الجمـهورية الجزائرية الديمقراطية الشعبيـة
وزارة التعليم العالي والبحث العلمي

جـامعـة سعـيـدة د. مـولاي الطـاهـر
كلية الرياضيات و الإعلام الآلي و الاتصالات
السلكية و اللاسلكية
قسم: الإعلام الآلي

Mémoire de Master en informatique

Spécialité : Réseaux Informatique et Systèmes Répartis

Thème

RANI MAAK : Système d'assistance sécurisé pour la localisation des patients atteints d'Alzheimer via des QR codes chiffrés et la géolocalisation mobile

▪ **Présenté par :**

Labani Faten Hadil
Djelouli Nour El Houda

▪ **Dirigé par :**

Benyahia Kadda

Année universitaire 2024-2025

Remerciements

Au terme de ce modeste travail, nous souhaitons exprimer nos plus sincères remerciements. Tout d'abord, nous rendons grâce à Dieu, source de force et de persévérance tout au long de ce parcours.

Nous tenons à adresser notre profonde gratitude à **Dr Benyahia Kadda** pour la qualité de son encadrement, sa disponibilité, ses conseils éclairés, ainsi que pour l'attention et la bienveillance qu'il nous a accordées. Ses orientations ont largement contribué à la réalisation de ce projet dans les meilleures conditions.

Nos remerciements vont également à **Dr. Benyahia Miloud**, pour son soutien ,son accompagnement pédagogique et ses remarques pertinentes qui ont enrichi

Notre réflexion et favorisé l'aboutissement de ce travail.

Nos remerciements s'adressent également aux membres du jury, que nous remercions chaleureusement pour avoir accepté d'évaluer notre travail.

Enfin, nous exprimons toute notre reconnaissance à nos familles, et tout particulièrement à nos parents, pour leur soutien inconditionnel, leur patience et leurs sacrifices constants. Leur présence à nos côtés a été essentielle à notre réussite, et nous leur devons une grande part de ce chemin accompli.

Dédicaces

*Je dédie ce projet de fin d'études à **ma mère**, celle qui a toujours été ma plus grande source de soutien et d'inspiration. Tes encouragements constants, ton amour inconditionnel et tes sacrifices ont été les piliers de ma réussite académique.*
*À **ma mère**, à **mon père**, à **ma sœur Ahlem**, ainsi qu'à **mes frères Mohammed et Ilyas**, je vous adresse ces mots empreints de reconnaissance et d'affection. Votre présence indéfectible et votre soutien constant ont été essentiels tout au long de ma vie.*

***Maman**, tu es le roc sur lequel je me suis appuyée avec gratitude et admiration.*
***Papa**, ta sagesse, ta patience et ta confiance en moi ont été un véritable guide. Merci pour ton soutien discret mais précieux, et pour les valeurs que tu m'as transmises.*
***Ahlem**, ma sœur chérie, ta bienveillance et ton amour inébranlable ont illuminé mes journées.*
***Mohammed et Ilyas**, mes frères adorés, votre soutien fidèle a été une source de force et de motivation.*

Je suis profondément fière d'avoir des êtres aussi exceptionnels que vous dans ma vie.
Cette dédicace est le témoignage de toute ma gratitude et de tout mon amour pour vous.
Merci d'être les piliers de ma vie.

Faten Hadil

En ce moment si spécial de ma vie, je tiens à dédier ce travail et cette réussite aux personnes qui ont été ma source de force, d'amour et d'inspiration.
*À **ma mère bien-aimée**, celle dont les prières silencieuses m'ont accompagné à chaque étape, celle dont le regard plein de tendresse suffisait à apaiser mes peines. Merci pour ton amour inconditionnel, pour tes sacrifices innombrables, pour ta patience et ton soutien constant. Tu es la lumière de ma vie, et sans toi, je n'aurais jamais trouvé la force d'aller aussi loin.*
*À **mon père Mohamed**, exemple de sagesse, de courage et de persévérance. Merci pour ta confiance, tes conseils et ton appui discret mais toujours présent. Tu m'as appris à ne jamais baisser les bras et à croire en mes capacités.*
*À **mes frères, Abdo et Youssef**, mes compagnons de vie et de cœur. Merci pour votre présence rassurante, pour vos mots simples mais sincères, pour chaque geste d'encouragement, chaque sourire offert au bon moment. Vous avez été pour moi une source de bonheur et de motivation.*

Ce diplôme, ce n'est pas seulement l'aboutissement d'années d'efforts personnels, c'est aussi le reflet de votre amour, de votre patience et de votre confiance en moi.
*À vous, **ma famille**, je dédie cette réussite avec tout mon amour et toute ma reconnaissance.*
Que cette étape soit un hommage à tout ce que vous êtes pour moi.

Nour El Houda

TABLE DES MATIERES

Liste des figures

Liste des Symboles & Abréviations

RANI MAAK : Nom du projet d'application mobile développé.
Signifie « Je suis avec toi » en arabe dialectal. Il s'agit d'une solution de sécurité personnelle permettant l'envoi d'alertes sécurisées par QR code, SMS et géo localisation.

RGPD : Règlement Général sur la Protection des Données (Réglementation européenne)**.**

HIPAA : Health Insurance Portability and Accountability Act (Réglementation américaine).

ICE : In Case of Emergency
C'est une carte médicale .

RSA : Rivest-Shamir-Adleman (algorithme de chiffrement asymétrique).

AES : Advanced Encryption Standard
Algorithme de chiffrement symétrique utilisé pour sécuriser les données dans ce projet.

API : Application Programming Interface
Interface permettant l'interaction entre le client (application mobile) et le serveur.

JSON : JavaScript Object Notation
Format de données léger et facile à utiliser pour l'échange de données, notamment pour l'historique des alertes.

PHP : Hypertext Preprocessor
Langage de script côté serveur utilisé pour la gestion des données (QR code, patient, alertes).

QR Code : Quick Response Code
Code-barres bidimensionnel utilisé pour contenir des informations sécurisées.

SMS : Short Message Service
Service permettant l'envoi de messages textes via des téléphones mobiles.

XAMPP : Cross-Platform, Apache, MySQL, PHP, and Perl
Ensemble de logiciels permettant de configurer un serveur local pour le développement.

MySQL : My Structured Query Language
Système de gestion de base de données utilisé pour stocker et gérer les données des patients et alertes.

