la simple récupération de la base de données et de sa clé.

Face à l'impossibilité d'accéder aux données WhatsApp sur un appareil Android, une approche alternative consiste à obtenir un accès privilégié au système via le routage.

## 4.4 Root Android

### 4.4.1 Définition du routage

Le routage d'un appareil Android est le processus technique permettant à l'utilisateur d'obtenir un contrôle privilégié, connu sous le nom d'accès "root" ou "superutilisateur", sur le système d'exploitation Android. Android étant basé sur le noyau Linux, l'accès root est analogue aux permissions d'administrateur sur les systèmes Linux ou Unix [87].

### 4.4.2 Avantages

Les utilisateurs routent leurs appareils pour diverses raisons, notamment :

- **Personnalisation avancée** : Modifier l'apparence (thèmes, polices), supprimer les applications préinstallées ("bloatware") [88].
- **Installation d'Applications Spécialisées** : Utiliser des applications nécessitant

un accès root (pare-feu avancés, outils de sauvegarde complets comme Titanium Backup [89], applications d'automatisation profonde) [90].

- **Amélioration des Performances** : Ajuster la fréquence du processeur (overclocking pour plus de vitesse, underclocking pour économiser la batterie) [90].
- **Sauvegarde et Restauration Complètes** : Créer des images complètes du système (Nandroid backups) via une récupération personnalisée [91].

#### **4.4.3 Risques induits par le routage**

Malgré ses avantages, le routage comporte des risques significatifs et multiples qui doivent être soigneusement considérés.

- **Vulnérabilités de sécurité accrues** : Le routage désactive ou contourne une grande partie des mécanismes de sécurité intégrés d'Android, notamment le sandboxing applicatif. Une application malveillante qui obtient l'accès root peut accéder à toutes les données de l'appareil, modifier des fichiers système critiques, installer d'autres malwares, enregistrer les frappes, etc., sans aucune restriction [88].
- **Annulation de la Garantie** : La quasi-totalité des fabricants et opérateurs considèrent que le routage modifie le logiciel de manière non autorisée et constitue une violation des conditions de service. En conséquence, la garantie matérielle et logicielle de l'appareil est généralement annulée [90].
- **Instabilité du Système et Risque de "Bricking"** : Le processus de routage si mal exécuté (mauvais fichiers, mauvaise procédure, interruption), peut entraîner des erreurs graves rendant l'appareil totalement inutilisable – un état appelé "bricked" [88].
- **Refus de service** : De nombreuses applications sensibles à la sécurité, notamment les applications bancaires, les applications de paiement mobile, certaines applications de streaming vidéo et des applications d'entreprise intègrent des mécanismes de détection de root (Root Detection [92]). Si elles détectent que l'appareil est rooté, elles peuvent refuser de fonctionner ou limiter leurs fonctionnalités pour des raisons de sécurité [88].
- **Perte potentielle de données** : Le déverrouillage du bootloader, souvent une étape préalable nécessaire au routage, entraîne systématiquement une réinitialisation d'usine de l'appareil, effaçant toutes les données de l'utilisateur [93]. Des erreurs pendant le processus de flashage d'une récupération ou d'une ROM peuvent également corrompre la partition de données et entraîner une perte de données si aucune sauvegarde préalable n'a été effectuée [88].
- **Problèmes avec les mises à jour officielles** : Les appareils rootés ne peuvent

généralement pas installer les mises à jour logicielles officielles fournies "Over-The-Air" (OTA) par le fabricant ou l'opérateur [93].

L'avantage principal et quasi unique dans ce contexte est de surmonter toutes les restrictions d'accès aux données imposées par le système d'exploitation, permettant la récupération directe du fichier key nécessaire au déchiffrement des messages WhatsApp.

En définitive, si le routage de l'appareil permet effectivement de contourner les restrictions d'Android et d'accéder directement à la clé de chiffrement et à déchiffrer la base de données des messages WhatsApp, résolvant ainsi la problématique initiale d'accès direct aux données, il n'en demeure pas moins que les risques associés sont considérables. Cette méthode expose l'appareil à des vulnérabilités de sécurité accrues, à l'annulation de la garantie, à une potentielle instabilité du système et au risque de "bricking", ainsi qu'au refus de service de certaines applications critiques. Ces inconvénients majeurs rendent le routage une solution peu viable et non souhaitable pour une application grand public.

Par conséquent, bien que le routage offre une solution technique à l'accès, la priorité doit être donnée au développement de solutions de contrôle parental qui n'exigent pas une telle compromission du système, tout en restant efficaces dans leur mission de surveillance. Ainsi, une nouvelle problématique se dessine clairement : "*comment est-il possible d'accéder au contenu des messages WhatsApp de manière fiable, sans recourir au routage de l'appareil et, par conséquent, sans pouvoir accéder à la base de données ?*".

## 4.5 Techniques actuelles de monitoring sans root

Avec les restrictions renforcées introduites par Android 13 et les versions ultérieures, notamment concernant l'accès direct aux données des applications et l'octroi de permissions sensibles, les méthodes de surveillance sans root ont dû s'adapter. Elles dépendent désormais massivement de techniques indirectes. Plutôt que d'essayer d'accéder aux bases de données stockées.

### 4.5.1 Mise en miroir des notifications

Cette technique, utilisant la permission Notification Listener, reste une méthode viable sur Android 13+. Les applications ayant obtenu cette permission peuvent lire le contenu des notifications WhatsApp dès leur arrivée [94]. Des applications commerciales comme AirDroid [94] et potentiellement d'autres outils de contrôle parental l'utilisent pour fournir un aperçu de l'activité de messagerie.

- **Avantages :** Moins gourmande en ressource que la lecture d'écran, peut fonctionner même si WhatsApp n'est pas au premier plan.
- **Inconvénients :** Paramètres restreints, contenu limité, inefficace si les notifications sont désactivées.

#### 4.5.2 Services d'accessibilité (Lecture d'écran)

Les Services d'Accessibilité permettent de lire le contenu textuel affiché à l'écran [95]. Les applications de surveillance modernes (souvent commercialisées comme contrôle parental ou spyware) exploitent cette capacité pour extraire le texte des conversations WhatsApp directement depuis l'écran lorsque l'application est utilisée par la cible. Elles analysent la disposition des éléments de l'interface utilisateur pour identifier les messages entrants et sortants, les noms des contacts, et potentiellement l'heure des messages [94].

- **Avantage :** Permet de capturer le contenu textuel tel qu'il apparaît à l'utilisateur, offrant un contexte plus complet que les notifications.
- **Inconvénients :** Dépend de la structure de l'interface de WhatsApp, dégradation des performances.

#### 4.5.3 Mise en miroir/ Enregistrement d'écran

La méthode de capture d'écran native d'Android, initialement conçue pour l'enregistrement et le partage d'écran légitimes, peut être détournée par des applications de surveillance. Ces applications, telles qu'AirDroid Parental Control, mSpy et KidsGuard Pro, proposent l'enregistrement vidéo de l'écran ou sa diffusion en direct (mise en miroir) vers un appareil distant [94].

- **Avantage :** Capture l'intégralité de ce qui est affiché à l'écran, y compris les messages complets, les images, les vidéos, les statuts, et l'interface de WhatsApp telle que vue par l'utilisateur.
- **Inconvénients :** Nécessite une autorisation explicite de l'utilisateur à chaque démarrage de la capture, consommation de ressources( CPU, bande passante, stockage).

#### 4.5.4 Enregistrement de frappes (Keylogging)

Vise à capturer tout ce que l'utilisateur tape au clavier via les Services d'accessibilité. Un service d'accessibilité peut être configuré pour écouter les événements de saisie de texte dans les champs de l'interface utilisateur, y compris les champs de message de WhatsApp [85].

- **Avantage :** Capture des messages tapés avant leur envoi.
- **Inconvénients :** Paramètres restreints, ne capture pas les messages vocaux, contenu limité.

#### **4.5.5 Liaison avec WhatsApp Web**

Consiste à utiliser un serveur dédié pour exécuter une instance de WhatsApp Web dans un environnement isolé. Cette instance est connectée au compte WhatsApp cible. Des scripts automatisés extraient les données de l'interface WhatsApp Web. Ces informations sont présentées sur un tableau de bord accessible aux parents.

- **Avantage :** Fournit un accès complet aux conversations.
- **Inconvénients :** Risques de sécurité liés à l'accès du compte, persistance de la connexion, ne capture pas les appels.

### **4.6 Limites des approches existantes**

L'analyse des techniques actuelles de monitoring sans root révèle plusieurs méthodes pour tenter de surveiller l'activité de WhatsApp. Cependant, chacune de ces approches présente des limitations qui entravent l'atteinte d'un monitoring complet et fiable tel que visé par notre projet :

- La mise en miroir des notifications ne capture que les messages reçus et s'avère totalement inefficace si l'utilisateur a désactivé les notifications pour WhatsApp ou pour des conversations spécifiques.
- La lecture d'écran impacte drastiquement les performances de l'appareil.
- La mise en miroir/enregistrement d'écran requiert une autorisation explicite de l'utilisateur à chaque session et elle est très gourmande en ressources.
- L'enregistrement des frappes est également problématique. Cette méthode manque cruellement de contexte pour les messages envoyés et ne capture pas les messages reçus.
- Enfin, la liaison avec WhatsApp Web, bien qu'elle puisse fournir un accès plus complet aux conversations, introduit des risques de sécurité non négligeables en exigeant un accès direct au compte WhatsApp de l'utilisateur.

Au-delà des limites des techniques de contournement logiciel analysées, la recherche d'un accès à la clé de chiffrement de WhatsApp via des vulnérabilités Android s'est avérée infructueuse.

Les méthodes existantes ne répondant pas aux exigences de fiabilité, complétude et sécurité, une nouvelle approche s'imposait. L'objectif a donc été de concevoir une solution

apte à surmonter ces obstacles, en visant un monitoring intégré, sécurisé et performant, dont l'architecture est présentée ci-après.

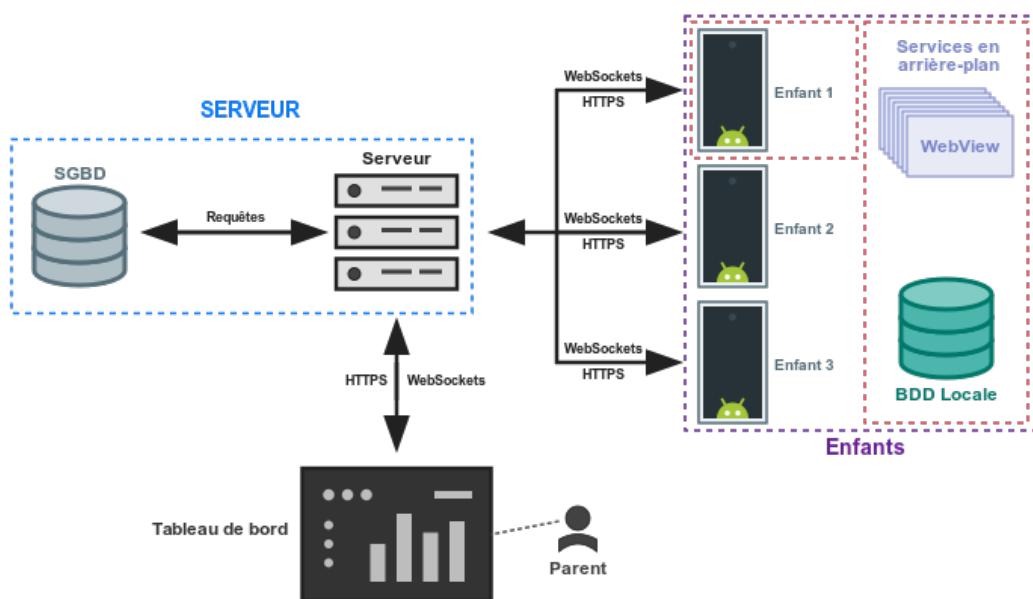
## 4.7 Solution proposée

### 4.7.1 Introduction

Face aux limitations des méthodes de surveillance existantes, aux risques de sécurité induits par le routage et aux difficultés d'accès direct aux données imposées par les récentes versions d'Android, une approche alternative s'est avérée nécessaire. La solution que nous avons conçue et développée repose sur l'exploitation de la fonctionnalité native "*Appareils connectés*" de WhatsApp. Cette méthode permet à notre application, installée sur l'appareil cible, d'agir comme un "appareil connecté" autorisé, recevant ainsi les flux de messages et de données directement de l'instance principale de WhatsApp sur le téléphone source. Une interface web dédiée permet ensuite aux parents d'accéder aux données collectées et de gérer les paramètres de surveillance.

### 4.7.2 Architecture

Notre solution adopte une architecture client-serveur distribuée. Elle s'articule autour de trois composants principaux : l'application installée sur l'appareil cible, un serveur d'application central et un tableau de bord parental. La Figure 4.1 illustre les interactions entre ces composants.



**Figure 4.1:** Architecture de la solution

### **4.7.3 Composants**

#### **4.7.3.1 Serveur central**

- Héberge une application serveur responsable de la logique métier principale, incluant l'authentification sécurisée des applications cibles et des utilisateurs du tableau de bord.
- Assure la gestion des communications et des flux de données entre les applications cibles et les tableaux de bord parentaux :
  - La gestion spécifique des données de communication WhatsApp (messages, médias, détails de contacts) : Le serveur agit ici comme un relais sécurisé et ne stocke pas ces informations de manière persistante. Lorsqu'un parent demande à consulter ces données, le serveur transmet la requête à l'application cible. Les informations récupérées sont alors acheminées via le serveur vers le tableau de bord parental pour un affichage en temps réel, sans être conservées sur le SGBD du serveur.
  - Le traitement des commandes initiées par le parent : Le serveur reçoit les commandes du tableau de bord et les transmet de manière sécurisée à l'application cible concernée pour exécution.
- Un Système de Gestion de Base de Données (SGBD) est utilisé exclusivement pour stocker :
  - Les informations relatives aux comptes utilisateurs (comptes familiaux, profils enfants et parents, appareils associés).
  - Les configurations de surveillance spécifiques à chaque profil enfant.
  - Les alertes générées.
  - Les métadonnées de fonctionnement et d'utilisation (temps d'écran, localisation).
  - Les enregistrements d'appel effectués.
- Un mécanisme de mise en cache, alimenté par un magasin en mémoire, pour servir de couche d'accès rapide devant notre SGBD principal.

#### **4.7.3.2 Application cible**

- Installée sur l'appareil de l'enfant, cette application intègre des services fonctionnant en arrière-plan.
- Intègre un client qui établit une connexion sécurisée (real time / client serveur) avec le serveur central.
- Utiliser une page web pour interagir avec une instance locale de WhatsApp Web.

- Nécessite l'octroi de certaines permissions spéciales pour son fonctionnement optimal.
- Les données de WhatsApp (messages, médias, comptes ,etc.) sont récupérées dynamiquement via la liaison établie et transmises directement au serveur uniquement lorsque le parent en fait la demande depuis le tableau de bord.
- Une BDD Locale est utilisée pour :
  - Le stockage du temps d'écran de WhatsApp.
  - Mettre en cache temporairement des données en attente de transmission au serveur.
  - Conserver des configurations spécifiques comme la liste de mots-clés pour les alertes ou les paramètres de planification pour le blocage de l'application.

#### **4.7.3.3 Tableau de Bord Parental**

- Fournit un accès sécurisé à la visualisation des données collectées par l'application cible.
- Permet la gestion des configurations de surveillance et l'initiation d'actions de contrôle à distance.
- Permet la gestion de multiples profils enfants de manière individualisée.

