

Cahier des charges

Application Mobile ShadowGuard

Année universitaire 2025/2026

Table des matières

1	Introduction	2
2	Présentation du projet	3
2.1	Contexte	3
2.2	Problématique	3
2.3	Étude de l'existant	3
2.4	Limites de l'existant	3
2.5	Objectifs généraux	4
3	Spécifications fonctionnelles	4
3.1	Fonctionnalités principales	4
3.2	Fonctionnalités secondaires	5
4	Spécifications techniques	6
4.1	Architecture système	6
4.1.1	Architecture physique	6
4.1.2	Architecture logique	6
5	Spécifications non fonctionnelles	8
6	Contraintes et limites	9
6.1	Contraintes techniques	9
6.1.1	Limitations système	9
6.1.2	Contraintes de performance	9
6.2	Contraintes légales et réglementaires	9
6.2.1	RGPD	9
6.2.2	Conditions d'utilisation des stores	9
6.3	Limites de responsabilité	9
7	Annexes	10
7.1	Glossaire	10
7.2	Références et sources	10

1 Introduction

Dans un monde de plus en plus connecté, la sécurité de l'information est devenue un enjeu fondamental pour les individus, les entreprises et les institutions. Chaque jour, des milliards de données personnelles — identités, messages, positions géographiques, habitudes de navigation — sont collectées, stockées et exploitées par des applications mobiles, souvent à l'insu des utilisateurs. Cette exploitation massive et parfois non encadrée soulève de sérieux problèmes en matière de confidentialité, d'intégrité et de disponibilité des informations, trois piliers essentiels de la sécurité informatique (modèle CIA : Confidentiality, Integrity, Availability).

Pour répondre à ces enjeux, plusieurs normes internationales et bonnes pratiques ont été mises en place afin d'assurer une gestion rigoureuse de la sécurité de l'information :

- ❖ **ISO/IEC 27001** : norme de référence pour la mise en œuvre d'un Système de Management de la Sécurité de l'Information (SMSI).
- ❖ **RGPD (Règlement Général sur la Protection des Données)** : cadre légal européen garantissant la protection et le traitement transparent des données personnelles.
- ❖ **OWASP Mobile Security Project** : ensemble de recommandations pour sécuriser les applications mobiles contre les vulnérabilités courantes.
- ❖ **ISO/IEC 27005** : norme spécialisée dans la gestion des risques liés à la sécurité de l'information.

Malgré ces standards, la majorité des utilisateurs de smartphones ne disposent ni des connaissances ni des outils nécessaires pour évaluer les risques liés à leurs propres applications. De nombreuses apps accèdent à des informations sensibles (micro, caméra, position GPS, fichiers personnels) sans justification explicite, exposant les utilisateurs à des risques de surveillance numérique, de profilage publicitaire ou encore de fuite de données.

C'est dans ce contexte que s'inscrit le projet ShadowGuard, une solution innovante qui vise à renforcer la protection des données personnelles sur mobile. En combinant intelligence artificielle, analyse comportementale et visualisation pédagogique, ShadowGuard permet à chaque utilisateur de comprendre, contrôler et limiter la collecte non autorisée de ses informations personnelles. Le projet s'inscrit ainsi dans une démarche conforme aux principes de sécurité et de conformité internationale, tout en rendant la cybersécurité accessible, éducative et proactive.

2 Présentation du projet

2.1 Contexte

Dans un contexte où les violations de la vie privée et la collecte non transparente de données personnelles se multiplient, les utilisateurs manquent souvent d'outils leur permettant de comprendre, analyser et contrôler les autorisations accordées à leurs applications.

ShadowGuard répond à ce besoin en proposant une application mobile capable de détecter les risques liés à la confidentialité, analyser le comportement des applications installées, et protéger les données personnelles de l'utilisateur grâce à une approche basée sur l'intelligence artificielle et la surveillance comportementale.

2.2 Problématique

Avec l'accélération de la transformation numérique, la sécurité des données personnelles est devenue un enjeu majeur. Les utilisateurs installent de nombreuses applications sans réellement savoir quelles informations sont collectées ni comment elles sont utilisées. Les outils de sécurité existants (antivirus, pare-feux, etc.) restent souvent complexes, réactifs et peu adaptés au grand public.

Le projet ShadowGuard vise à répondre à ce besoin en proposant une application mobile intelligente capable de détecter, analyser et bloquer les collectes de données non autorisées, tout en sensibilisant les utilisateurs à la protection de leur vie privée.