GPS : Global Positioning System
Système de géo localisation par satellite permettant de déterminer la position géographique de l'utilisateur avec une grande précision. Dans ton projet, le GPS est utilisé pour récupérer la localisation de l'utilisateur afin d'inclure cette information dans les alertes envoyées.

IDE : Integrated Development Environment
Environnement de développement intégré. Un IDE est un logiciel qui fournit un ensemble d'outils nécessaires à la programmation, tels que des éditeurs de code, des outils de débogage, et des gestionnaires de projets. Dans ton projet, des IDE comme Android Studio (pour le développement Androïde) et Visual Studio (pour le développement du site web) sont utilisés pour écrire, tester et

déployer les applications et les scripts.

CBC : Cipher Block Chaining
Mode de chiffrement utilisé avec AES. Chaque bloc de données est chiffré après avoir été combiné avec le bloc précédent, augmentant la sécurité du chiffrement.

GSM : Global System for Mobile Communications
norme de communication mobile utilisée pour la transmission de la voix et des données. Dans ce projet, il permet de localiser approximativement un utilisateur via la triangulation des antennes relais.

Wi-Fi : Wireless Fidelity
technologie de réseau sans fil utilisée principalement pour la connexion Internet en intérieur. Elle permet aussi la géolocalisation dans des bâtiments disposant de plusieurs points d'accès.

INTRODUCTION GENERALE

I. INTRODUCTION GENERALE

La sécurité des données de santé est de nos jours, un enjeu central dans nos sociétés numériques, car les données de santé sont les données les plus sensibles, les fuites de celles-ci ayant des conséquences graves (atteinte à la vie privée, discriminations, utilisations malveillantes, etc.). C'est pourquoi il existe des réglementations strictes comme le Règlement général sur la protection des données (RGPD) en Europe ou le Health Insurance Portability and Accountability Act (HIPAA) aux États-Unis, qui instaurent des obligations fortes en matière de protection de la confidentialité, de l'intégrité et de la traçabilité des données personnelles de santé [1][2].

A cette problématique de sécurité des données, il faut ajouter celle, indissociablement liée, de la prise en charge de situations d'urgence familiale et des institutions médicales que constituent la perte, l'oubli de personnes vulnérables ; en particulier des personnes âgées, en situation de Alzheimer ou d'un trouble du comportement. Ces situations inattendues, qui peuvent advenir à tout instant, exigent une réponse rapide afin de préserver la sécurité de la personne concernée ; en l'occurrence d'un accompagnement médical. Le facteur temps est alors un vecteur essentiel de la sécurité de la victime, dans la mesure où le délai d'intervention permet d'assurer sa sauvegarde [3].

Face à ce double enjeu – la protection des données sensibles et la sécurité physique des patients – il apparaît nécessaire d'articuler un dispositif de sécurité et de protection des personnes – alerte, très réactive, fiable et respectueuse des données personnelles. C'est dans cette optique que s'inscrit le projet en cours permettant d'associer, solidarité familiale et technique, au moyen d'un système de chiffrement de données, d'un système d'identification par QR code et d'un système de géo localisation d'urgence. Le but principal de ce dispositif est d'assurer la sauvegarde des informations à caractère personnel et médical des patients à l'aide de techniques de cryptographie modernes, à l'instar de l'algorithme AES (Advanced Encryptions Standard) d'une robustesse et d'une rapidité largement reconnues dans les systèmes sécurisés [4]. De plus, il s'agit de donner la possibilité d'une identification immédiate et fiable grâce à un QR code unique attribué à chaque patient. Le QR code scanné par un tiers enclenche alors le processus d'alerte consistant à rechercher l'identité du patient, sa position géographique grâce au GPS, puis à envoyer par SMS un message d'alerte à un proche ou à un personnel médical.
Ce système utilise principalement deux plateformes : une application mobile Androïde et une interface web. L'application mobile permet le scan du QR code, le déchiffrement local des données, la récupération de la position GPS, et l'envoi des alertes. L'interface web permet de gérer les patients, de consulter les alertes enregistrées et de suivre les événements en temps réel. La base de données centralisée assure le stockage sécurisé de toutes les informations indispensables au fonctionnement du système.

En agençant avec soin des technologies de pointe dans les domaines de la sécurité par chiffrement des données, de la géo localisation active et de la communication mobile, ce projet de recherche apporte une réponse originale à une problématique humaine et sociale de premier plan : protéger le public vulnérable dans le respect de sa vie privée.

Chapitre1. État de l’art

Chapitre 1

État de l'art

I.1 Sécurité des données médicales

La sécurisation des données médicales doit être une priorité pour les systèmes d'information de santé, car elles constituent une information très sensible, telle que l'identité des patients, leurs antécédents médicaux, les diagnostics, les traitements, et si elles sont divulguées illicitement, cela peut porter gravement atteinte à la vie privée, entraîner des discriminations, voire permettre des fraudes [5] .

Pour répondre à ces enjeux, plusieurs cadres juridiques ont été développés dans différentes régions du monde. En Europe, le Règlement Général sur la Protection des Données (RGPD) impose des exigences en matière de consentement, de minimisation des données, et de sécurité technique, extrêmement précises [6] ; tandis qu'aux États-Unis, la loi HIPAA (Health Insurance Portability and Accountability Act) énonce des standards de protection des informations de santé, et impose des mesures organisationnelles au niveau de la traçabilité, l'accès physique, et du chiffrement [7] .

Figure 1 : Les 4 étapes essentielles du RGPD appliquées aux données de santé. [8]

La Figure 1 présente les quatre étapes incontournables pour être en conformité avec le Règlement Général sur la Protection des Données (RGPD), adapté depuis mai 2018 au niveau de l'Union européenne. Rappelons en effet que ce règlement a pour but de renforcer la protection des données personnelles et de placer la responsabilité sur toute entité traitant de telles données, ce qui est aussi le cas de l'ensemble du secteur de la santé.

1. Le registre des traitements

Le RGPD impose à tout responsable de traitement de tenir un registre des traitements effectués, en indiquant : finalités, catégories de données, durées de conservation et mesures de sécurité (article 30 du RGPD) [9] .

-Objectif : Assurer traçabilité et transparence des traitements.

2. Le tri des données

Le principe de minimisation des données (article 5.1.c) exige de ne collecter que les données strictement nécessaires à la finalité du traitement [10] . Cela implique un audit pour faire disparaître les données obsolètes, non pertinentes ou non collectées sur une base légale.
-Objectif : Réduire les risques liés à des volumes d données sensibles très importants.