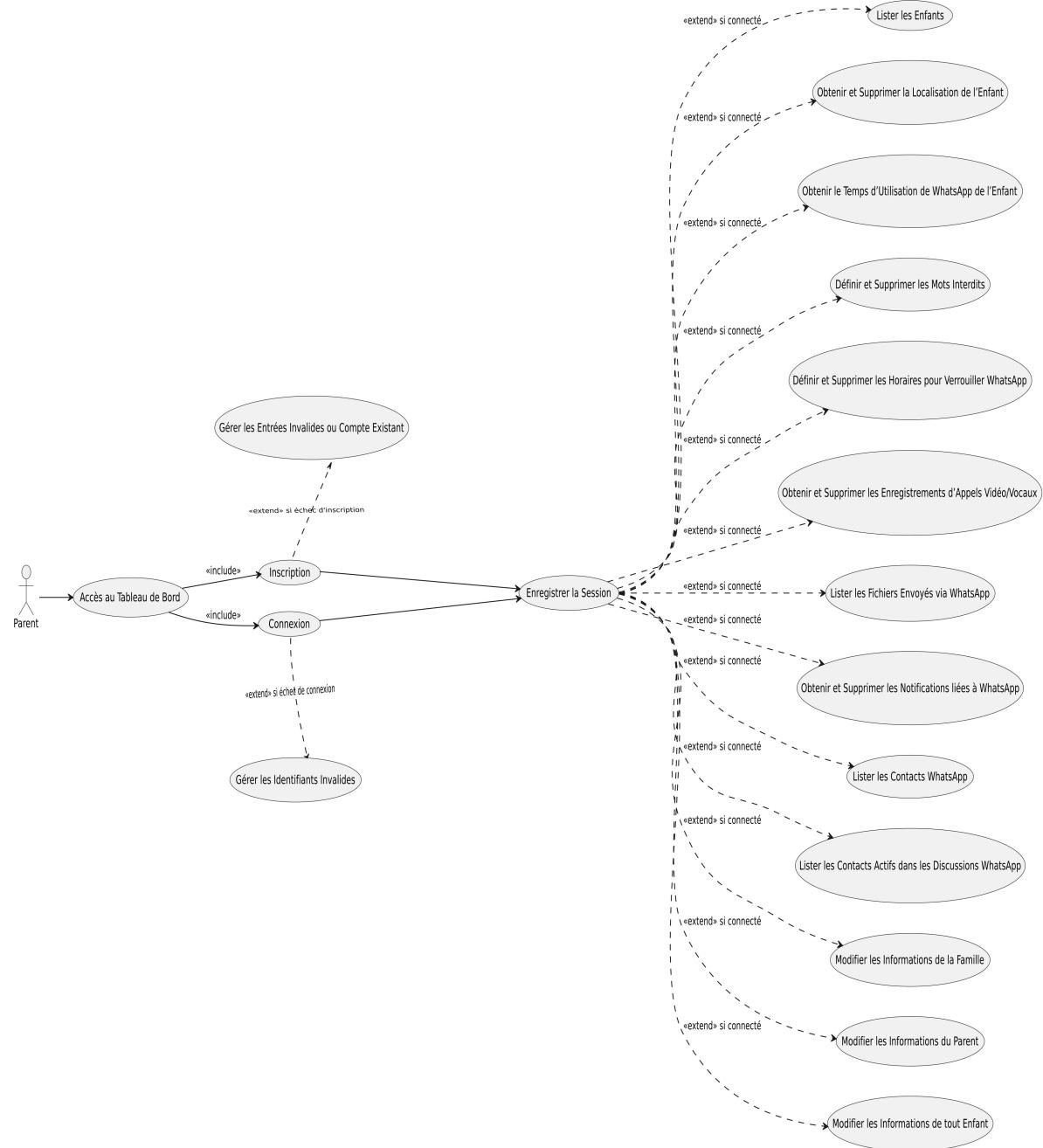
### **4.7.4 Modélisation de la solution**

La modélisation de la solution a pour objectif de représenter les aspects fonctionnels et structurels du système. Elle débute par l'identification des interactions clés des utilisateurs avec le système à travers les diagrammes de cas d'utilisation.

#### **4.7.4.1 Diagrammes de Cas d'utilisation**

Les diagrammes de cas d'utilisation suivants illustrent les fonctionnalités offertes par le système du point de vue des principaux acteurs : le Parent et l'Enfant.

La Figure 4.2 ci-dessous représente les interactions du parent avec le tableau de bord. Ce diagramme détaille les fonctionnalités accessibles au parent via le tableau de bord. L'interaction principale est "Accès au Tableau de Bord", qui conditionne l'accès aux autres fonctionnalités. Cet accès initial se décompose en : Inscription ou connexion suivi d'un enregistrement de session.



**Figure 4.2:** Diagramme de cas d'utilisation - Acteur "Parent"

La Figure 4.3 ci-dessous représente les interactions principales de l'enfant avec l'application installée sur son appareil. Le processus débute par un accès à l'application, cet accès peut mener à une inscription ou une connexion si aucune session n'est enregistrée. L'enfant peut alors voir les informations de base de son profil, le temps passé sur WhatsApp et les plages horaires d'utilisation ou de restriction de WhatsApp.

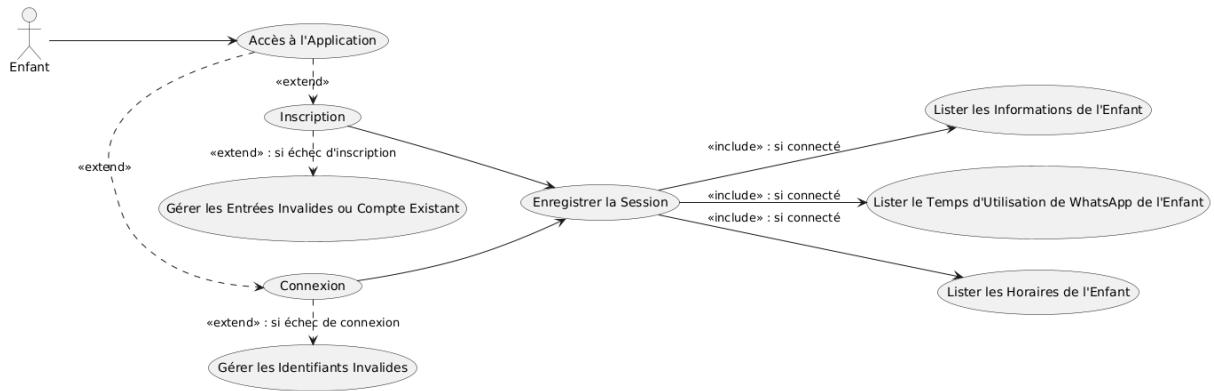


Figure 4.3: Diagramme de cas d'utilisation - Acteur "Enfant"

#### 4.7.4.2 Modèle logique de Données

Le MLD précise la structure de persistance des données gérées par le serveur central :

**Schéma relationnelle :**

**User** (id, username, password, email, first\_name, last\_name, is\_staff, is\_active, is\_superuser, last\_login, date\_joined)  
**BaseUser** (id, gender, birthday, phone\_number, first\_ip, ip, created\_at, deleted, photo)  
**Parent** (id\*, user\_id\*, is\_confirmed, conform\_code, qr\_code, qr\_image, photo)  
**Child** (id\*, user\_id\*, phone\_locked, photo)  
**Family** (id, name, about, father\_id\*, mother\_id\*, deleted, created\_at, last\_updated, qr\_code, qr\_image, photo)  
**Family\_kids** (family\_id\*, child\_id\*)  
**ResetPassword** (id, username\_email, phone\_number, code, created\_at, checked)  
**HourlyUsage** (id, hour, usage\_seconds)  
**UserUsage** (id, child\_id\*)  
**UserUsage\_hourly\_usages** (userusage\_id\*, hourlyusage\_id\*)  
**ChildLocation** (id, child\_id\*, latitude, longitude, accuracy, timestamp, created\_at, is\_deleted)  
**Day** (id, value)  
**Schedule** (id, child\_id\*, name, start\_time, end\_time, start\_date, end\_date, created\_at, is\_deleted)  
**Schedule\_days** (schedule\_id\*, day\_id\*)  
**Notification** (id, child\_id\*, title, content, timestamp, type, is\_read, is\_deleted)  
**BadWord** (id, word)  
**ChildBadWords** (id, child\_id\*)  
**ChildBadWords\_bad\_words** (childbadwords\_id\*, badword\_id\*)

**ChildCallRecording** (**id**, **child\_id\***, date, timestamp, is\_deleted, is\_read, record\_file, recording\_type)

#### 4.7.4.3 Diagrammes de séquence

Pour illustrer le comportement dynamique du système et les interactions entre ses principaux composants, les diagrammes de séquence suivants sont présentés pour des scénarios d'utilisation typiques :

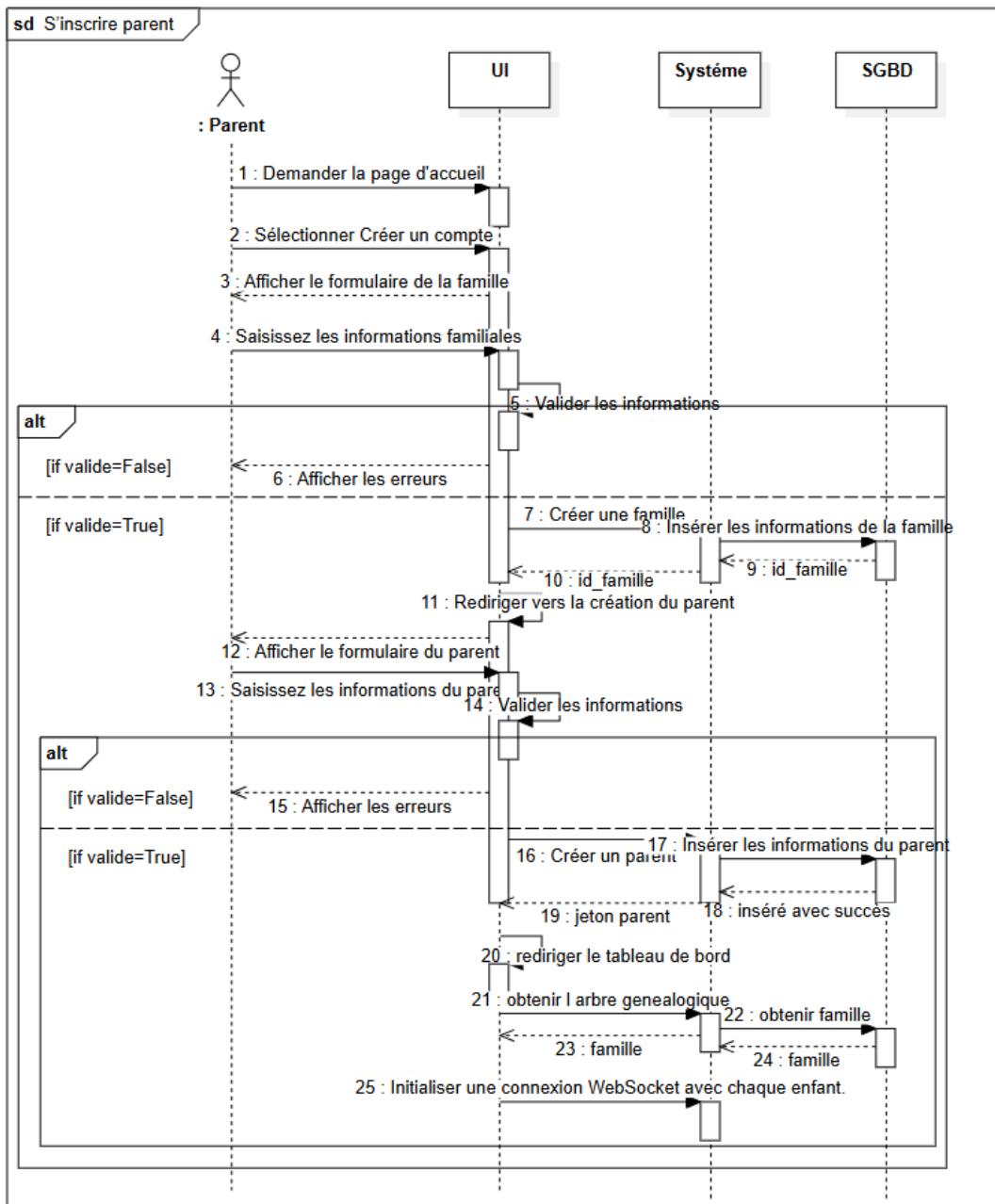


Figure 4.4: Diagramme de séquence - Incription Parent

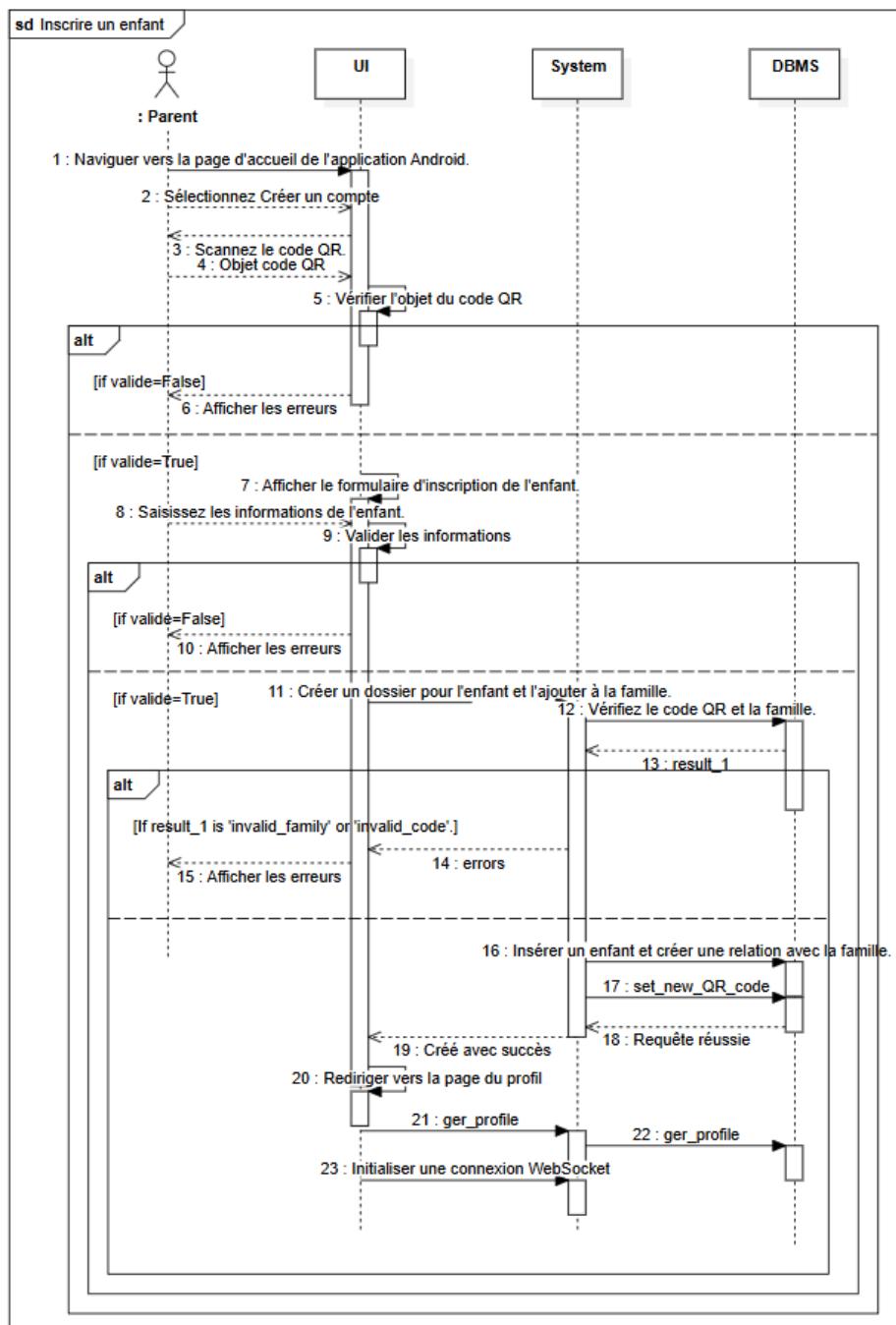


Figure 4.5: Diagramme de séquence - Inscription Enfant

#### 4.7.4.4 Diagramme de classes

Le diagramme de classes est généralement considéré comme le plus important dans un développement orienté objet. Il représente l'architecture conceptuelle du système :