2.3 Étude de l'existant

Actuellement, plusieurs solutions de cybersécurité existent sur le marché :

- ❖ **Antivirus et pare-feux** : (ex. : Avast, Kaspersky, Bitdefender) qui se concentrent sur la détection de virus et malwares, mais sans visibilité claire sur les données collectées par les applications.
- ❖ **Applications de confidentialité** : comme DuckDuckGo Privacy Essentials ou Jumbo Privacy, qui analysent certaines permissions, mais n'offrent pas de suivi en temps réel ni de visualisation complète des flux de données.
- ❖ **Outils développeurs** : (OWASP, AppCensus) orientés vers les professionnels de la sécurité, souvent difficiles à comprendre pour un utilisateur non technique.

2.4 Limites de l'existant

- ❖ Les solutions actuelles sont fragmentées : aucune ne combine détection, analyse et pédagogie dans une seule application.
- ❖ La plupart sont réactives (elles agissent après l'attaque, non avant).
- ❖ Les outils existants nécessitent des connaissances techniques pour être utilisés efficacement.
- ❖ Le manque de transparence sur l'utilisation réelle des données reste un problème majeur.

- ❖ Peu d'applications respectent à la fois les normes de cybersécurité (ISO 27001, OWASP) et les réglementations de protection des données (RGPD) tout en restant accessibles au grand public.

2.5 Objectifs généraux

Le projet ShadowGuard vise à :

- ❖ Développer une application mobile intuitive et sécurisée pour Android et iOS
- ❖ Fournir une analyse prédictive des risques avant l'installation d'une application
- ❖ Surveiller en temps réel les comportements suspects d'applications existantes
- ❖ Sensibiliser les utilisateurs à la cybersécurité et à la protection des données

3 Spécifications fonctionnelles

3.1 Fonctionnalités principales

N°	Fonctionnalité	Description
F1	Analyse prédictive	Évaluer le risque d'une application avant son installation via un score de confidentialité généré par IA. L'analyse doit inclure : permissions demandées, réputation du développeur, historique de mises à jour, avis utilisateurs analysés par NLP.
F2	Surveillance en temps réel	Surveiller les comportements anormaux des applications installées (accès aux capteurs, aux fichiers, connexions réseau suspectes). Le système doit détecter : accès caméra/micro en arrière-plan, géolocalisation excessive, lecture de contacts, tentatives de connexion à des serveurs suspects.
F3	Shadow Profile	Reconstituer le profil publicitaire de l'utilisateur à partir des données collectées par les applications. Afficher : types de données collectées, applications collectrices, estimation de la valeur des données, trackers détectés.
F4	Scanner local	Analyser les applications déjà installées et les classer selon leur niveau de risque (Faible/Moyen/Élevé/Critique). Pour chaque application : permissions utilisées, comportements détectés, recommandations d'action.
F5	Centre de sécurité	Tableau de bord présentant le score global de confidentialité (0-100), l'historique des alertes et les recommandations. Vue d'ensemble : nombre d'apps à risque, dernières alertes, évolution du score, actions recommandées.

N°	Fonctionnalité	Description
F6	Alerte de sécurité	Notification en cas de détection d'un comportement suspect. Types d'alertes : critique (rouge), importante (orange), informative (jaune). L'utilisateur peut : voir les détails, bloquer l'application, marquer comme faux positif.
F7	Historique et statistiques	Visualiser les analyses précédentes et l'évolution du score de sécurité dans le temps. Graphiques : évolution du score, nombre d'alertes par période, applications les plus surveillées, statistiques de collecte de données.

3.2 Fonctionnalités secondaires

N°	Fonctionnalité	Description
F8	Mode apprentissage	Fournir des conseils et bonnes pratiques sur la sécurité numérique. Contenu : tutoriels interactifs, quiz de sensibilisation, actualités cybersécurité, guides de configuration.
F9	Mode sombre/clair	Offrir un choix de thème visuel adapté aux préférences de l'utilisateur. Basculement automatique selon l'heure ou manuel.
F10	Comparateur d'applications	Permettre à l'utilisateur de comparer le niveau de risque de plusieurs applications similaires (ex : comparer 3 applications de messagerie). Critères de comparaison : score de sécurité, permissions, données collectées, réputation.
F11	Rapport exportable	Générer un rapport PDF détaillé de l'état de sécurité du téléphone pour consultation ou partage.
F12	Paramètres de confidentialité	Permettre à l'utilisateur de configurer : fréquence des scans, sensibilité des alertes, données à surveiller en priorité.