3. Conserve les droits des personnes

Le RGPD donne plus de droits aux personnes : droits d'accès, de rectification, d'opposition, d'effacement (droit à l'oubli), à la portabilité (articles 12 à 23) [9] . Il faut donc mettre en œuvre des procédures pour répondre aux demandes dans les délais réglementaires.
-Objectif : Renforcer le contrôle des personnes sur leurs données.

4. Sécuriser les données

L'article 32 du RGPD impose de mettre en œuvre des mesures techniques et organisationnelles adéquates : chiffrement, anonymisation, gestion des accès, journalisation des actions, etc. pour garantir la confidentialité, l'intégrité et la disponibilité [11] .
-Objectif : Protéger les données de tout accès, toute modification, toute perte non autorisée.

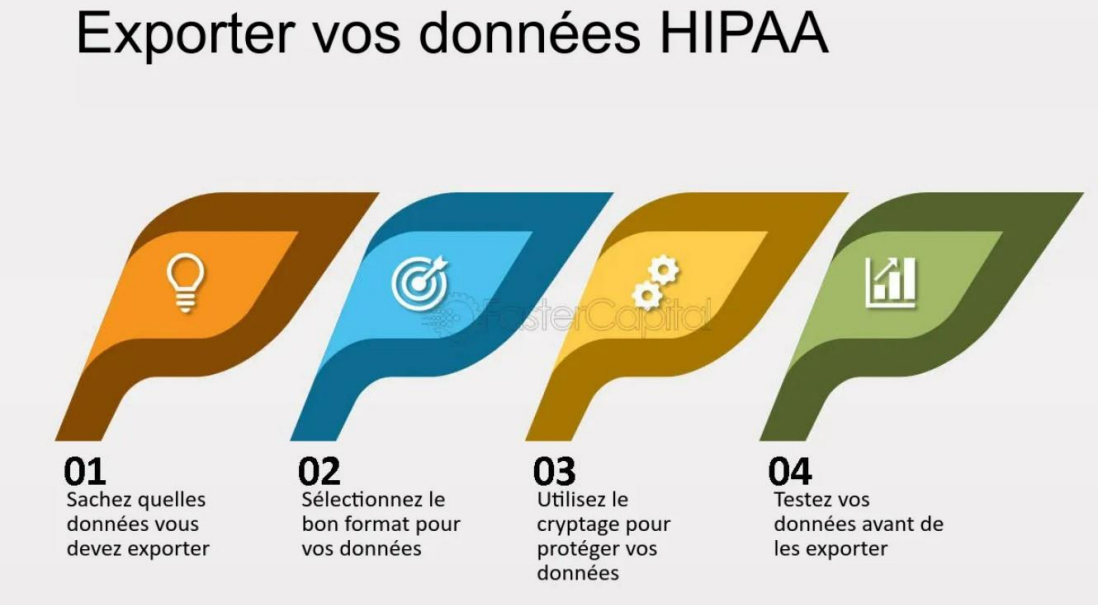


Figure 2 : Étapes pour une exportation sécurisée des données de santé selon la norme HIPAA. [12]

La Figure 2 propose les bonnes pratiques pour le transfert des données de santé dans le respect de la loi américaine HIPAA (Health Insurance Portability and Accountability Act), sur le territoire des États-Unis. L'installation de quatre étapes-clés permettrait de garantir la sécurité des données sensibles :

1) Identification des données à transférer : il s'agit de ne transférer que les seules données nécessaires (dans une optique de minimisation), conformément aux recommandations de

l'HIPAA et du RGPD en Europe [13] , permettant de réduire les risques en cas de viralisation des données.

2) Choix du format adéquat : il convient d'avoir recours à des formats normalisés (comme JSON, XML ou HL7/FHIR) garantissant l'interopérabilité entre systèmes mais aussi, facilitant leur intégration dans des environnements sécurisés [14] .

3) Utilisation d'un chiffrement : le chiffrement (ou cryptage) des données en transit (en se fondant sur : AES-256, TLS 1.3), est un passage obligé pour éviter la fuite des données si elles devaient être interceptées [15] . La loi HIPAA impose l'utilisation du chiffrement comme modalité technique de sécurité excluant l'éventualité qu'elles circulent en « clair », lorsqu'elles transitent électroniquement.

4) Contrôle et test des données : et avant un transfert, il est recommandé de valider la conformité des données, d'effectuer une simulation du transfert dans une instance typique pour éviter les vices d'erreurs ou la fuite des données [16] .

I.2 Méthodes de chiffrement utilisées en santé

Le chiffrement constitue un élément essentiel pour garantir la confidentialité des données. Par exemple, dans le secteur de la santé, les dispositifs de chiffrement symétrique (tels que AES) et asymétrique (comme RSA) sont les plus utilisés. En revanche, le chiffrement symétrique est souvent de rigueur dans les transmissions rapides déjà évoquées, telles que par exemple les applications mobiles [17] ou les systèmes embarqués.

D'autres solutions font aussi souvent appel à des techniques de pseudonymisation et d'anonymisation, comme par exemple dans les projets de recherche clinique. Or, seule la cryptographie permet de garantir que les données ne puissent être lues qu'avec la clé correspondante, garantissant alors vraiment leur confidentialité.

Caractéristique	Chiffrement symétrique (ex : AES)	Chiffrement asymétrique (ex : RSA)
Nombre de clés	Une seule clé (même pour le chiffrement et le déchiffrement)	Deux clés : publique et privée
Vitesse d'exécution	Très rapide	Plus lent
Utilisation principale	Chiffrement local ou embarqué (applications, QR codes)	Transmission sécurisée de clés, signature numérique
Complexités	Chiffrement local ou embarqué (applications, QR codes)	Transmission sécurisée de clés, signature numérique
Exemples en santé	Dossier médical dans mobile, QR code chiffré	Transmission sécurisée entre hôpitaux ou laboratoires
Inconvénients	Besoin de transmettre la clé secrète de façon sécurisée	Plus lent, difficile à utiliser pour les grandes quantités

Figure 3 : Comparaison entre chiffrement symétrique et asymétrique dans le domaine de la santé.

Cette figure précise le large écart, les différences fondamentales qui s'opposent entre deux niveaux de cryptage utilisés pour la sécurité des données, notamment les données en santé, d'une part.