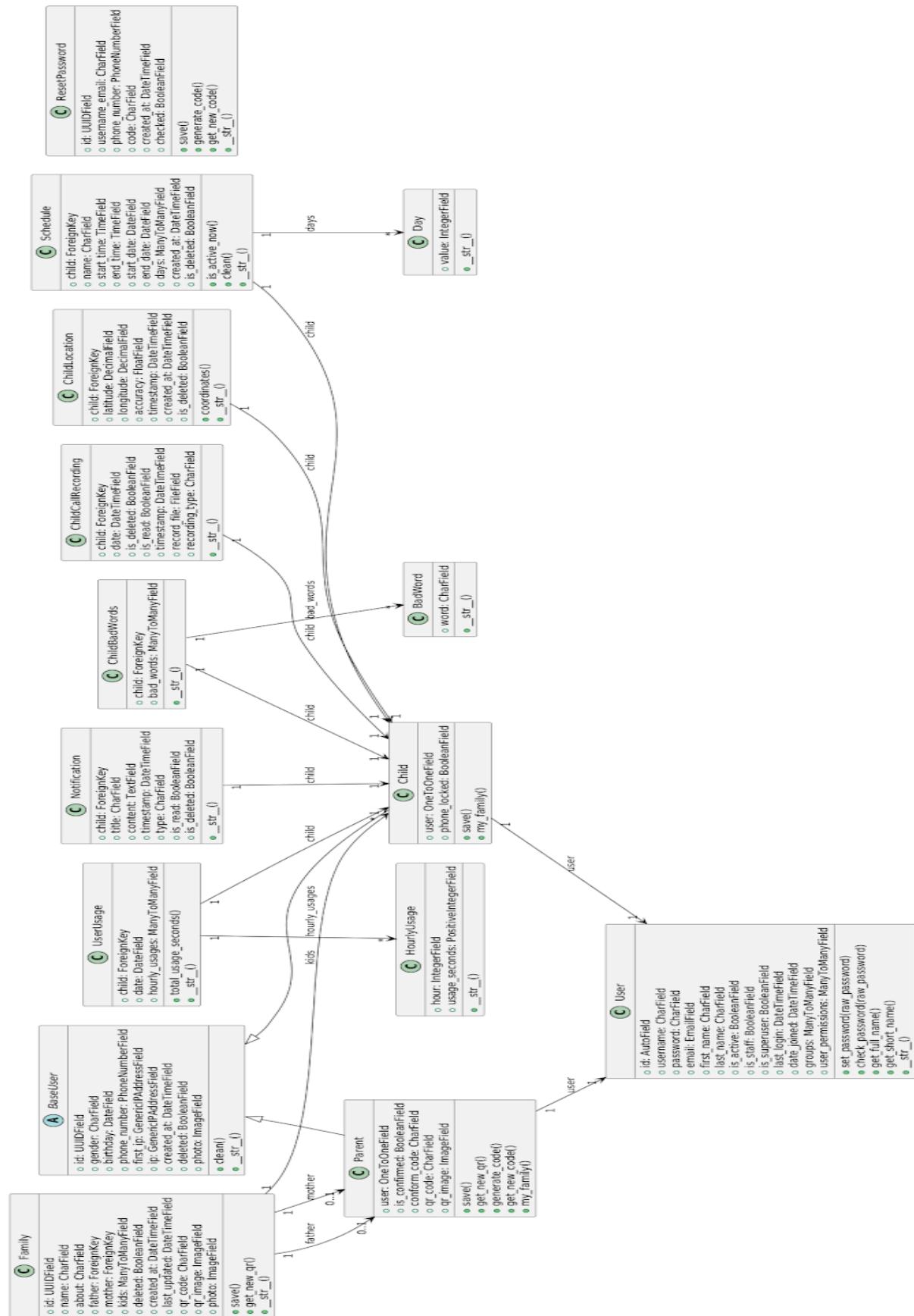


Figure 4.6: Diagramme des classes

#### 4.7.5 Algorithmes de scraping

Nous décrivons ci-dessous quelques-uns des principaux algorithmes de «web scraping» utilisés dans le cadre de ce projet, afin de donner un aperçu de leur mise en œuvre et de leur fonctionnalité.

---

##### **Algorithm 1** Extraire les contacts WhatsApp depuis les discussions

---

**Data :** Liste des discussions WhatsApp visibles  
**Résultat :** Tableau JSON contenant les informations de contact

Simuler la touche Flèche Bas pour activer la navigation  
Mettre le focus sur la barre de recherche  
Récupérer le nombre total de discussions visibles  
Initialiser le tableau **contacts** vide

**foreach** *discussion i dans la liste do*

- Attendre  $10 \times i$  ms
- Sélectionner la discussion active
- if** *la discussion est valide then*
  - Extraire nom, horodatage, dernier message, non lus, icône
  - Ajouter au tableau **contacts**
- else**
  - Ignorer la discussion
- end**
- Simuler l'appui sur Flèche Bas

**end**

Déterminer la langue de l'interface WhatsApp  
Définir les étiquettes traduites : "Non lu", "Fermer discussion", etc.

**foreach** *discussion i dans la liste do*

- if** *discussion a un badge vert then*
  - Attendre 300 ms
  - Ouvrir le menu contextuel
  - Cliquer sur "Marquer comme non lu"
- end**

**end**

Attendre 300 ms  
Cliquer sur l'icône menu de la discussion  
Cliquer sur "Fermer la discussion"  
**if** *le panneau des discussions existe then*

- Réinitialiser le défilement en haut de la liste

**end**

Convertir **contacts** en JSON  
Sauvegarder dans le stockage local sous la clé "WHATSAPP\_CONTACTS"

---

Cet algorithme automatise l'extraction des informations des contacts des discussions WhatsApp en parcourant la liste des chats via la navigation clavier (touche "Flèche Bas"). Pour chaque discussion, il collecte le nom, l'horodatage, le dernier message, le nombre de

messages non lus et l'icône du contact. Il permet également d'effectuer des actions comme marquer une discussion comme non lue ou la fermer, tout en gérant les variations de langue de l'interface WhatsApp. Des délais courts sont inclus pour assurer la stabilité de l'exécution, et les données extraites sont sauvegardées localement pour une utilisation future.

#### **4.7.6 Fonctionnalités**

##### **→ Accès aux messages texte échangés sur WhatsApp**

Permet aux parents de veiller à la sécurité de leur enfant en identifiant et en prévenant les risques potentiels tels que le cyberharcèlement, l'exposition à des contenus inappropriés ou les contacts avec des inconnus malveillants. Pour récupérer les messages de la conversation, l'application cible utilise une technique de web scraping. Un service dédié lance une vue web qui simule l'accès à WhatsApp Web. Des scripts analysent ensuite le contenu affiché dans cette WebView pour en extraire les messages échangés avant de les transmettre au parent.

##### **→ Accès à l'historique des appels entrants et sortants**

Offre aux parents une visibilité sur les interactions vocales de leur enfant, permettant d'identifier des contacts inconnus, des appels à des heures inappropriées, ou une fréquence d'appels qui pourrait indiquer un problème d'harcèlement ou de dépendance. Pour ce faire, l'application cible est configurée pour écouter et intercepter les notifications générées par WhatsApp lors d'appels.

##### **→ Visualisation des enregistrements d'appels**

Permet aux parents, face à des inquiétudes majeures, d'accéder aux enregistrements complets (audio et vidéo) des appels passés via WhatsApp. Lorsque l'enfant participe à un appel audio ou vidéo sur WhatsApp, l'application cible est conçue pour activer l'enregistrement. Ces enregistrements multimédias (fichiers audio/vidéo) sont ensuite stockés temporairement sur l'appareil de manière sécurisée avant d'être transmis vers le serveur central.

##### **→ Accès aux contacts**

Permet aux parents de connaître les personnes avec lesquelles leur enfant est en contact ou peut entrer en contact sur WhatsApp. Cela aide à identifier les contacts inconnus ou potentiellement suspects. Pour récupérer la liste des contacts WhatsApp, l'application cible utilise une technique de web scraping. Un service dédié lance une vue web qui simule l'accès à WhatsApp Web. Des scripts analysent et interagissent ensuite le contenu affiché dans cette WebView pour en extraire la liste complète des contacts disponibles.

→ **Accès aux médias échangés**

Permet aux parents de visualiser les fichiers médias que leur enfant envoie et reçoit sur WhatsApp. Les images, vidéos, et messages vocaux peuvent révéler des contextes, des émotions, ou des informations cruciales non apparentes dans le texte seul (par exemple, cyber harcèlement visuel, sextage, exposition à des contenus choquants, documents potentiellement dangereux). L'accès à ces médias est donc vital pour une protection complète contre les risques en ligne. Pour accéder aux médias échangés, l'application cible utilise les autorisations systèmes d'accès aux fichiers médias de l'appareil.

→ **Accès aux temps passé sur WhatsApp**

Cette fonctionnalité utilise les autorisations d'accès à l'historique d'utilisation des applications sur Android pour collecter des informations précises sur le temps passé sur WhatsApp. Elle permet aux parents d'identifier une utilisation excessive ou une dépendance potentielle en fournissant des statistiques claires sur les périodes d'activité de l'enfant.

→ **Accès à la localisation de l'appareil à la demande**

L'application utilise le GPS et une connexion en temps réel pour localiser l'enfant. Si le GPS est désactivé, les parents en sont informés. Cette fonctionnalité est essentielle pour assurer la sécurité et savoir où se trouve l'enfant à tout moment.

→ **Bloquer un contact ou Quitter un groupe**

Permet aux parents d'intervenir directement pour protéger leur enfant en cas de harcèlement avéré, de contact avec une personne malveillante, ou d'exposition à un groupe WhatsApp diffusant des contenus inappropriés ou dangereux.

Cette fonctionnalité repose sur des techniques de scraping pour effectuer automatiquement certaines actions, comme bloquer un contact ou quitter un groupe WhatsApp, directement depuis le téléphone de l'enfant.

→ **Bloquer l'accès à WhatsApp**

L'application permet de bloquer l'accès à WhatsApp sur le téléphone de l'enfant, en fonction de règles définies par le parent. Ce blocage est renforcé par un système de code PIN, empêchant l'enfant de modifier les paramètres ou de contourner la restriction. Deux modes de blocage sont disponibles : Blocage immédiat, Blocage programmé.

→ **Alertes basées sur des mots clés**

Permet aux parents d'être notifiés automatiquement lorsque des mots ou expressions spécifiques sont détectés dans les messages WhatsApp de leur enfant.

## 4.8 Justification du choix

Cette approche a été privilégiée pour plusieurs raisons :

- **Accès complet et fiable** : Contrairement à la capture de notifications (limitée aux aperçus) ou à la lecture d'écran (vulnérable aux mises à jour), notre solution permet un accès plus complet et structurellement plus stable aux conversations.
- **Indépendance des permissions restreintes** : Elle ne dépend pas directement des permissions les plus problématiques sous Android 13+ comme les Services d'Accessibilité ou l'Écouteur de Notifications, qui sont soumises aux Paramètres Restreints lors d'installations manuelles (sideloading).
- **Pas de root nécessaire** : La solution fonctionne sans nécessiter le rootage de l'appareil, évitant ainsi les risques de sécurité majeurs, l'annulation de la garantie et les problèmes de compatibilité associés au root.

## Conclusion

Ce chapitre a défini la conception de notre solution de surveillance pour WhatsApp, un défi complexifié par les robustes mécanismes de sécurité d'Android. Après avoir constaté l'inadéquation des approches traditionnelles – le routage étant trop risqué et les techniques sans root existantes trop limitées en fiabilité et en fonctionnalités – nous avons dû innover.

Notre solution s'appuie sur l'exploitation de la fonctionnalité "Appareils connectés" de WhatsApp. Nous avons présenté son architecture client-serveur, sa modélisation détaillée (cas d'utilisation, modèle de données, séquences d'interactions) et l'ensemble des fonctionnalités de surveillance qu'elle propose.

# Chapitre 5

## Implémentation

### Introduction

Après l'étude conceptuelle du chapitre précédent, nous entrons maintenant dans la phase de réalisation et d'implémentation de notre application. Nous commencerons par examiner l'environnement de travail que nous avons choisi, puis nous passerons en revue les outils et les techniques que nous avons utilisés pour mener à bien ce projet. Enfin, pour mieux illustrer le résultat, nous mettrons en évidence les principales fonctionnalités à l'aide de captures d'écran.

### 5.1 Environnement de Travail

Pour garantir un développement efficace, nous avons soigneusement sélectionné un ensemble d'outils et de ressources adaptés à nos besoins. Voici les principaux éléments de notre environnement technique :

#### 5.1.1 Langages de programmation

##### 5.1.1.1 Kotlin

Kotlin est un langage de programmation moderne, à typage statique, entièrement interopérable avec Java. Il a été conçu pour améliorer la productivité des développeurs et la sécurité du code. C'est le langage préféré pour le développement d'applications Android, car il offre des fonctionnalités telles que la sécurité null, les coroutines pour une programmation asynchrone rationalisée, ainsi qu'un solide écosystème de bibliothèques. Kotlin minimise le code standard, améliore l'expressivité du code et est pris en charge par



des outils tels qu'Android Studio et IntelliJ IDEA, ce qui en fait un choix optimal pour le développement d'applications fiables et faciles à maintenir [96].

#### 5.1.1.2 Python

Python est un langage de programmation interprété, lisible et polyvalent, prenant en charge les paradigmes orienté objet, fonctionnel et procédural. Idéal pour le développement web, la science des données, l'automatisation et l'intelligence artificielle, il se distingue par sa syntaxe claire, sa bibliothèque standard étendue et son écosystème riche (Django, Flask, NumPy, Pandas), ce qui optimise le développement. Facile à apprendre, évolutif et soutenu par une large communauté, il est prisé par les débutants comme par les experts [97].



#### 5.1.1.3 Javascript

JavaScript est un langage de script polyvalent essentiel pour créer des fonctions dynamiques et interactives sur les pages web. Il permet des fonctionnalités telles que les mises à jour de contenu en temps réel, les cartes interactives et les animations, ce qui en fait un élément fondamental du développement web moderne. JavaScript fonctionne aux côtés de HTML et CSS, formant les technologies de base du web. Sa flexibilité permet aux développeurs d'améliorer considérablement l'expérience de l'utilisateur en mettant en œuvre des fonctionnalités complexes qui vont au-delà du contenu statique [98].



### 5.1.2 Frameworks utilisés

#### 5.1.2.1 Django

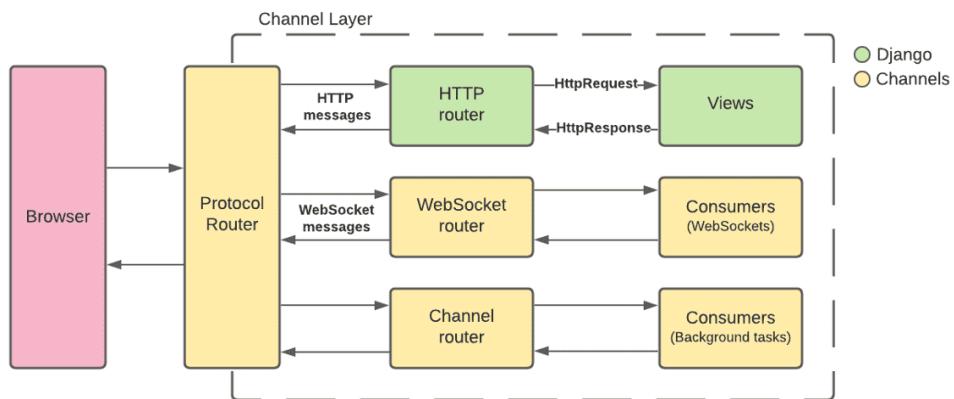
Django est un framework web Python de haut niveau conçu pour un développement rapide et une conception propre et pragmatique. Libre et gratuit, il permet aux développeurs de créer des sites web sûrs et faciles à entretenir. Ses principales caractéristiques sont une interface d'administration automatique, un système ORM (Object-Relational Mapping) et des mesures de sécurité intégrées contre les menaces courantes telles que l'injection SQL et le cross-site scripting. L'architecture de Django promeut le principe DRY (Don't Repeat Yourself), qui permet de rationaliser le processus de développement. Le framework est particulièrement réputé pour sa rapidité



et son évolutivité, ce qui le rend adapté aussi bien aux petits projets qu’aux applications à grande échelle [99].