4 Spécifications techniques

4.1 Architecture système

4.1.1 Architecture physique

L'architecture physique de ShadowGuard repose sur une infrastructure client-serveur distribuée. Elle comprend deux applications clientes mobiles (Android développée en Kotlin et iOS en Swift), connectées à un serveur central NestJS via une API REST sécurisée par le protocole HTTPS. Le backend communique avec une base de données MongoDB pour le stockage des informations et un cache Redis pour la gestion des sessions et l'optimisation des performances. Un module d'intelligence artificielle intégré au backend est chargé d'analyser les comportements des applications installées et de détecter les activités suspectes.

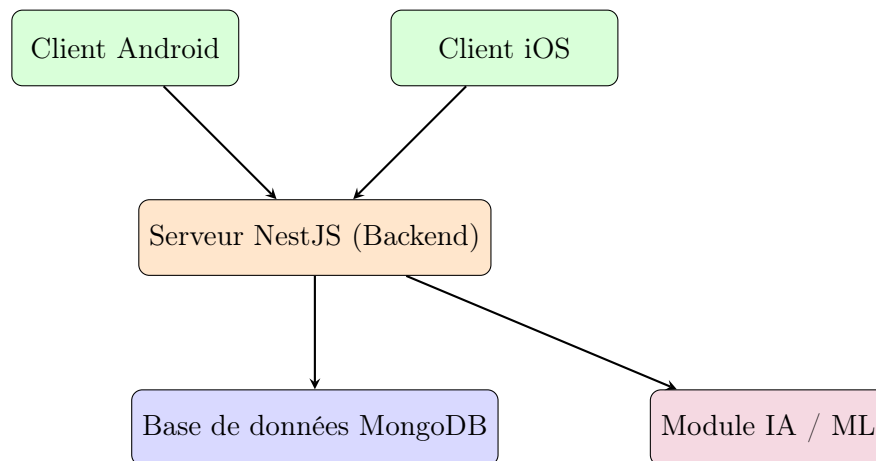


FIGURE 1 – Schéma de l'architecture physique de ShadowGuard

4.1.2 Architecture logique

L'architecture logique de ShadowGuard est organisée selon trois couches principales :

- ❖ **Couche présentation** : composée des applications mobiles Android et iOS, elle gère l'interface utilisateur, la saisie des données et la visualisation des alertes.
- ❖ **Couche logique métier** : hébergée dans le backend NestJS, elle traite les requêtes, applique les règles de sécurité et orchestre les modules d'analyse.
- ❖ **Couche données** : comprend la base MongoDB pour le stockage des informations et Redis pour la mise en cache rapide.

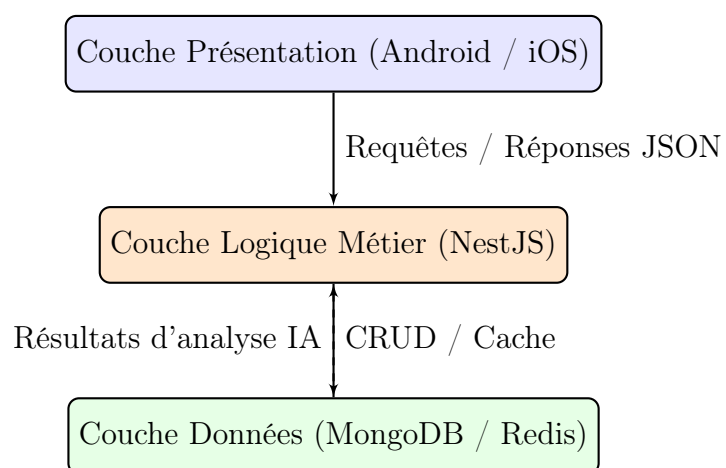


FIGURE 2 – Schéma de l'architecture logique de ShadowGuard

5 Spécifications non fonctionnelles

Les spécifications non fonctionnelles de **ShadowGuard** définissent les critères de qualité, de performance et de sécurité nécessaires pour garantir la fiabilité et la durabilité du système.

❖ Performance

- ◇ Temps de réponse de l'application inférieur à 3 secondes.
- ◇ Analyse de sécurité terminée en moins de 30 secondes pour un lot standard.
- ◇ Consommation mémoire inférieure à 150 MB et impact batterie $< 5\%$.