- Le cryptage dit de type symétrique, de type AES, utilise une clé partagée unique entre l'émetteur et le récepteur. Il est reconnu rapide, léger et adapté aux environnements contraints (QR codes embarqués sur les cartes patients, applications mobiles [18]) mais pose le défi, en revanche, d'assurer la mise en sécurité de la transmission de la clé partagée.
- Le cryptage dit de type asymétrique, de type RSA, utilise une paire de clés (publique/privée), permettant des échanges sécurisés, sans avoir partagé un secret a priori. Il est alors mieux approprié pour des échanges entre des entités éloignées, comme hôpitaux ou laboratoires [19] . Cependant, cela le rend plus lourd, voire inapproprié pour un cryptage de données massives ou en temps réel.

C'est pourquoi notre projet a retenu le cryptage symétrique AES, garant de la confidentialité des données intégrées dans les QR codes sans nuire à la performance et à l'intégration au sein d'une application mobile légère, comme celle réalisée dans le projet RANI MAAK.

I.3 Cryptographie symétrique et AES

I.3.1 Principe du chiffrement AES

L'algorithme de chiffrement symétrique AES (Advanced Encryption Standard) est un standard publié par le NIST en 2001, qui chiffre des blocs de 128 bits selon trois tailles de clés possibles : 128, 192 ou 256 bits. Le fonctionnement de l'AES repose sur un réseau de substitution-permutation constitué de plusieurs étapes répétées (ou rounds) : substitutions, permutations, mélange des colonnes, ajout de clé [20] .

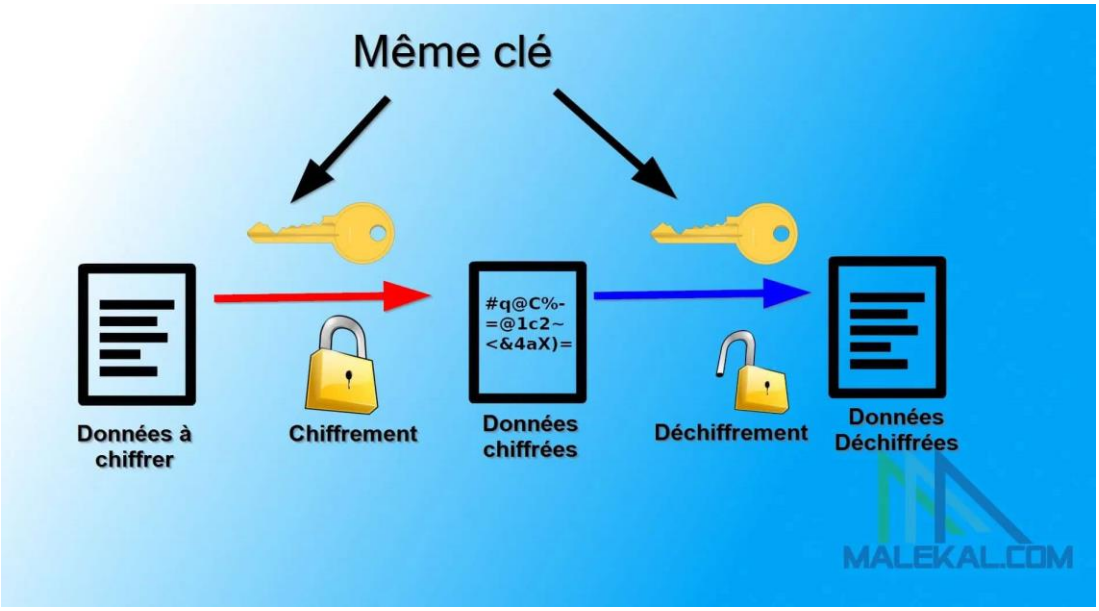


Figure 4 : Fonctionnement interne de l'algorithme AES (128 bits). [21]

L'illustration ci-dessus représente le processus de chiffrement et déchiffrement symétriques à l'aide d'une même clé, comme pour l'AES. Les données en clair (à gauche), sont chiffrées à l'aide de la clé secrète partagée. La clé utilisée pour le chiffrement est également utilisée pour déchiffrer à l'arrivée. Ce mode de fonctionnement rapide et performant est souvent choisi dans les applications de santé mobile et les dispositifs embarqués, où la vitesse d'exécution est primordiale.

I.3.2 Avantages et limites

Les bénéfices de l'AES sont multiples : il est à la fois rapide, sécurisé, peu consommateur de ressources, facile à mettre en œuvre et largement éprouvé ; et sans doute un des algorithmes les plus sûrs pour le chiffrement de données sensibles.
Cependant, sa principale faiblesse réside dans la gestion des clés. Une clé exposée entraîne celle de toutes les données chiffrées. Effectivement, il est impératif d'employer des méthodes robustes de stockage et de distribution sécurisée des clés [22] .

I.4 Utilisation des QR codes en santé

I.4.1 Codage des données sensibles dans les QR codes

Le code QR (ou code à réponse rapide) est un format d'encodage bidimensionnel permettant l'enregistrement d'une quantité d'informations relativement importante (au maximum environ 3 000 caractères alphanumériques) dans un format rapidement lisible par un Smartphone ou tout terminal compatible. Développée initialement pour l'industrie automobile japonaise, son utilisation s'est de plus en plus répandue dans d'autres domaines tels le commerce, l'éducation ou la santé notamment, dans lequel il est une solution innovante pour embarquer des données médicalement sensibles sous forme compactée, portable et accessible [23] .

Dans un cadre médical, les QR codes peuvent inclure des données très critiques telles que les antécédents médicaux, le groupe sanguin, les allergies, le traitement en cours, les résultats d'analyses ou des instructions en cas d'urgence. Dans les cas de transferts inter-hospitaliers notamment ou dans des situations d'urgence, cette forme de données peut être particulièrement utile dans la mesure où l'accès à l'information y est d'une grande rapidité. Toutefois, son usage dans ce champ médical interroge les enjeux de sécurité et de confidentialité [24][25] .

Dans le but d'assurer la pérennité de ces données, il existe couramment un certain nombre de pratiques de sécurité :
Chiffrement symétrique (AES-128 ou AES-256) : Les données sont chiffrées en fonction de l'algorithme AES (Advanced Encryptions Standard), considéré comme extrêmement solide. Sa mise en œuvre requiert l'usage d'une clé secrète à partager à destination des encodages et décodages des informations, de sorte que seules les entités autorisées disposent d'accès à ces informations [26][27] .
Encodage Base64 : Les données ont le statut de données chiffrées binaires, format dans lequel elles sont disponibles via l'encodage Base64 pour les concilier avec les conducteurs et interprètes de QR codes qui, à l'origine, opèrent en chaînes de caractères.
Ajout d'un identifiant de vérification ou d'un hash (empreinte cryptographique) : cela permet de permettre d'assurer l'intégrité des données, de pouvoir détecter s'il y a eu falsification ou modification non autorisée.