### 5.1.2.2 Django Channels

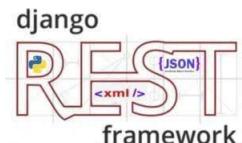
Est une extension du framework Django qui permet de gérer des protocoles asynchrones tels que les WebSockets, les protocoles de chat et les protocoles IoT, en plus des requêtes HTTP traditionnelles. Elle s’appuie sur l’interface ASGI (Asynchronous Server Gateway Interface), qui permet des styles de communication à la fois synchrones et asynchrones. Cette fonctionnalité est essentielle pour le développement d’applications web en temps réel, telles que les applications de chat, qui nécessitent des connexions de longue durée [100]. La Figure 5.1 illustre le fonctionnement de Django channels :



**Figure 5.1:** Flux de communication entre le navigateur et le serveur

### 5.1.2.3 Django Framework rest

Est une boîte à outils puissante et flexible pour la création d’API Web. Il offre des fonctionnalités telles qu’une API consultable, des politiques d’authentification, la sérialisation de données complexes et une documentation complète. Ce cadre permet aux développeurs de créer des API faciles à utiliser et à intégrer à diverses sources de données, y compris des données ORM et non ORM. En outre, il prend en charge les vues et le routage personnalisables, ce qui le rend adapté à un large éventail d’applications [101].



### 5.1.2.4 SvelteKit

Est un framework conçu pour développer rapidement des applications web robustes et performantes à l'aide de Svelte. Il fournit une solution complète pour la construction d'applications web en incorporant les meilleures pratiques modernes et en répondant aux défis de développement les plus courants. Les principales fonctionnalités comprennent un routeur basé sur le système de fichiers, des optimisations de construction, un support hors ligne et des options de rendu configurables, ce qui facilite la création d'applications efficaces et conviviales. Pour ceux qui connaissent d'autres frameworks, SvelteKit est analogue à Next.js pour React et Nuxt.js pour Vue [102].



## 5.1.3 Base de données

### 5.1.3.1 PostgreSQL

PostgreSQL est un puissant système de gestion de bases de données relationnelles (SGBDR) open-source qui met l'accent sur l'extensibilité et la conformité à la norme SQL. Il supporte les transactions avec des propriétés d'atomicité, de cohérence, d'isolation et de durabilité (ACID), les vues actualisables automatiquement, les vues matérialisées, les déclencheurs, les clés étrangères et les procédures stockées. PostgreSQL s'appelait à l'origine POSTGRES et a été développé à l'Université de Californie, Berkeley, sous la direction du professeur Michael Stonebraker. Le projet a été renommé PostgreSQL en 1996 pour refléter son support de SQL [103].



### 5.1.3.2 Redis

Redis (REmote DIctionary Server) est un magasin de clés et de valeurs NoSQL en mémoire, à code source ouvert, utilisé principalement comme cache rapide ou base de données. En stockant les données en mémoire, il permet des opérations de lecture et d'écriture extrêmement rapides, ce qui améliore les performances des applications par rapport aux bases de données sur disque. Redis prend en charge de nombreuses structures de données et offre des fonctionnalités telles que la réplication, la haute disponibilité et la persistance sur disque, ce qui le rend idéal pour les applications à faible latence et à haut débit telles que l'analyse en temps réel et la gestion de session [104].



## 5.1.4 Environnements de développement

### 5.1.4.1 Android Studio

Android Studio est l'environnement de développement intégré (IDE) officiel du système d'exploitation Android de Google, conçu spécifiquement pour le développement d'applications Android. Il est basé sur le logiciel IntelliJ IDEA de JetBrains et a été annoncé le 16 mai 2013 lors de la conférence Google I/O. Android Studio fournit un ensemble complet d'outils et de fonctionnalités qui aident les développeurs à concevoir, construire, tester et déboguer des applications Android [105].



### 5.1.4.2 Visual Studio Code

Visual Studio Code est un éditeur de code gratuit, léger et puissant de Microsoft, compatible avec Windows, macOS, Linux et Raspberry Pi OS. Il offre un environnement efficace pour coder, déboguer et exécuter du code, et prend en charge de nombreux langages (JavaScript, TypeScript, Node.js, Python, etc.) ainsi que des extensions. Parmi ses fonctionnalités, on compte l'IntelliSense, le débogage graphique, le linting, l'édition multicurseur et l'intégration Git [106].



## 5.1.5 Outils

### 5.1.5.1 Git

Git est un système de contrôle de version distribué, gratuit et open-source, qui permet de gérer efficacement des projets de toute taille. Il permet à plusieurs développeurs de travailler simultanément sans conflits et est apprécié pour sa rapidité, ses capacités de branchement et de fusion. Avec des fonctionnalités telles qu'une zone de stockage et la prise en charge de différents flux de travail, Git est un outil flexible pour le développement collaboratif [107].



## 5.2 Fonctionnalités Principales

Pour mieux illustrer ce que notre application permet de faire, nous avons sélectionné quelques captures d'écran. Ces visuels donnent un aperçu concret des principales fonctionnalités et de l'ergonomie du produit final.

### 5.2.1 Côté enfant (Application Android)

Du côté de l'enfant, nous fournissons une application Android qui sert de point central pour la collecte d'informations essentielles telles que la localisation, l'activité WhatsApp et le temps passé sur cette application.

Nous présentons ci-dessous quelques captures d'écran illustrant les processus d'inscription et de connexion de notre application. Les utilisateurs peuvent facilement s'inscrire ou se connecter en scannant simplement un code QR. Chaque code QR est unique et ne peut être réutilisé pour lancer une nouvelle session, ce qui garantit que l'accès reste à la fois simple et sécurisé.

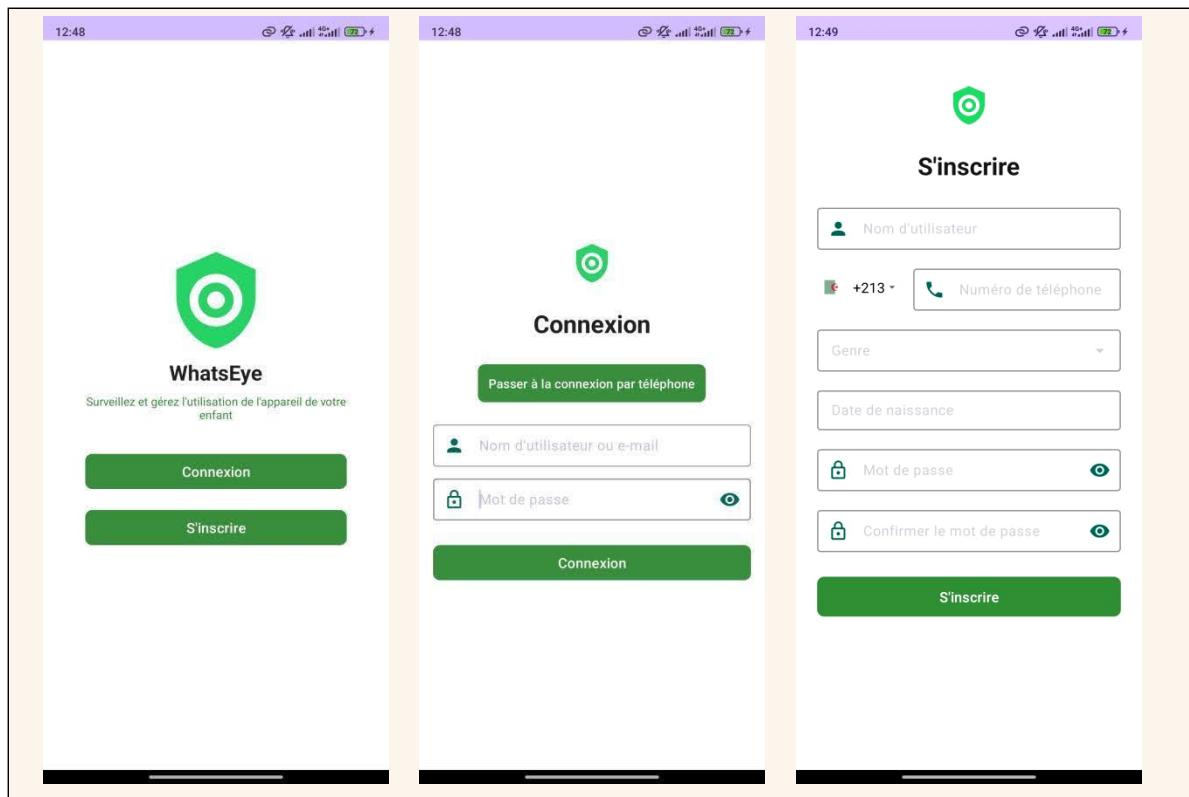


Figure 5.2: Interfaces d'inscription et de connexion - Android

## 5.2.2 Côté parent (Dashboard Web)

Du côté des parents, nous proposons un tableau de bord en ligne leur permettant de surveiller plusieurs enfants simultanément. Les parents peuvent y suivre le temps d'utilisation de WhatsApp, définir des plages horaires et accéder aux espaces de discussion de leurs enfants. Ci-dessous, nous présentons quelques pages du tableau de bord pour illustrer le processus d'utilisation.

### 5.2.2.1 Connexion et inscription

Les captures d'écran de la Figure 5.3 illustrent les pages de connexion et d'inscription. Pour commencer, le parent doit d'abord créer un groupe familial. Une fois le groupe familial créé, le compte du parent y est automatiquement ajouté.



**Figure 5.3:** Interfaces de connexion et d'inscription - Web

## Conclusion

Cette section a permis de mieux comprendre le travail accompli en présentant les différentes interfaces du projet. Elle clôture ainsi la phase de développement de notre application de contrôle parental, qui comprend une application Android et un tableau de bord web .

# Conclusion Générale

Ce travail a permis d'analyser en profondeur l'environnement Android ainsi que le fonctionnement détaillé de WhatsApp, deux composantes majeures de la communication mobile moderne. À travers l'étude de l'architecture du système, des mécanismes de gestion de la mémoire et du stockage ainsi que des dispositifs de sécurité intégrés à Android, nous avons montré que cet écosystème repose sur des concepts à la fois riches et complexes, offrant une flexibilité sans précédent pour le développement d'applications adaptées à des usages spécifiques. L'attention s'est ensuite portée sur WhatsApp, application de messagerie instantanée incontournable à l'échelle mondiale, afin d'en détailler le fonctionnement, la structure ainsi que les mécanismes de chiffrement bout en bout garantissant la confidentialité des échanges. Cette étude a permis de mettre en lumière les enjeux spécifiques liés à l'usage intensif de WhatsApp par les plus jeunes, ainsi que les limites des dispositifs de contrôle parental existants. C'est justement dans ce contexte qu'a été élaborée et détaillée la solution proposée, visant à concevoir un outil de surveillance parentale ciblé, respectueux de la vie privée, adapté à l'environnement Android, et capable de répondre efficacement à des besoins concrets tels que la protection des enfants vis-à-vis de contenus dangereux, de groupes à risque ou de contacts malveillants. Le travail de conception ainsi que l'implémentation de la solution illustrent à la fois la faisabilité technique du projet ainsi que la valeur qu'il peut apporter aux parents soucieux de la sécurité numérique de leurs enfants.

Ce travail n'est certainement pas parfait et pourrait être amélioré à bien des égards. D'autres fonctionnalités pourraient ainsi compléter la solution envisagée, notamment l'ajout d'alertes en temps réel lors de la détection de contenus suspects, la mise en place d'algorithmes de traitement du langage naturel (NLP) pour identifier de manière proactive des conversations à risque, ainsi que le renforcement de l'expérience utilisateur du tableau de bord parent à travers des visualisations plus détaillées et intuitives. Par ailleurs, l'intégration de modèles d'apprentissage automatique pourrait permettre d'affiner la précision du filtrage ainsi que la personnalisation des règles de surveillance selon l'âge de l'enfant ou le contexte d'utilisation. En définitive, ce travail s'inscrit dans une réflexion

## *CONCLUSION GÉNÉRALE*

---

plus large sur la protection des plus jeunes dans un environnement mobile en constante évolution. À mesure que les technologies progressent, la mise en place de dispositifs de contrôle plus adaptés, plus précis et plus respectueux de la vie privée restera un défi majeur. Ce mémoire fournit ainsi une base solide pour des futurs travaux visant à concevoir des mécanismes de contrôle parental plus performants, plus intelligents et mieux adaptés à la diversité des usages du numérique, contribuant ainsi à construire un environnement digital plus sûr pour tous.

## Annexe A

# Historique des versions d'Android

La Figure A.1 présente les principales versions d'Android depuis la première version en 2008.

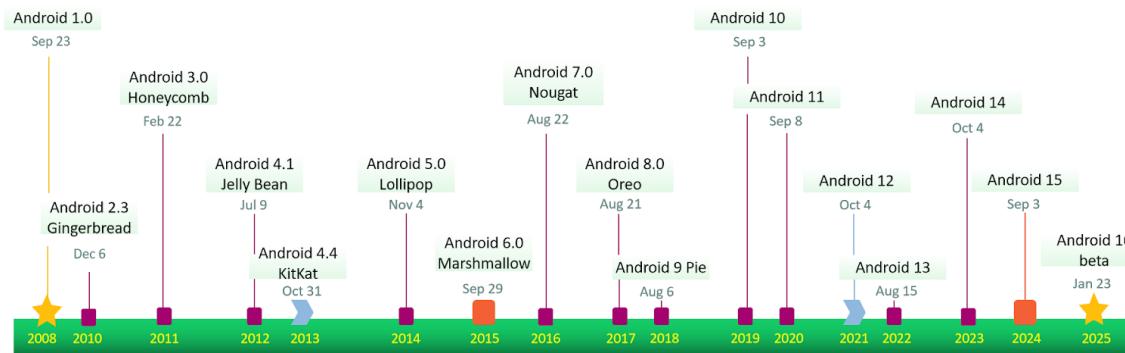


Figure A.1: Versions d'Android 2008-2025

Depuis sa création en 2008, le système d'exploitation a subi d'importantes transformations et de nombreuses versions ont été publiées au fil des ans. De la version 1.0 à la dernière version bêta 16 en 2024, le système d'exploitation a considérablement évolué, avec l'intégration de nouvelles fonctionnalités, d'améliorations et de perfectionnements.

Le 22 août 2019, il a été annoncé qu'Android Q serait simplement désigné par "Android 10" [108], marquant ainsi un changement dans la convention de nommage de Google. Ce changement marque la fin de la pratique consistant à utiliser des noms de code alphabétiques basés sur des produits de confiserie pour les versions majeures. Cette nouvelle approche vise à simplifier et à clarifier la nomenclature, permettant aux utilisateurs d'identifier plus facilement les versions sans avoir recours à des noms de code sur le thème des desserts.

En 2017, Google a apporté une modification importante aux règles du Google Play Store, exigeant que les applications ciblent une version récente d'Android. Cette initia-

tive vise à garantir que toutes les applications bénéficient pleinement des dernières fonctionnalités, améliorations et renforcements de sécurité offerts par les nouvelles versions d'Android [109].

En raison de ce changement significatif, nous ne couvrirons que les fonctionnalités et les mises à jour majeures des versions récentes d'Android 13 à Android 16 bêta, disponibles dans le Tableau A.1.