❖ Sécurité et confidentialité

- ◇ Données chiffrées (AES-256, HTTPS, JWT).
- ◇ Conformité avec les normes **ISO 27001**, **OWASP MASVS niveau 2** et **RGPD**.
- ◇ Implémentation du principe *Privacy by Design* (collecte minimale et consentement explicite).

❖ Disponibilité et fiabilité

- ◇ Disponibilité du service : 99%.
- ◇ Temps de récupération après panne < 1 heure.
- ◇ Gestion automatique des erreurs et reprise après échec.

❖ Compatibilité

- ◇ Fonctionnement sur Android 10 et iOS 14.
- ◇ Support des tablettes Android et iPad.
- ◇ Interface multilingue (Français, Anglais) avec prise en charge i18n.

❖ Scalabilité et maintenance

- ◇ Architecture NestJS modulaire et scalable (jusqu'à 10 000 utilisateurs simultanés).
- ◇ Base de données MongoDB optimisée (index, partitionnement).
- ◇ Code structuré selon les principes **SOLID**.
- ◇ Documentation complète (technique et utilisateur).
- ◇ Couverture de tests $> 80\%$.

❖ Ergonomie et accessibilité

- ◇ Interface simple et intuitive (Material Design et Human Interface Guidelines).
- ◇ Support des lecteurs d'écran et contrastes adaptés.
- ◇ Taille de police ajustable.

6 Contraintes et limites

6.1 Contraintes techniques

6.1.1 Limitations système

- ❖ **Android** : Restrictions sur l'accès aux logs système à partir d'Android 11
- ❖ **iOS** : Limitations strictes sur la surveillance en arrière-plan
- ❖ **Permissions** : Nécessité d'autorisations spéciales (Accessibility Service, Usage Stats)
- ❖ **Batterie** : Surveillance continue limitée pour préserver l'autonomie

6.1.2 Contraintes de performance

- ❖ Analyse en temps réel sans impact sur les performances du téléphone
- ❖ Limitations mémoire sur les appareils bas de gamme
- ❖ Bande passante limitée pour les utilisateurs en données mobiles

6.2 Contraintes légales et réglementaires

6.2.1 RGPD

- ❖ Consentement explicite pour la collecte de données
- ❖ Droit à l'oubli : suppression complète des données sur demande
- ❖ Portabilité des données
- ❖ Notification en cas de violation de données (72h)
- ❖ Désignation d'un DPO si nécessaire

6.2.2 Conditions d'utilisation des stores

- ❖ Respect des guidelines Google Play et App Store
- ❖ Interdiction de collecter des données sans consentement
- ❖ Transparence totale sur les fonctionnalités
- ❖ Politique de confidentialité obligatoire

6.3 Limites de responsabilité

- ❖ L'application fournit des **indicateurs** de risque, pas des garanties absolues
- ❖ Aucune responsabilité en cas de faux négatifs (application malveillante non détectée)
- ❖ Les recommandations sont basées sur des analyses automatisées (IA) et peuvent contenir des erreurs
- ❖ L'utilisateur reste responsable de ses choix d'installation/désinstallation

7 Annexes

7.1 Glossaire

API Application Programming Interface - Interface de programmation applicative

Backend Partie serveur d'une application

Frontend Partie client d'une application (interface utilisateur)

JWT JSON Web Token - Système d'authentification par token

Machine Learning (ML) Apprentissage automatique

NestJS Framework Node.js pour le développement backend

NLP Natural Language Processing - Traitement du langage naturel

RGPD Règlement Général sur la Protection des Données

REST Representational State Transfer - Architecture d'API

SDK Software Development Kit - Kit de développement logiciel

Shadow Profile Profil publicitaire reconstitué à partir des données collectées

Tracker Outil de suivi et collecte de données utilisateur

UAT User Acceptance Testing - Tests d'acceptation utilisateur

UX/UI User Experience / User Interface - Expérience et interface utilisateur

Web Scraping Extraction automatisée de données depuis des sites web

7.2 Références et sources

- RGPD - Règlement (UE) 2016/679
- OWASP Mobile Security Testing Guide (MSTG)
- ISO/IEC 27001 - Sécurité de l'information
- Google Play Store Developer Policy
- Apple App Store Review Guidelines
- Android Developers Documentation
- iOS Developer Guidelines