Le recours à des QR codes chiffrés propose ainsi une sécurité de double niveau :
Protection physique : L'accès est limité à des dispositifs spécifiques (applications mobiles, plateformes sécurisées), réduisant ainsi le risque de diffusion accidentelle ou d'exploitation non empathique ;
Protection logique : Sans la clé de déchiffrement, aucune des données visibles demeure ainsi lisible. Elles gardent leur confidentialité et leur intégrité même en cas de copie ou d'accès non autorisé.

Les recherches contemporaines viennent, effectivement, de démontrer tout l'intérêt de cette approche. Les travaux d'Abdul-Jabbar et Farhan (2023) signalent ainsi un système utilisant le chiffrement AES pour protéger la confidentialité des informations médicales, le hachage pour garantir leur intégrité, la compression ADN pour en assurer tout le poids dans un code QR d'interopérabilité, combinés à un protocole sécurisé de gestion de la clé pour générer des codes QR médicaux à la fois compacts, absolument sécurisés et interopérables, selon les exigences de la sécurité des données de santé [28] .

1.4.2 Applications existantes

Touchant presque tous les secteurs d'activité, les QR codes sont également fortement intégrés dans le domaine de la santé, par exemple pour identifier rapidement un patient, accéder à son dossier médical ou déclencher des alertes [29] .

a) Cartes médicales d'urgence

Un certain nombre de systèmes fournissent aux patients une carte ou un bracelet contenant un QR code. En cas d'urgence, les secouristes peuvent scanner ce QR code afin d'accéder aux informations utiles : allergies, groupe sanguin, traitements… [30]

Figure 5 : Carte médicale ICE (In Case of Emergency) avec QR code intégré our l'accès aux données. [31]

Les cartes ICE Medical Cards, très répandues aux États-Unis, permettent d'accéder à un profil médical stocké soit en ligne, soit dans le QR code. [32]

b) Certificats sanitaires numériques

Au cours de la pandémie de COVID-19, dans l'objectif d'étayer l'exigence de vaccination, les passe sanitaires fournissaient le statut vaccinal au moyen de QR codes, qui étaient accessibles via des certificats de santé électronique contenant des données signées numériquement ou chiffrées, en assurant ainsi l'authenticité et la confidentialité [33] .

Figure 6 : Certificat numérique COVID de l'Union européenne (EU DCC) avec QR code contenant des données médicales protégées. [34]

c) Systèmes de surveillance pour patients vulnérables

Les applications de suivi des personnes âgées ou atteintes de troubles cognitifs permettent l'association d'un QR code à chaque patient, affiché sur ses vêtements, un badge ou un bracelet, présentant des données utiles en cas de perte ou en cas de crise médicale [35] .

Figure 7 : Bracelet médical avec QR code pour l'identification des patients atteints d'Alzheimer (projets pilotes en Espagne et au Japon). [36]

I.5 Systèmes de localisation et d'alerte

I.5.1 Technologies de géo localisation

Dans le cadre des dispositifs destinés aux personnes vulnérables, âgées, ou souffrant de troubles cognitifs (comme la maladie d'Alzheimer) ou de handicap, la localisation est une fonction clé, puisqu'un individu peut être localisé en temps réel afin de déclencher automatiquement (ou manuellement) une alerte d'urgence, dénonçant les risques de perte de repères ou d'errance [37] .

Les principales technologies de géo localisation utilisées sont :

- GPS (Global Positioning System)
Le GPS fonctionne via un réseau de satellites, permettant une localisation dont la précision est souvent meilleure qu'une marge d'erreur de 5 mètres mais uniquement en extérieur, et dans le cadre d'un suivi en temps réel et adapté à des espaces ouverts (rues, parcs, etc.). En intérieur, ou en cas d'obstacles physiques (bâtiment, tunnel, forêt dense), ses performances deviennent médiocres [38] .

- GSM (Global System for Mobile Communications)
S'appuyant sur la triangulation entre plusieurs antennes relais cellulaires, le GSM présente une précision moins bonne (généralement entre 100 et 500 mètres, selon la densité du réseau), mais offre une couverture très large, même dans certaines zones mal couvertes par le GPS, tout en ne nécessitant pas l'usage d'un réseau téléphonique [39] .

-Référentiels Wifi
En milieu intérieur, comme les hôpitaux, les maisons médicalisées ou les domiciles, il est (peut) possible se géo localiser à l'aide des réseaux Wifi existants, en calculant la puissance et l'identifiant (SSID, BSSID) des différents points d'accès Wifi pour obtenir une précision d'estimation de position de l'ordre de 10 mètres, voire meilleur dans les espaces très couverts [40]. Cette méthode trouve son intérêt lorsque le GPS n'est pas dans le champ d'investigation, mais dépend d'une infrastructure réseau stable.

Ces technologies peuvent être complémentaires pour servir une meilleure précision et fiabilité de positionnement, en particulier au sein des systèmes de géo localisation hybride des Smartphones ou montres connectées [41] .

Technologie	Précision	Portée	Avantages	Inconvénients	Utilisation typique
GPS	Haute (3 à 10 mètres en extérieur)	Monde entier (via satellites)	- Très précise en extérieur- Fonctionne partout sur Terre	- Inefficace en intérieur ou zones urbaines denses- Consommation énergétique élevée	Navigation, suivi de véhicules, applications de randonnée
GSM	Faible à moyenne (100m à plusieurs km)	Zones couvertes par les antennes GSM	- Fonctionne dans la plupart des zones couvertes- Faible consommation	- Précision très faible- Dépend de la densité des antennes relais	Localisation approximative d'appels ou d'utilisateurs mobiles
Wi-Fi	Moyenne à élevée (5 à 50 mètres)	Zone de couverture du réseau Wi-Fi	- Bonne précision en intérieur- Faible consommation- Disponible en zones urbaines	- Nécessite des réseaux Wi-Fi connus ou enregistrés	Localisation en intérieur (bâtiments, aéroports, centres commerciaux)

Figure 8: Comparaison des technologies de géo localisation (GPS, GSM, Wifi).