Version	Fonctionnalités
Android 13	<ul style="list-style-type: none"><li>● Personnalisation de Material You : des options de personnalisation améliorées permettent aux applications non Google de s'adapter au thème et aux couleurs du fond d'écran, créant ainsi un aspect plus cohérent sur votre écran d'accueil. Toutefois, pour bénéficier de cette fonctionnalité, les développeurs doivent l'accepter [110].</li><li>● Permet de personnaliser davantage le mode « Sommeil » grâce à l'atténuation du fond d'écran et au thème sombre. Ces options d'écran aident vos yeux à s'adapter à l'obscurité lorsque vous allez vous coucher, et à vous rendormir si vous vous réveillez la nuit pour consulter votre téléphone [110].</li><li>● Finis les temps où vous deviez partager l'intégralité de votre bibliothèque multimédia avec vos applications. Dans Android 13, vous pouvez sélectionner les photos et vidéos auxquelles les applications doivent avoir accès [110].</li><li>● Empêchez tout accès indésirable à votre presse-papiers. Si vous copiez des données sensibles telles que votre adresse e-mail, votre numéro de téléphone ou vos identifiants de connexion sur votre appareil, Android effacera automatiquement l'historique de votre presse-papiers au bout d'un certain temps [110].</li><li>● Permet de contrôler vos notifications et de vous assurer que vous ne recevez que les alertes dont vous avez exprimé le besoin. Les applications devront désormais obtenir votre autorisation explicite pour envoyer des notifications, au lieu d'être autorisées par défaut [110].</li></ul>

<b>Android 14</b>	<ul style="list-style-type: none"><li>• Le sélecteur de personnalisation mis à jour d'Android 14 facilite le passage d'un fond d'écran à l'autre et permet de mettre à jour ce que vous souhaitez voir d'un seul coup d'œil. Vous pouvez désormais définir des raccourcis personnalisés sur l'écran de verrouillage, comme le lecteur QR ou l'application Google Home, afin d'accéder rapidement et d'un seul geste aux commandes les plus utilisées, directement depuis l'écran de verrouillage d'Android [111].</li><li>• Offre des méthodes plus intuitives pour se connecter et interagir avec vos appareils auditifs. Vous disposez notamment d'un flux de configuration dédié aux appareils auditifs dans les paramètres d'accessibilité, d'un moyen facile d'acheminer l'audio vers différentes sorties et d'un raccourci pour accéder rapidement aux commandes des appareils auditifs. De même, les sons de notification, les sonneries ou les alertes [111].</li><li>• Vous bénéficiez également d'une meilleure visibilité sur la façon dont vos données sont utilisées par les applications qui en font la demande. Grâce aux nouvelles mises à jour du partage des données dans Android 14, lorsque vous êtes invité à autoriser des applications à accéder à des informations telles que votre position, vous serez averti si une application partage des données de position avec des tiers, et vous pourrez décider en connaissance de cause d'autoriser ou non l'accès à ces données [111].</li><li>• La protection numérique sur Android 14 s'étend également à vos informations les plus sensibles, comme les numéros d'identification personnels (PIN) de votre appareil. Android 14 renforce la sécurité du code PIN en vous encourageant à en choisir un de six chiffres. Après avoir saisi le bon code PIN de six chiffres ou plus, votre appareil se déverrouillera automatiquement, sans nécessiter d'appui sur la touche Entrée [111].</li></ul>
<b>Android 15</b>	<ul style="list-style-type: none"><li>• Étend la prise en charge de la connectivité par satellite, permettant ainsi aux applications de messagerie SMS et RCS préchargées ainsi qu'aux applications de messagerie des opérateurs d'utiliser la connectivité par satellite pour envoyer et recevoir des messages [112].</li></ul>

		<ul style="list-style-type: none"><li>• Sur les appareils pliables et les tablettes, vous pouvez facilement épingler et désépingler votre barre des tâches sur l'écran. Vous pouvez ainsi personnaliser votre affichage et garder vos applications préférées, comme Google Photos ou Gmail, à portée de main pour un accès plus rapide et une meilleure productivité [112].</li><li>• Le nouveau verrou de détection de vol utilise l'intelligence artificielle pour assurer la sécurité de vos données. En cas de vol avec fuite à pied, à vélo ou en voiture, il se verrouille automatiquement. Vous pouvez également utiliser le verrouillage à distance pour verrouiller rapidement votre appareil depuis n'importe quel appareil en entrant votre numéro de téléphone dans un simple contrôle de sécurité. Ces fonctionnalités sont désormais disponibles pour la plupart des appareils Android 10+ [112].</li></ul>
<b>Android 15</b>		<ul style="list-style-type: none"><li>• L'espace privé dans Android 15 agit comme un coffre-fort numérique sur votre téléphone. Vous pouvez y créer un espace séparé pour organiser les applications sensibles, comme vos applications de rencontre, bancaires ou sociales. Lorsque l'espace privé est verrouillé, les applications restent pratiquement invisibles pour les autres et sont cachées de votre liste d'applications, de l'affichage des applications récentes, des notifications et des paramètres. Pour y accéder, une couche supplémentaire d'authentification permet de sécuriser les applications et de les mettre à l'abri des regards indiscrets. Pour plus de confidentialité, vous pouvez également choisir de masquer l'existence de l'espace privé sur votre téléphone [112].</li></ul>
<b>Android bêta</b>	<b>16</b>	<ul style="list-style-type: none"><li>• Mises à jour en direct Il s'agit de notifications dynamiques qui aident les utilisateurs à suivre et à accéder rapidement aux activités importantes en cours, telles que le covoiturage et la livraison de repas, en temps réel [113].</li><li>• Apps adaptatives Cette fonction permet aux apps d'adapter leurs fonctionnalités en fonction du contexte et des préférences de l'utilisateur, offrant ainsi une expérience plus personnalisée [113].</li><li>• Prend également en charge le codec APV (Advanced Professional Video), qui offre un codage intra-trame uniquement à haut débit, une qualité vidéo sans perte perceptive et des débits binaires élevés, même lors de prises de vue en 4K et 8K [113].</li></ul>

<b>Android bêta</b>	<b>16</b>	<ul style="list-style-type: none"><li>• Privacy Sandbox permet d'améliorer le cryptage des données et le traitement des informations sensibles, offrant ainsi une sécurité accrue pour les utilisateurs [114].</li><li>• Google ajoute la prise en charge de fonctions de sécurité robustes dans la localisation Wi-Fi sur les appareils compatibles avec la norme 802.11az du Wi-Fi 6. Grâce à cela, les applications peuvent désormais combiner la plus grande précision, l'évolutivité et la planification dynamique du protocole avec des améliorations en matière de sécurité, notamment le cryptage AES-256 et la protection contre les attaques MITM. Cela permet de l'utiliser de manière plus sûre dans les cas d'utilisation de proximité, comme le déverrouillage d'un ordinateur portable ou d'une porte de véhicule par exemple [114].</li></ul>
---------------------	-----------	---

**Tableau A.1:** Les nouvelles fonctionnalités des dernières versions d'Android

# Annexe B

## Interfaces de la solution

### B.1 Côté enfant (Application Android)

#### B.1.1 Autorisations requises

Vous trouverez ci-dessous des captures d'écran illustrant les autorisations demandées par l'application. Ces autorisations sont indispensables pour garantir le bon fonctionnement de l'application (voir les Figures B.1 et B.2).

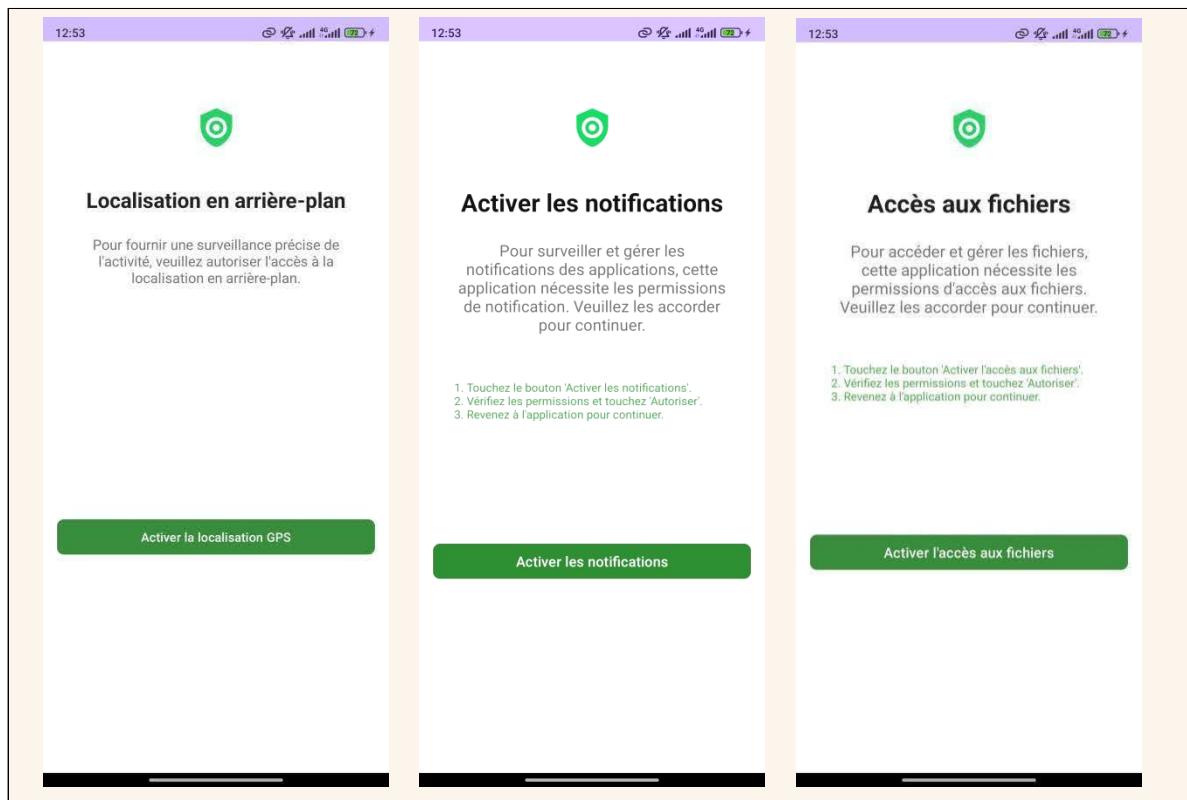


Figure B.1: Autorisations requises I

## ANNEXE B. INTERFACES DE LA SOLUTION

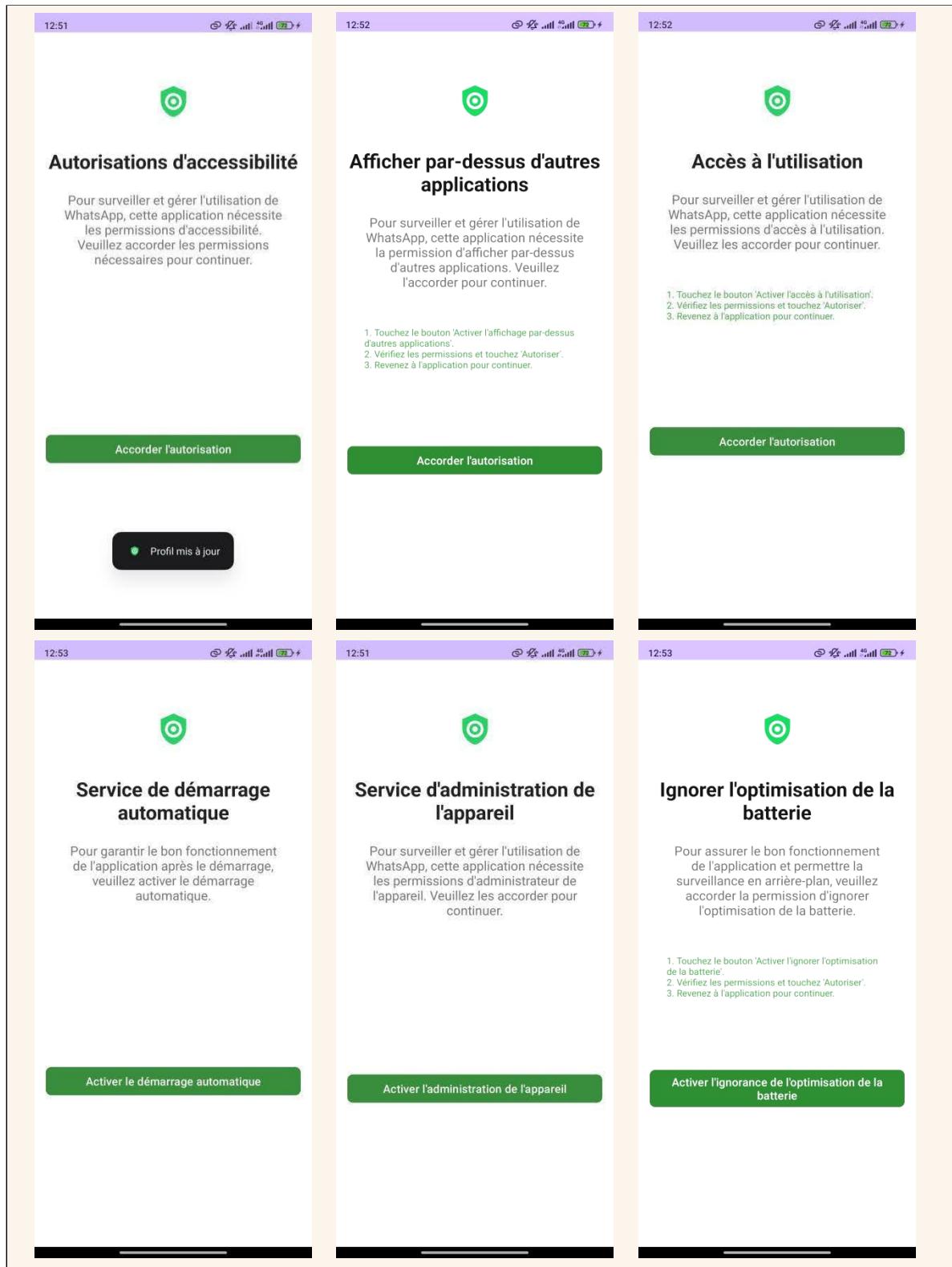


Figure B.2: Autorisations requises II

### B.1.2 Interfaces de l'application

Les captures d'écran de la Figure B.3 illustrent la page de demande de code PIN, la page par défaut accessible à l'enfant et la page permettant au parent de mettre à jour les paramètres à partir du téléphone de l'enfant. Cette dernière est protégée par un code PIN pour des raisons de sécurité.

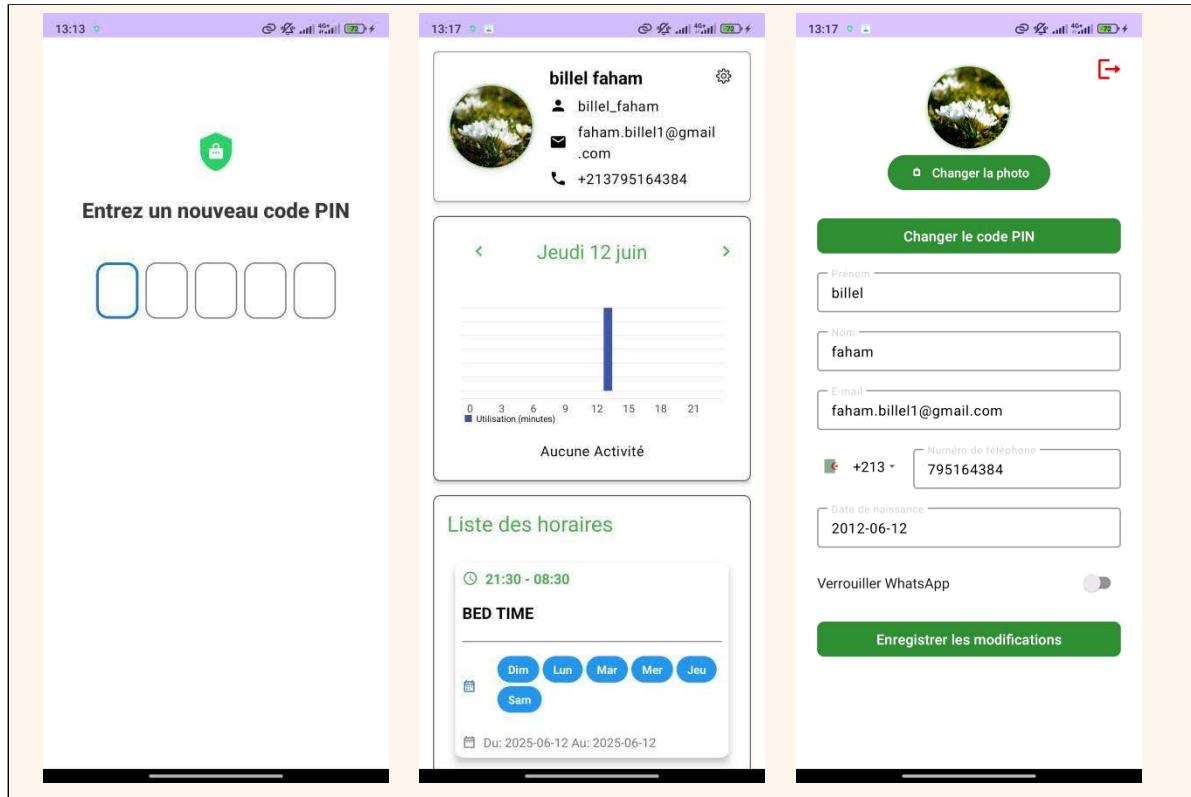


Figure B.3: Intefraces Android

## B.2 Côté parent (Dashboard Web)

### B.2.1 Page d'accueil du tableau de bord parental

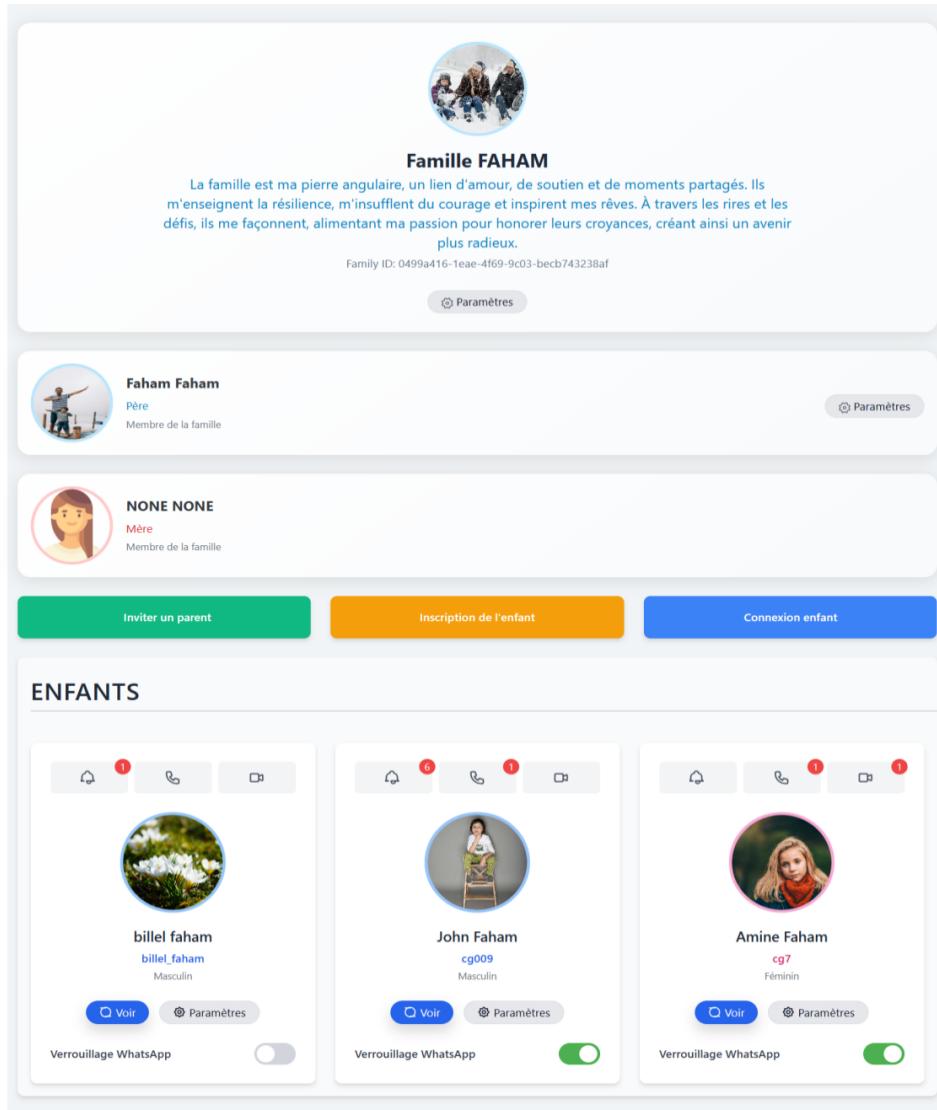


Figure B.4: Page d'accueil du tableau de bord

## B.2.2 Page d'accueil du tableau de bord après la sélection d'un profil enfant

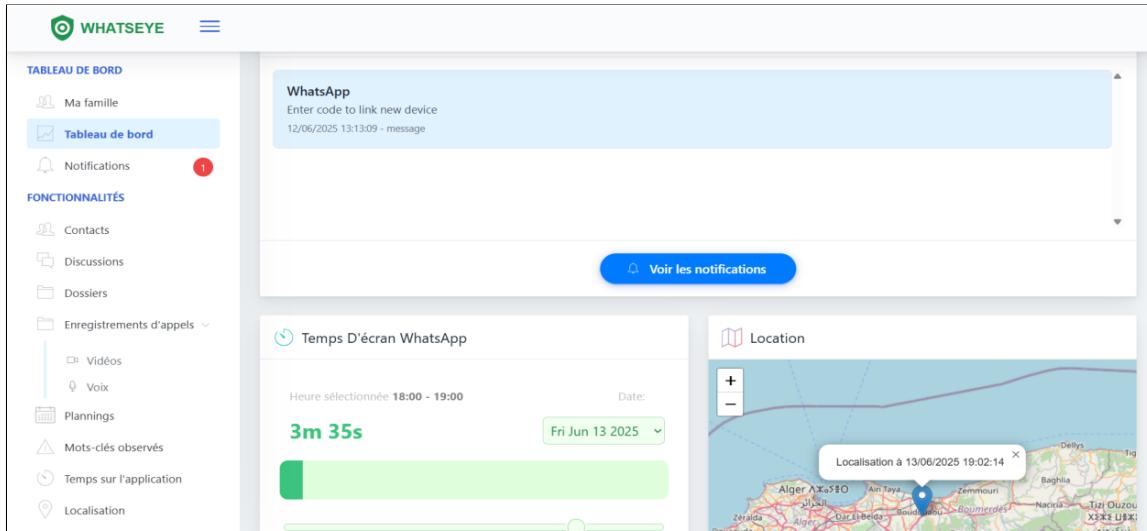


Figure B.5: Tableau de bord - Enfant sélectionné

## B.2.3 Page de notifications

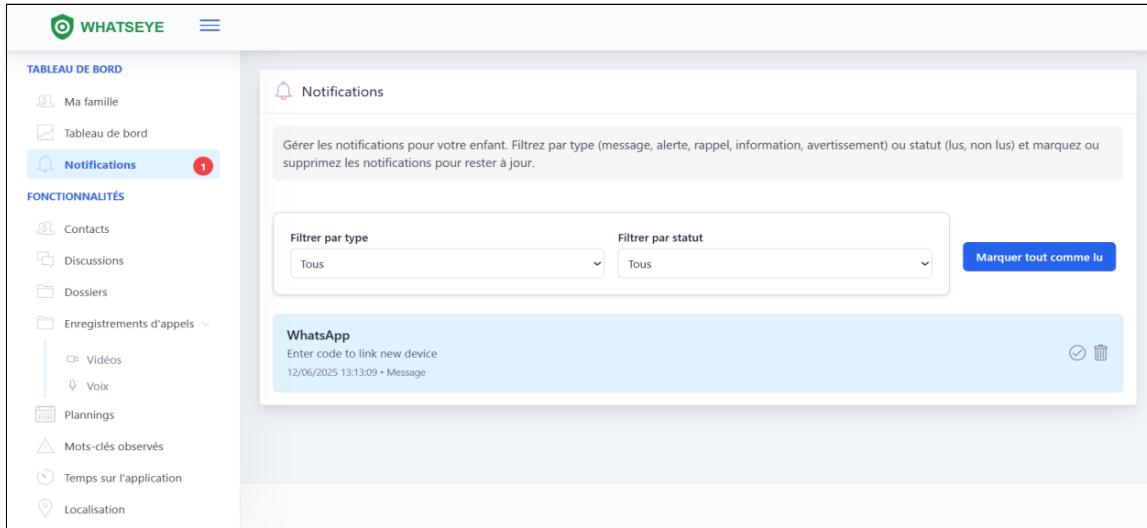


Figure B.6: Tableau de bord - Notifications

### B.2.4 Page de liste des contacts WhatsApp

**TABLEAU DE BORD**

- Ma famille
- Tableau de bord
- Notifications

**FONCTIONNALITÉS**

- Contacts** (selected)
- Discussions
- Dossiers
- Enregistrements d'appels
- Plannings
- Mots-clés observés
- Temps sur l'application
- Localisation

**Contacts**

- + Message yourself
- A
- Hey there! I am using WhatsApp.
- a Hey there! I am using WhatsApp.
- Salut ! J'utilise WhatsApp.
- Salut ! J'utilise WhatsApp.

Figure B.7: Tableau de bord - Contacts

### B.2.5 Page de discussion et de salons de discussions WhatsApp

**TABLEAU DE BORD**

- Ma famille
- Tableau de bord
- Notifications

**FONCTIONNALITÉS**

- Contacts
- Discussions** (selected)
- Dossiers
- Enregistrements d'appels
- Plannings
- Mots-clés observés
- Temps sur l'application
- Localisation

**Chats**

- fb Yesterday
- Space group Yesterday
- USTHB team Yesterday
- WhatsApp Wednesday
- OPFE Sunday
- Group 28/05/2025