I.5.2 Solutions d'alerte pour personnes vulnérables

La sécurité des personnes en situation de vulnérabilité, tel que les personnes âgées, les personnes atteintes de troubles cognitifs (tels que la maladie d'Alzheimer) ou encore les patients en perte d'autonomie, reposent sur des systèmes d'alerte intelligents et réactifs permettant d'alerter un proche ou une unité d'urgence en cas de danger (chute, errance, malaise…).

Les principales solutions d'alerte peuvent être reparties en 3 grandes typologies :

a) Boutons d'alerte ou bracelets SOS

Ces dispositifs, souvent utilisables qui prennent la forme de bracelets, de pendentifs, de montres connectées permettent à l'utilisateur d'émettre une alerte de manière manuelle (simple pression sur le bouton). Elle sera alors transmise à des parent, des soignants ou une centrale d'assistance, souvent rejointe d'une localisation par GPS. [42]

Certains modèles se couplent à un capteur de détection de chutes ou de rythme cardiaque et déclenche automatiquement l'alerte en cas d'asymétrie détectée. [43]

b) Alertes géo localisées par QR codes

La mise en œuvre de QR codes personnalisés stockant des informations médicales ou identitaires (chiffrées et anonymisées pour la confidentialité), permet de faciliter le début de la prise en charge lors de la découverte d'un patient désorienté. Ainsi, scanné avec un téléphone, ce QR code peut générer automatiquement une alerte à partir de la position GPS du téléphone, afin d'interpeller proches ou secours [44] . Il s'agit d'un mode de communication particulièrement adapté aux patients Alzheimer, très exposés à des épisodes d'errance.

c) Applications mobiles intelligentes

Aujourd'hui, des applications mobiles spécialisées sont créées pour suivre en temps réel des patients vulnérables, repérer une situation à risque, alerter en cas de nécessité, etc. Ces applications intègrent plusieurs fonctionnalités avancées, pour la plupart :

Un module de géo localisation permanente, permettant de suivre en continu la position du patient (p. ex. : Life360, GeoZilla) ;

Un système de géofencing, permettant de déclencher une alerte automatique lorsque l'utilisateur sort d'une zone de sécurité préétablie (p. ex. : Safe365, AngelSense) ;

L'envoi automatique de messages d'alerte (par SMS ou WhatsApp), avec les coordonnées GPS du patient, à un ou plusieurs contacts (p. ex. : MySOS Family, FallSafety Home) ;Un historique des alertes et déplacements, servant à une analyse médicale ou à un suivi par la famille (p. ex. : CarePredict, Watch Over Me).

Chapitre 1
État de l'art

Il s'agit de systèmes reposant sur la convergence de dispositifs de géo localisation (GPS, GSM, Wifi), de capteurs embarqués (accéléromètre, gyroscope) et d'un serveur centralisé de collecte et d'archivage des données, en conformité avec la réglementation sur les données personnelles (RGPD, HIPAA).[45][46]

Chapitre2. Conception du système

Chapitre 2

Conception du système

II.1 Architecture Générale

II.1.1 Composants du système

Le système est composé de quatre éléments interdépendants et performatifs : chacun d'eux répond à une fonction précise dans le processus d'identification, de localisation et d'alerte d'un patient Alzheimer.

1. Application web (plateforme de gestion)

Développer en PHP et doté d'une interface HTML/CSS, la plateforme permet :

- Enregistrement, mise à jour et suppression des données des patients.

- Gestion des utilisateurs autorisés (users).

- Affichage en temps réel des alertes via une carte intégrée (Google Maps).

- Consultation de l'historique des déplacements via la table trace.

2. Base de données MySQL

Le SGBD MySQL permet d'enregistrer l'ensemble des données (sensibles ou non) indispensables au bon fonctionnement du système :

- Table patients : enregistre les informations personnelles du patient (id , nom, prénom , maladie , code_qr , adresse , telephone_parents , date_creation , telephone_fixe , nom_responsable , prenom_responsable , adresse_responsable).

- Table users : enregistre les accès administrateurs de la plateforme web (id , nom , prenom , choix , mot_de_passe , date_creation).

- Table trace : enregistre les alertes géographiques (id , id_user , nom_user ,code_qr localisation , date ,tache).

3. Application Mobile Androïde

Développée en Java , cette application est utilisée par les aidants ou citoyens pour :

- Scanner le QR code cousu sur les vêtements du patient.

- Décrypter le code Qr via AES.

- Obtenir la géo localisation GPS.

- Alerter via SMS le responsable du patient (parent/tuteur/proches/famille) en indiquant sa position.

Les échanges entre les différents composants du système : Les divers composants s'échangent des informations par API PHP, sur requêtes HTTP sécurisées, avec stockage des utilisateurs en base MySQL. Dans le QR code est stockée une chaîne chiffrée par AES contenant l'identifiant patient et la clé intégrée au code. Lorsque le QR code est scanné, la position GPS est récupérée par le service Androïde Location Services, puis transférée pour être affichée dans l'application web .

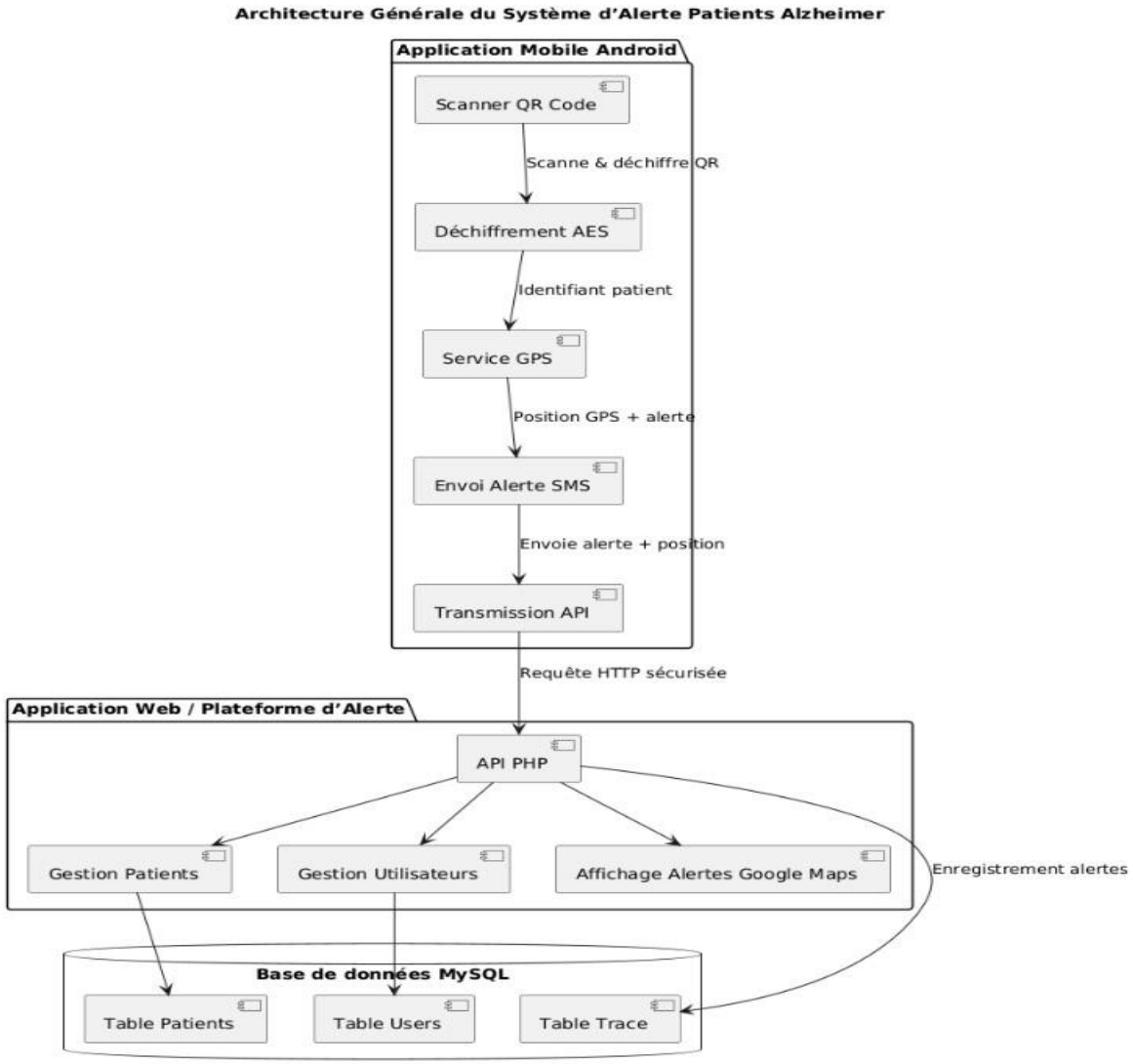


Figure 9 : Architecture générale du système d'alerte pour patients Alzheimer .[47]

Chapitre 2

Conception du système

La figure 9 met en lumière l'architecture globale du système proposé, illustrant ainsi les interactions entre l'application mobile, l'API PHP, la plateforme web et la base de données MySQL. Ce schéma permet de suivre les différentes étapes pour passer de l'épisode du scan du QR code de la personne à l'enregistrement sécurisé de l'alerte.
Le schéma de cas d'utilisation ci-après présente les interactions entre les différents acteurs du système (administrateur, associateur, utilisateur mobile, responsable du patient) et les cas d'usage qu'ils déclenchent dans la plateforme Alzheimer. Il permet de modéliser les fonctionnalités disponibles selon les rôles, les processus de scan du QR code, d'envoi d'alerte, et de gestion des patients.

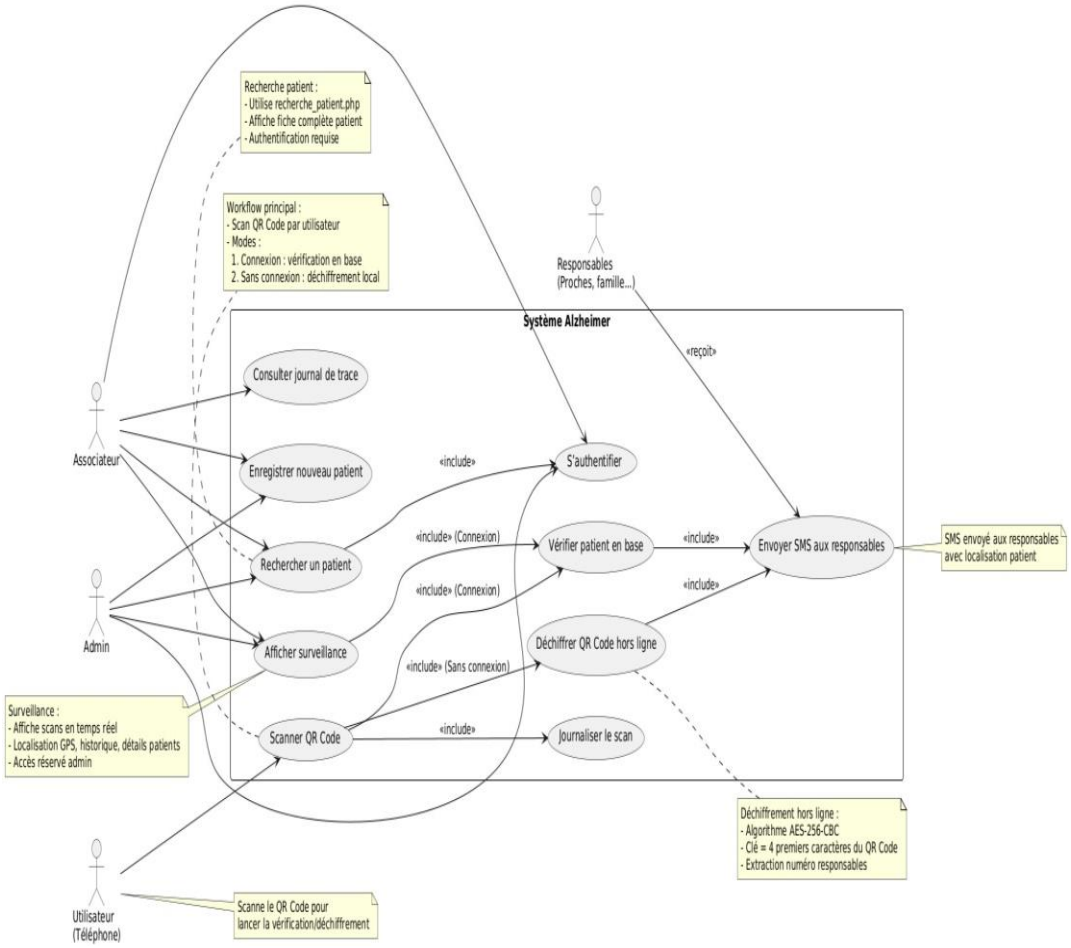


Figure 10 : Diagramme de cas d'utilisation du système Alzheimer .[48]

Notre système repose sur quatre principaux acteurs que sont « Admin », « Associateur », « Utilisateur mobile » et « Responsable ». Les principaux cas d'usage qui le caractérisent sont : « authentification, enregistrement, recherche de patient, scan de QR code, consultation du journal, envoi de SMS d'alerte ». Deux modes d'usage mobile existent :
« connecté »(vérification serveur) et « hors ligne » (déchiffrement local AES). Des dépendances fonctionnelles « inclure » offrent le bon enchaînement des actions (décryptage ou vérification avant l'envoi de l'alerte par exemple).