Figure B.8: Tableau de bord - Discussions

### B.2.6 Page d'accès au dossier multimédia de WhatsApp

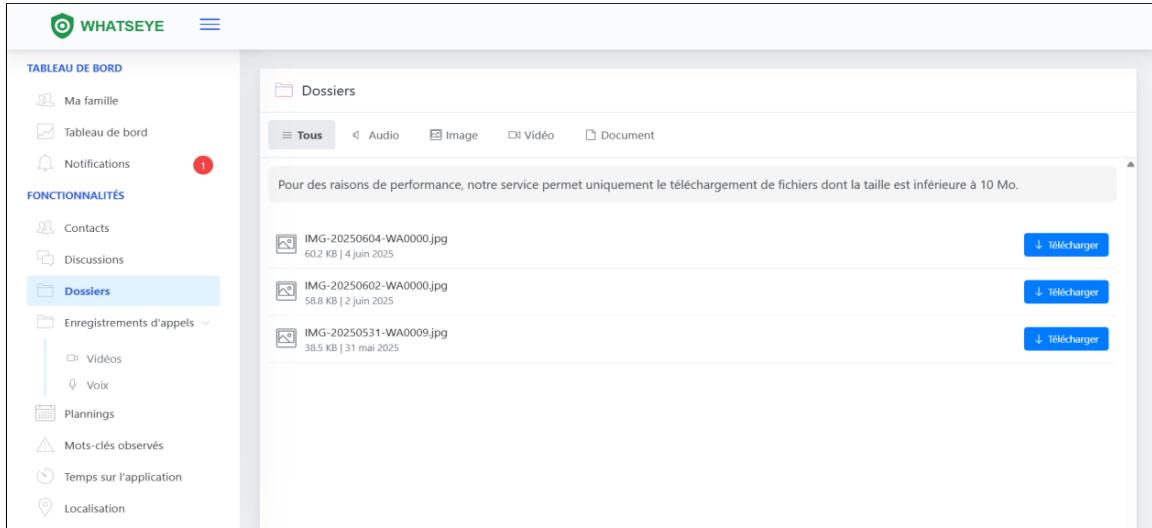


Figure B.9: Tableau de bord - Dossiers

### B.2.7 Page de configuration du calendrier d'utilisation de WhatsApp

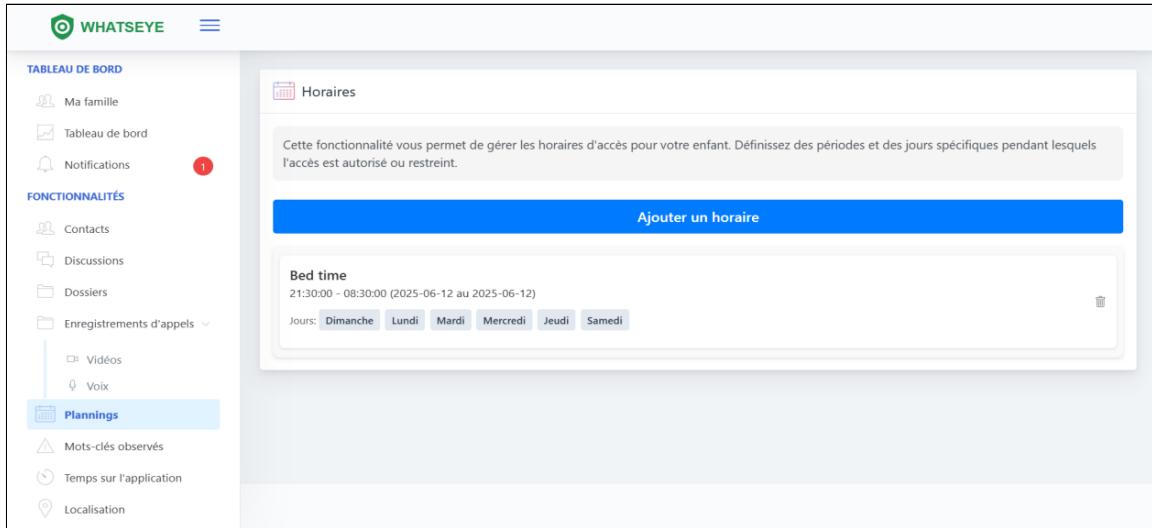


Figure B.10: Tableau de bord - Plannings

### B.2.8 Page d'enregistrement des appels vocaux et vidéos

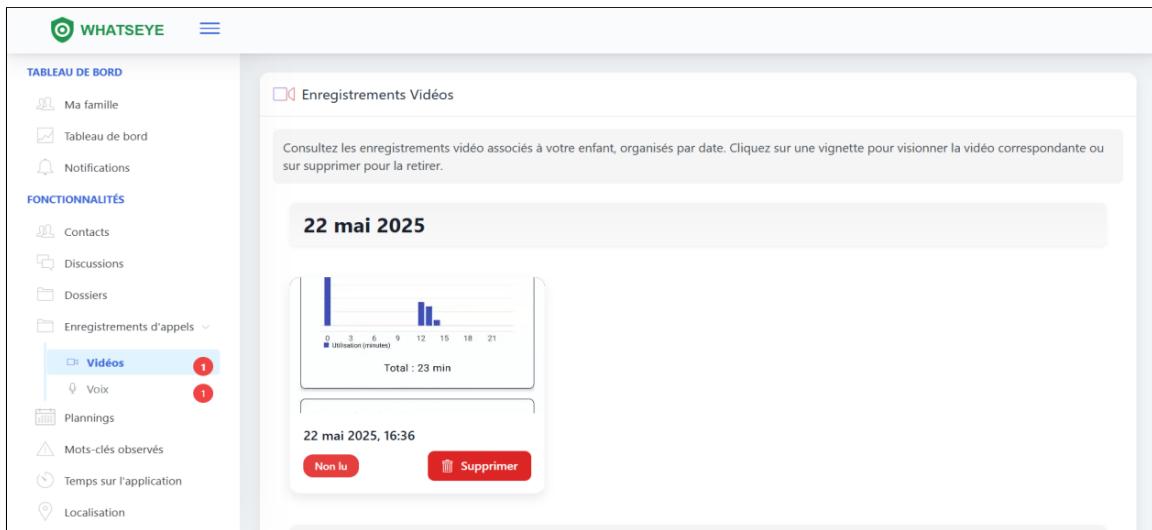


Figure B.11: Tableau de bord - Vidéos

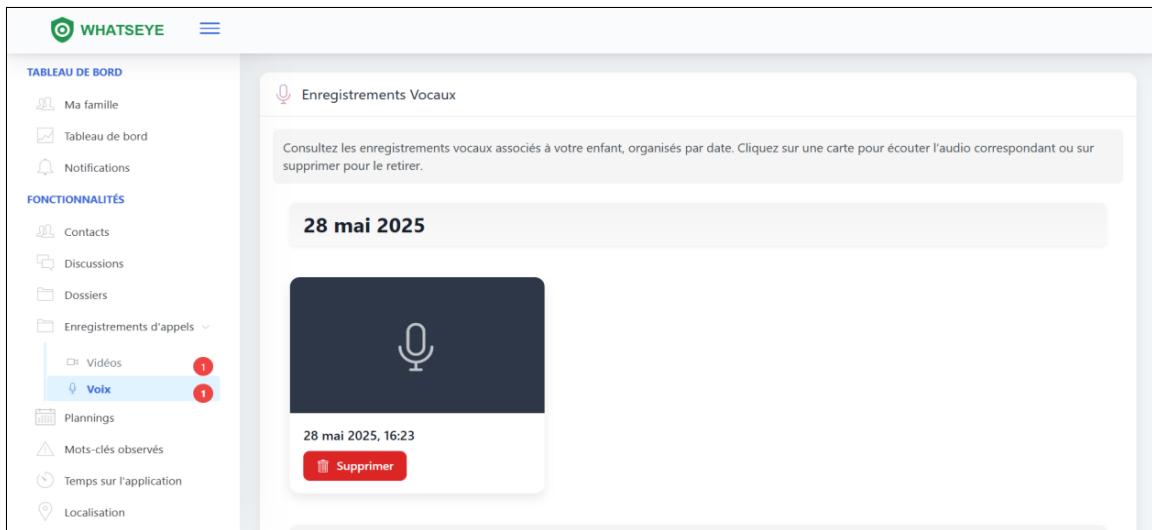


Figure B.12: Tableau de bord - Voix

## ANNEXE B. INTERFACES DE LA SOLUTION

### B.2.9 Page d'alertes de langage inapproprié

The screenshot shows the Whatseye dashboard interface. On the left, there is a sidebar with various navigation options: Ma famille, Tableau de bord, Notifications, Contacts, Discussions, Dossiers, Enregistrements d'appels (with Vidéos and Voix), Plannings, Mots-clés observés (which is highlighted in blue), Temps sur l'application, and Localisation. A red circle with the number '1' is visible next to the Notifications icon. The main content area is titled 'Mots Clés Observés' and contains a sub-section 'Ajouter un mot interdit' (Add a prohibited word) with a text input field and a 'Ajouter' (Add) button. Below this, the word 'moi' is listed in a scrollable list.

**Figure B.13:** Tableau de bord - Mots Clés

### B.2.10 Page de statistiques d'utilisation de WhatsApp

The screenshot shows the Whatseye dashboard interface. The sidebar is identical to Figure B.13. The main content area is titled 'Temps D'écran' (Screen Time). It displays a timeline from 00:00 to 23:00 with a green bar indicating usage from 13:00 to 14:00. The total usage for the day is shown as '0h 26m 25s'. Below this, a section titled 'Temps total de la journée' (Total day time) shows the usage for specific dates: mercredi 28 mai (0h 15m 59s), mardi 27 mai (0h 2m 46s), lundi 26 mai (0h 26m 25s, which is highlighted in blue), and dimanche 25 mai (0h 2m 2s).

**Figure B.14:** Tableau de bord - Temps d'écran

### B.2.11 Page de localisation

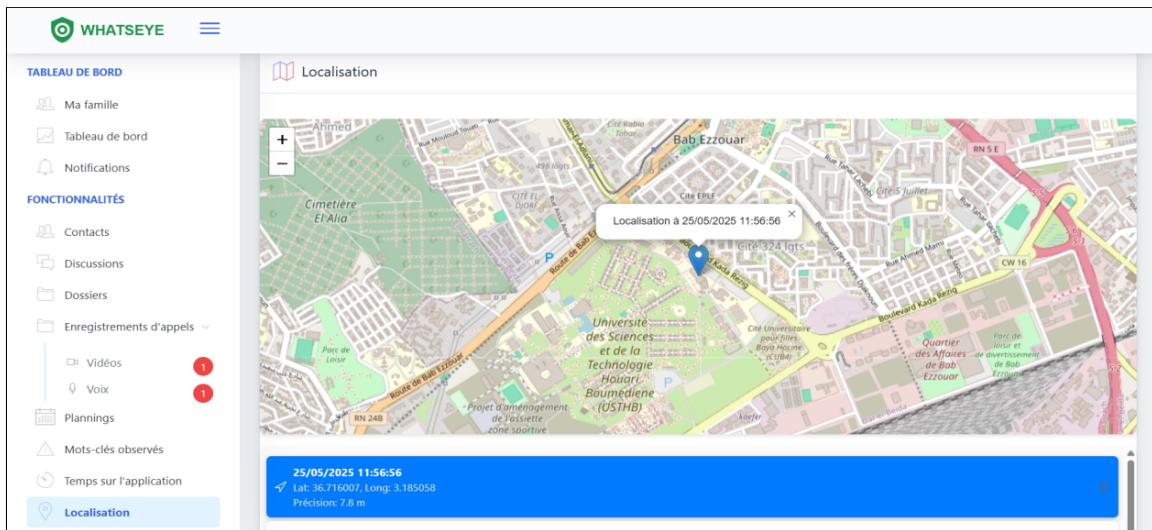


Figure B.15: Tableau de bord - Localisation

# Bibliographie

- [1] « Mobile Operating System Market Share Worldwide », StatCounter Global Stats. Consulté le : 14 février 2025. [En ligne]. Disponible sur : <https://gs.statcounter.com/os-market-share/mobile/worldwide>
- [2] B. Logerot, « De 2003 à 2023, retour sur l'histoire d'Android et comment l'OS s'est imposé dans le monde », L'Éclaireur Fnac. Consulté le : 14 février 2025. [En ligne]. Disponible sur : <https://leclaireur.fnac.com/article/336140-de-2003-a-2023-retour-sur-lhistoire-dandroid-et-comment-los-sest-imposee>
- [3] « Android history : The evolution of the biggest mobile OS in the world ». Consulté le : 14 février 2025. [En ligne]. Disponible sur : <https://www.androidauthority.com/history-android-os-name-789433/>
- [4] « Platform architecture », Android Developers. Consulté le : 14 février 2025. [En ligne]. Disponible sur : <https://developer.android.com/guide/platform>
- [5] « Kernel overview », Android Open Source Project. Consulté le : 14 février 2025. [En ligne]. Disponible sur : <https://source.android.com/docs/core/architecture/kernel>
- [6] « Hardware abstraction layer (HAL) overview », Android Open Source Project. Consulté le : 14 février 2025. [En ligne]. Disponible sur : <https://source.android.com/docs/core/architecture/hal>
- [7] « Android runtime and Dalvik », Android Open Source Project. Consulté le : 14 février 2025. [En ligne]. Disponible sur : <https://source.android.com/docs/core/runtime>
- [8] KmDev, « Exploring the Differences Between Dalvik and ART Runtimes in Android », Medium. Consulté le : 14 février 2025. [En ligne]. Disponible sur : <https://medium.com/@mkcode0323/exploring-the-differences-between-dalvik-and-art-runtimes-in-android-4d1bacfb3dc>
- [9] C. Ferry, « ART's Garbage Collector : Strategies for best performance », Medium. Consulté le : 14 février 2025. [En ligne]. Disponible sur : [https://medium.com/@c.ferry\\_11111/art-s-garbage-collector-strategies-for-best-performance-5a2a2a2a2a2a](https://medium.com/@c.ferry_11111/art-s-garbage-collector-strategies-for-best-performance-5a2a2a2a2a2a)

- ligne]. Disponible sur : <https://sonique6784.medium.com/arts-garbage-collector-strategies-for-best-performance-1f5c79208851>
- [10] « Get started with Jetpack Compose », Android Developers. Consulté le : 14 février 2025. [En ligne]. Disponible sur : <https://developer.android.com/develop/ui/compose/documentation>
- [11] « App resources overview | App architecture », Android Developers. Consulté le : 14 février 2025. [En ligne]. Disponible sur : <https://developer.android.com/guide/topics/resources/providing-resources>
- [12] « Notifications overview | Views », Android Developers. Consulté le : 14 février 2025. [En ligne]. Disponible sur : <https://developer.android.com/develop/ui/views/notifications>
- [13] « Application fundamentals | App architecture », Android Developers. Consulté le : 14 février 2025. [En ligne]. Disponible sur : <https://developer.android.com/guide/components/fundamentals>
- [14] « Content providers | App data and files », Android Developers. Consulté le : 14 février 2025. [En ligne]. Disponible sur : <https://developer.android.com/guide/topics/providers/content-providers>
- [15] « Memory allocation among processes | App quality », Android Developers. Consulté le : 14 février 2025. [En ligne]. Disponible sur : <https://developer.android.com/topic/performance/memory-management>
- [16] « Overview of memory management | App quality », Android Developers. Consulté le : 14 février 2025. [En ligne]. Disponible sur : <https://developer.android.com/topic/performance/memory-overview>
- [17] « Memory management best practices | Places SDK for Android », Google for Developers. Consulté le : 14 février 2025. [En ligne]. Disponible sur : <https://developers.google.com/maps/documentation/places/android-sdk/memory-best-practices>
- [18] S. G, « Memory Management in Android ». Consulté le : 14 février 2025. [En ligne]. Disponible sur : <https://www.robosoftin.com/blog/memory-management-in-android>
- [19] « Data and file storage overview | App data and files », Android Developers. Consulté le : 14 février 2025. [En ligne]. Disponible sur : <https://developer.android.com/training/data-storage>

- [20] Opensource.com, « What is open source ? | Opensource.com ». Consulté le : 17 février 2025. [En ligne]. Disponible sur : <https://opensource.com/resources/what-open-source>
- [21] « Licences open source : types et comparaison », Snyk. Consulté le : 14 février 2025. [En ligne]. Disponible sur : <https://snyk.io/fr/articles/open-source-licenses/>
- [22] « All About Permissive Licenses - FOSSA », Dependency Heaven. Consulté le : 14 février 2025. [En ligne]. Disponible sur : <https://fossa.com/blog/all-about-permissive-licenses/>
- [23] « All About Copyleft Licenses - FOSSA », Dependency Heaven. Consulté le : 14 février 2025. [En ligne]. Disponible sur : <https://fossa.com/blog/all-about-copyleft-licenses/>
- [24] « Contributor license agreements and headers », Android Open Source Project. Consulté le : 14 février 2025. [En ligne]. Disponible sur : <https://source.android.com/docs/setup/contribute/licenses>
- [25] « Android, AOSP, and what Open-Source Licensing means for you or your company », electrikjesus blog. Consulté le : 14 février 2025. [En ligne]. Disponible sur : <https://electrikjesus.github.io/blog/Android-AOSP-and-what-Open-Source-Licensing-means-for-you-or-your-company/>
- [26] « Android security features », Android Open Source Project. Consulté le : 14 février 2025. [En ligne]. Disponible sur : <https://source.android.com/docs/security/features>
- [27] « App signing | Android Open Source Project ». Consulté le : 19 février 2025. [En ligne]. Disponible sur : <https://source.android.com/docs/security/features/apksigning>
- [28] « Authentication | Android Open Source Project ». Consulté le : 19 février 2025. [En ligne]. Disponible sur : <https://source.android.com/docs/security/features/authentication>
- [29] « Biometrics | Android Open Source Project ». Consulté le : 19 février 2025. [En ligne]. Disponible sur : <https://source.android.com/docs/security/features/biometric>
- [30] « Encryption », Android Open Source Project. Consulté le : 19 février 2025. [En ligne]. Disponible sur : <https://source.android.com/docs/security/features/encryption>

- [31] « Hardware-backed Keystore | Android Open Source Project ». Consulté le : 19 février 2025. [En ligne]. Disponible sur : <https://source.android.com/docs/security/features/keystore>
- [32] « Security-Enhanced Linux in Android | Android Open Source Project ». Consulté le : 19 février 2025. [En ligne]. Disponible sur : <https://source.android.com/docs/security/features/selinux>
- [33] « Trusty TEE | Android Open Source Project ». Consulté le : 19 février 2025. [En ligne]. Disponible sur : <https://source.android.com/docs/security/features/trusty>
- [34] « Verified Boot | Android Open Source Project ». Consulté le : 19 février 2025. [En ligne]. Disponible sur : <https://source.android.com/docs/security/features/verifiedboot>
- [35] M. McDunnigan, « Security Risks of Androids », Chron - Small Business. Consulté le : 14 février 2025. [En ligne]. Disponible sur : <https://smallbusiness.chron.com/security-risks-androids-68511.html>
- [36] « Android Security Issues ». Consulté le : 14 février 2025. [En ligne]. Disponible sur : [https://www.cse.wustl.edu/~jain/cse571-14/ftp/android\\_security/index.html](https://www.cse.wustl.edu/~jain/cse571-14/ftp/android_security/index.html)
- [37] « The Evolution of Instant Messaging : A Comprehensive Guide - nativeMsg ». Consulté le : 16 avril 2025. [En ligne]. Disponible sur : <https://nativemsg.com/resources/text-marketing/the-evolution-of-instant-messaging-a-comprehensive-guide/>
- [38] « The Internet Relay Chat (IRC) turned 30 – and it probably changed our lives ». Consulté le : 16 avril 2025. [En ligne]. Disponible sur : <https://www.zmescience.com/science/internet-relay-chat-irc-08112018/>
- [39] « A Brief History of Chat Apps · Guide to Chat Apps ». Consulté le : 16 avril 2025. [En ligne]. Disponible sur : [https://towcenter.gitbooks.io/guide-to-chat-apps/content/introductionthe\\_dawn\\_of/a\\_brief\\_history.html](https://towcenter.gitbooks.io/guide-to-chat-apps/content/introductionthe_dawn_of/a_brief_history.html)
- [40] « Les 12 meilleurs outils de messagerie instantanée en 2024 - Freshworks ». Consulté le : 16 avril 2025. [En ligne]. Disponible sur : <https://www.freshworks.com/fr/messaging-channels/software/>
- [41] G. E. Goodwin, « What is WhatsApp? A guide to navigating the free Meta-owned communication platform », Business Insider. Consulté le : 16 avril 2025.

- [En ligne]. Disponible sur : <https://www.businessinsider.com/guides/tech/what-is-whatsapp-guide>
- [42] C. Liu, « Introduction to WeChat », MavSocial. Consulté le : 16 avril 2025. [En ligne]. Disponible sur : <https://mavsocial.com/introduction-to-wechat/>
- [43] « What is Facebook Messenger ? | dummies ». Consulté le : 16 avril 2025. [En ligne]. Disponible sur : <https://www.dummies.com/article/technology/social-media/facebook/what-is-facebook-messenger-221164/>
- [44] « What is Telegram Messenger and why should I use it? - Android Authority ». Consulté le : 16 avril 2025. [En ligne]. Disponible sur : <https://www.androidauthority.com/what-is-telegram-messenger-979357/>
- [45] « WhatsApp Statistics, Users, Demographics as of 2024 », Whats the Big Data. Consulté le : 16 avril 2025. [En ligne]. Disponible sur : <https://whatsthebigdata.com/whatsapp-statistics/>
- [46] M. Dey, « WhatsApp Statistics By Region, User Growth, Active Users And Time Spent », Electro IQ. Consulté le : 16 avril 2025. [En ligne]. Disponible sur : <https://electroiq.com/stats/whatsapp-statistics/>
- [47] « WhatsApp | History & Facts | Britannica ». Consulté le : 16 avril 2025. [En ligne]. Disponible sur : <https://www.britannica.com/topic/WhatsApp>
- [48] « Confidentialité WhatsApp | Messages sécurisés et privés », WhatsApp.com. Consulté le : 16 avril 2025. [En ligne]. Disponible sur : <https://www.whatsapp.com/privacy>
- [49] « WhatsApp », WhatsApp.com. Consulté le : 16 avril 2025. [En ligne]. Disponible sur : <https://www.whatsapp.com/community>
- [50] « Exprimez-vous | Fonctionnalités WhatsApp », WhatsApp.com. Consulté le : 16 avril 2025. [En ligne]. Disponible sur : <https://www.whatsapp.com/expressyourself>
- [51] « Gardez le contact | Des messages, des appels et plus encore sur WhatsApp », WhatsApp.com. Consulté le : 16 avril 2025. [En ligne]. Disponible sur : <https://www.whatsapp.com/stayconnected>
- [52] « Most popular messaging apps 2025 », Statista. Consulté le : 16 avril 2025. [En ligne]. Disponible sur : <https://www.statista.com/statistics/258749/most-popular-global-mobile-messenger-apps/>
- [53] « Understanding WhatsApp's Architecture & System Design ». Consulté le : 16 avril 2025. [En ligne]. Disponible sur : <https://www.cometchat.com/blog/whatsapp-architecture-and-system-design>

- [54] derek, « Scaling with DevOps Best Practices – The WhatsApp Way» PipeOps Blog ». Consulté le : 16 avril 2025. [En ligne]. Disponible sur : <https://blog.pipeops.io/how-whatsapp-scaled-its-platform-using-devops-best-practices/>
- [55] A. P. Singh, « Design a Chat Application like WhatsApp - System Design Interview ». Consulté le : 16 avril 2025. [En ligne]. Disponible sur : <https://blog.algomaster.io/p/design-a-chat-application-like-whatsapp>
- [56] R. Verma, « How WhatsApp works », Medium. Consulté le : 16 avril 2025. [En ligne]. Disponible sur : [https://medium.com/@rajendra\\_51543/how-whatsapp-works-197bfc6d6b95](https://medium.com/@rajendra_51543/how-whatsapp-works-197bfc6d6b95)
- [57] « WhatsApp Tech Stack Explored — The Tech Behind Series », Intuji. Consulté le : 16 avril 2025. [En ligne]. Disponible sur : <https://intuji.com/whatsapp-tech-stack-explored/>
- [58] « Making messaging interoperability with third parties safe for users in Europe », Engineering at Meta. Consulté le : 16 avril 2025. [En ligne]. Disponible sur : <https://engineering.fb.com/2024/03/06/security/whatsapp-messenger-messaging-interoperability-eu/>
- [59] M. Schirrmacher, « Analyzing WhatsApp Calls », Medium. Consulté le : 16 avril 2025. [En ligne]. Disponible sur : <https://medium.com/@schirrmacher/analyzing-whatsapp-calls-176a9e776213>
- [60] « Digital Forensics : Artifact Profile - WhatsApp Messenger - Magnet Forensics ». Consulté le : 16 avril 2025. [En ligne]. Disponible sur : <https://www.magnetforensics.com/blog/artifact-profile-whatsapp-messenger/>
- [61] « Where is WhatsApp Backup Stored on Android and iPhone - BOBcloud ». Consulté le : 16 avril 2025. [En ligne]. Disponible sur : <https://www.bobcloud.net/where-is-whatsapp-backup-stored/>
- [62] « How WhatsApp enables multi-device capability », Engineering at Meta. Consulté le : 16 avril 2025. [En ligne]. Disponible sur : <https://engineering.fb.com/2021/07/14/security/whatsapp-multi-device/>
- [63] « WhatsApp Data Security : End-to-End Encryption and Backups ». Consulté le : 16 avril 2025. [En ligne]. Disponible sur : <https://www.wati.io/blog/understanding-whatsapp-data-security-understand-end-to-end-encryption-and-backup>
- [64] Ashwin, « WhatsApp Privacy and Security : Tips to Keep Your Chats Safe », Wati.io. Consulté le : 16 avril 2025. [En ligne]. Disponible sur : <https://www.wati.io/blog/whatsapp-privacy-security/>

- [65] « Politique de confidentialité », WhatsApp.com. Consulté le : 16 avril 2025. [En ligne]. Disponible sur : <https://www.whatsapp.com/legal/privacy-policy>
- [66] « WhatsApp Revolutionizing Global Communication - Fansoria ». Consulté le : 16 avril 2025. [En ligne]. Disponible sur : <https://www.fansoria.com/whatsapp-revolutionizing-global-communication/>
- [67] « The Rise of WhatsApp : Stats and Story Behind Its Global Success - TimelinesAI ». Consulté le : 16 avril 2025. [En ligne]. Disponible sur : <https://timelines.ai/whatsapp-stats/>
- [68] K. Allil, S. Faisal, et A. Zia, « Why Millennials Continue to Use WhatsApp ? A Focus on Culture and Computer-Human Dialogue », Human Behavior and Emerging Technologies, vol. 2024, no 1, p. 8439194, 2024, doi : 10.1155/2024/8439194.
- [69] « Is WhatsApp Secure - Comparitech ». Consulté le : 16 avril 2025. [En ligne]. Disponible sur : <https://www.comparitech.com/blog/vpn-privacy/is-whatsapp-secure/>
- [70] « Serious doubts raised over WhatsApp's misinformation strategy – new report », Loughborough University. Consulté le : 16 avril 2025. [En ligne]. Disponible sur : <https://www.lboro.ac.uk/news-events/news/2024/february/doubts-over-whatsapp-misinformation-policy/>
- [71] K. Labs, « WhatsApp Hack : Threats, Real Cases, and Security Strategies - Keepnet », Keepnet Labs. Consulté le : 16 avril 2025. [En ligne]. Disponible sur : <https://keepnetlabs.com/blog/whats-app-hack-threats-and-protection-strategies>
- [72] A. J. Mohammed Abubakar, « 10 Best WhatsApp Alternatives You Must Try in 2025 », Beebom. Consulté le : 16 avril 2025. [En ligne]. Disponible sur : <https://beebom.com/whatsapp-alternative-apps/>
- [73] « 5 Reasons Why Parental Control Is Important In The Digital Age - Halt.org ». Consulté le : 16 avril 2025. [En ligne]. Disponible sur : <https://www.halt.org/5-reasons-why-parental-control-is-important-in-the-digital-age>
- [74] « Is WhatsApp Safe for Kids ? How Predators Find Victims on the App ». Consulté le : 16 avril 2025. [En ligne]. Disponible sur : <https://gabb.com/blog/is-whatsapp-safe-for-kids/>
- [75] C. POPOV, « What Parents Need to Know : Is WhatsApp Safe for Children ? », Hot for Security. Consulté le : 16 avril 2025. [En ligne]. Disponible sur : <https://www.bitdefender.com/en-us/blog/hotforsecurity/parents-need-know-whatsapp>

- [76] « Why you need parental control software – and 5 features to look for ». Consulté le : 16 avril 2025. [En ligne]. Disponible sur : <https://www.welivesecurity.com/2023/05/12/why-need-parental-control-software-5-features-look-for/>
- [77] « Best Parental Control App for WhatsApp 2025 : Top Guide ! - Impulsec ». Consulté le : 16 avril 2025. [En ligne]. Disponible sur : <https://impulsec.com/parental-control-software/best-parental-control-app-for-whatsapp/>
- [78] « 7 Best Parental Controls for WhatsApp in 2025 ». Consulté le : 16 avril 2025. [En ligne]. Disponible sur : <https://www.safetydetectives.com/blog/best-parental-controls-for-whatsapp/>
- [79] M. Eriksson, « 10 Best Parental Control Apps for iPhone, iOS & Android 2025 », Private Proxy Guide. Consulté le : 16 avril 2025. [En ligne]. Disponible sur : <https://www.privateproxyguide.com/best-parental-control-apps-for-iphone/>
- [80] « The Future of Parenting : How WhatsApp Tracker App Enhance Child Safety ». Consulté le : 16 avril 2025. [En ligne]. Disponible sur : <https://www.outrightcrm.com/blog/future-of-parenting-whatsapp-tracker-app/>
- [81] « A “stalkerware” app leaked phone data from thousands of victims ». Consulté le : 16 avril 2025. [En ligne]. Disponible sur : <https://techcrunch.com/2020/02/20/kidsguard-spyware-app-phones/>
- [82] « Behavior changes : Apps targeting Android 13 or higher », Android Developers. Consulté le : 17 juin 2025. [En ligne]. Disponible sur : <https://developer.android.com/about/versions/13/behavior-changes-13>
- [83] amolbh, « What is the location of WhatsApp’s encryption key file ? », r/DataHoarder. Consulté le : 17 juin 2025. [En ligne]. Disponible sur : [https://www.reddit.com/r/DataHoarder/comments/11jpf49/what\\_is\\_the\\_location\\_of\\_whatsapp\\_s\\_encryption\\_key/](https://www.reddit.com/r/DataHoarder/comments/11jpf49/what_is_the_location_of_whatsapp_s_encryption_key/)
- [84] « Restricted Settings in Android 13 and 14 ». Consulté le : 17 juin 2025. [En ligne]. Disponible sur : <https://usa.kaspersky.com/blog/android-restricted-settings/29485/>
- [85] « tesi.pdf ». Consulté le : 17 juin 2025. [En ligne]. Disponible sur : <https://webthesis.biblio.polito.it/33137/1/tesi.pdf>
- [86] « Analyse forensique de WhatsApp sur Android. Partie I : Acquisition ». Consulté le : 17 juin 2025. [En ligne]. Disponible sur : <https://belkasoft.com/android-whatsapp-acquisition>

- [87] « What is Rooting and Jailbreaking – HWG Sababa ». Consulté le : 17 juin 2025. [En ligne]. Disponible sur : <https://www.hwgsababa.com/en/what-is-rooting-and-jailbreaking/>
- [88] « Appareils rootés : définition, avantages et risques de sécurité | Okta ». Consulté le : 17 juin 2025. [En ligne]. Disponible sur : <https://www.okta.com/identity-101/rooted-device/>
- [89] « Should you root your Android device? Pros and cons | McAfee ». Consulté le : 17 juin 2025. [En ligne]. Disponible sur : <https://www.mcafee.com/learn/what-is-a-rooted-android-device/>
- [90] « What Is Rooting? Rooted Devices & Android Root Access ». Consulté le : 17 juin 2025. [En ligne]. Disponible sur : <https://www.avast.com/c-rooting-android>
- [91] jiggunjer, « Answer to “What does ‘to root a phone’ mean?” », Android Enthusiasts Stack Exchange. Consulté le : 17 juin 2025. [En ligne]. Disponible sur : <https://android.stackexchange.com/a/129384>
- [92] « Root Detection | Glossary ». Consulté le : 17 juin 2025. [En ligne]. Disponible sur : <https://docs.talsec.app/glossary/root-detection>
- [93] « Rooted Device ». Consulté le : 17 juin 2025. [En ligne]. Disponible sur : <https://zimperium.com/glossary/rooted-device>
- [94] « 3 Effective Methods to Read Encrypted WhatsApp Messages ». Consulté le : 17 juin 2025. [En ligne]. Disponible sur : <https://www.airdroid.com/parent-control/read-encrypted-whatsapp-messages/>
- [95] « À propos des fonctionnalités d'accessibilité sur WhatsApp | Pages d'aide WhatsApp ». Consulté le : 17 juin 2025. [En ligne]. Disponible sur : [https://faq.whatsapp.com/3614672068767202/?cms\\_platform=android](https://faq.whatsapp.com/3614672068767202/?cms_platform=android)
- [96] « Kotlin overview », Android Developers. Consulté le : 17 juin 2025. [En ligne]. Disponible sur : <https://developer.android.com/kotlin/overview>
- [97] « What Is Python? (Definition, Uses, Difficulty) », Built In. Consulté le : 17 juin 2025. [En ligne]. Disponible sur : <https://builtin.com/software-engineering-perspectives/python>
- [98] « What is JavaScript? - Learn web development | MDN ». Consulté le : 17 juin 2025. [En ligne]. Disponible sur : [https://developer.mozilla.org/en-US/docs/Learn\\_web\\_development/Core/Scripting/What\\_is\\_JavaScript](https://developer.mozilla.org/en-US/docs/Learn_web_development/Core/Scripting/What_is_JavaScript)
- [99] « Introduction à Django - Apprendre le développement web | MDN ». Consulté le : 17 juin 2025. [En ligne]. Disponible sur : <https://developer.mozilla.org/en-US/docs/introduction-to-Django>

[org/en-US/docs/Learn\\_web\\_development/Extensions/Server-side/Django/Introduction](https://org/en-US/docs/Learn_web_development/Extensions/Server-side/Django/Introduction)

- [100] « Canaux Django — Documentation des canaux 4.2.0 ». Consulté le : 17 juin 2025. [En ligne]. Disponible sur : <https://channels.readthedocs.io/en/latest/>
- [101] « Accueil - Framework Django REST ». Consulté le : 17 juin 2025. [En ligne]. Disponible sur : <https://www.django-rest-framework.org/>
- [102] « Introduction • Docs • Svelte ». Consulté le : 17 juin 2025. [En ligne]. Disponible sur : <https://svelte.dev/docs/kit/introduction>
- [103] « PostgreSQL : À propos ». Consulté le : 17 juin 2025. [En ligne]. Disponible sur : <https://www.postgresql.org/about/>
- [104] « What is Redis Explained ? | IBM ». Consulté le : 17 juin 2025. [En ligne]. Disponible sur : <https://www.ibm.com/think/topics/redis>
- [105] « What is Android Studio ? », GeeksforGeeks. Consulté le : 17 juin 2025. [En ligne]. Disponible sur : <https://www.geeksforgeeks.org/overview-of-android-studio/>
- [106] « What is Visual Studio Code ? Microsoft's extensible code editor », InfoWorld. Consulté le : 17 juin 2025. [En ligne]. Disponible sur : <https://www.infoworld.com/article/2335960/what-is-visual-studio-code-microsofts-extensible-code-editor.html>
- [107] « Git ». Consulté le : 17 juin 2025. [En ligne]. Disponible sur : <https://git-scm.com/>
- [108] « Google Reveals the Dessert Name Android Q Was Most Likely to Have », Gadgets 360. Consulté le : 14 février 2025. [En ligne]. Disponible sur : <https://www.gadgets360.com/mobiles/news/android-q-queen-cake-quince-tart-android-10-dessert-name-revealed-2093103>
- [109] « Improving app security and performance on Google Play for years to come », Android Developers Blog. Consulté le : 14 février 2025. [En ligne]. Disponible sur : <https://android-developers.googleblog.com/2017/12/improving-app-security-and-performance.html>
- [110] « Lucky number Android 13 : The latest features and updates », Google. Consulté le : 14 février 2025. [En ligne]. Disponible sur : <https://blog.google/products/android/android-13/>
- [111] « Android 14 : More customization, control and accessibility features », Google. Consulté le : 14 février 2025. [En ligne]. Disponible sur : <https://blog.google/products/android/android-14/>

## *BIBLIOGRAPHIE*

---

- [112] « What's new in Android 15, plus more updates », Google. Consulté le : 14 février 2025. [En ligne]. Disponible sur : <https://blog.google/products/android/android-15/>
- [113] « The First Beta of Android 16 », Android Developers Blog. Consulté le : 14 février 2025. [En ligne]. Disponible sur : <https://android-developers.googleblog.com/2025/01/first-beta-android16.html>
- [114] « Android 16 : Confirmed features, codename, leaks, release date, and everything else we know so far », Android Authority. Consulté le : 14 février 2025. [En ligne]. Disponible sur : <https://www.androidauthority.com/android-16-features-3484159/>