Chapitre 2

Conception du système

Le schéma qui suit représente la structure orientée objet de l'application mobile, avec présentation des différentes classes logicielles, de leurs attributs et méthodes, de leurs relations. Cette modélisation permet ainsi de bien appréhender l'implémentation de l'application et son interaction avec les services de géo localisation, de base de données et de traitement des QR codes.

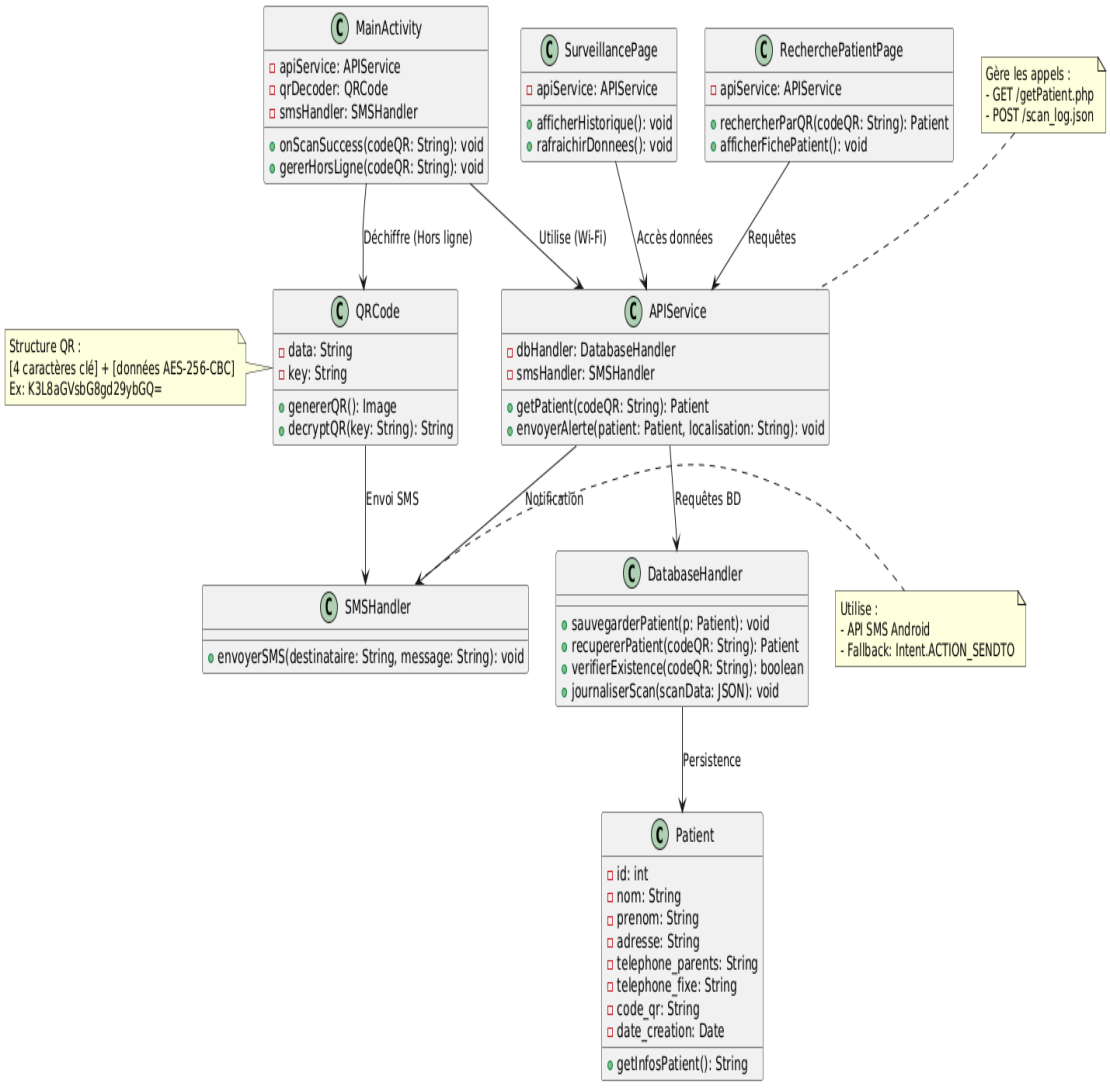


Figure 11 : Diagramme de classes de l'application mobile Alzheimer .[49]

Au cœur de cette application, plusieurs classes principales sont assurément présentes, « MainActivity », qui est tout d'abord le point d'entrée de l'application, ensuite l'application qui gère le mode hors ligne, déclenche le scan QR, « QRCode », qui d'une part s'occupent de la génération et du déchiffrement des QR codes (chiffrement AES-256-CBC en utilisant une clé intégrée). Pour pouvoir envoyer les alertes par SMS, « SMSHandler »fait appel soit à l'API Android soit à une éventuelle alternative pour envoyer les alertes SMS. « APIService » qui, entre l'interface utilisateur et le serveur (requêtes GET/POST) faitoffice d'intermédiaire, « DatabaseHandler » qui, accède aux données patients puis permet leur validation ainsi que la journalisation. « Patient » est le modèle de données qui inclut les informations personnelles. « SurveillancePage » et « RecherchePatientPage » sont les interfaces permettant de visualiser l'historique de surveillance ou de rechercher un patient à partir du QR code.

II.1.2 Flux d'information global

La proposition de système s'appuie sur une articulation soignée de plusieurs éléments : une application mobile, une plateforme web et une base de données. Elle permet un traitement rapide et sécurisé des alertes relatives aux patients atteints de la maladie d'Alzheimer. Ce flot garantit la fiabilité de la transmission des informations, depuis la détection jusqu'à la gestion (suivi) des alertes.

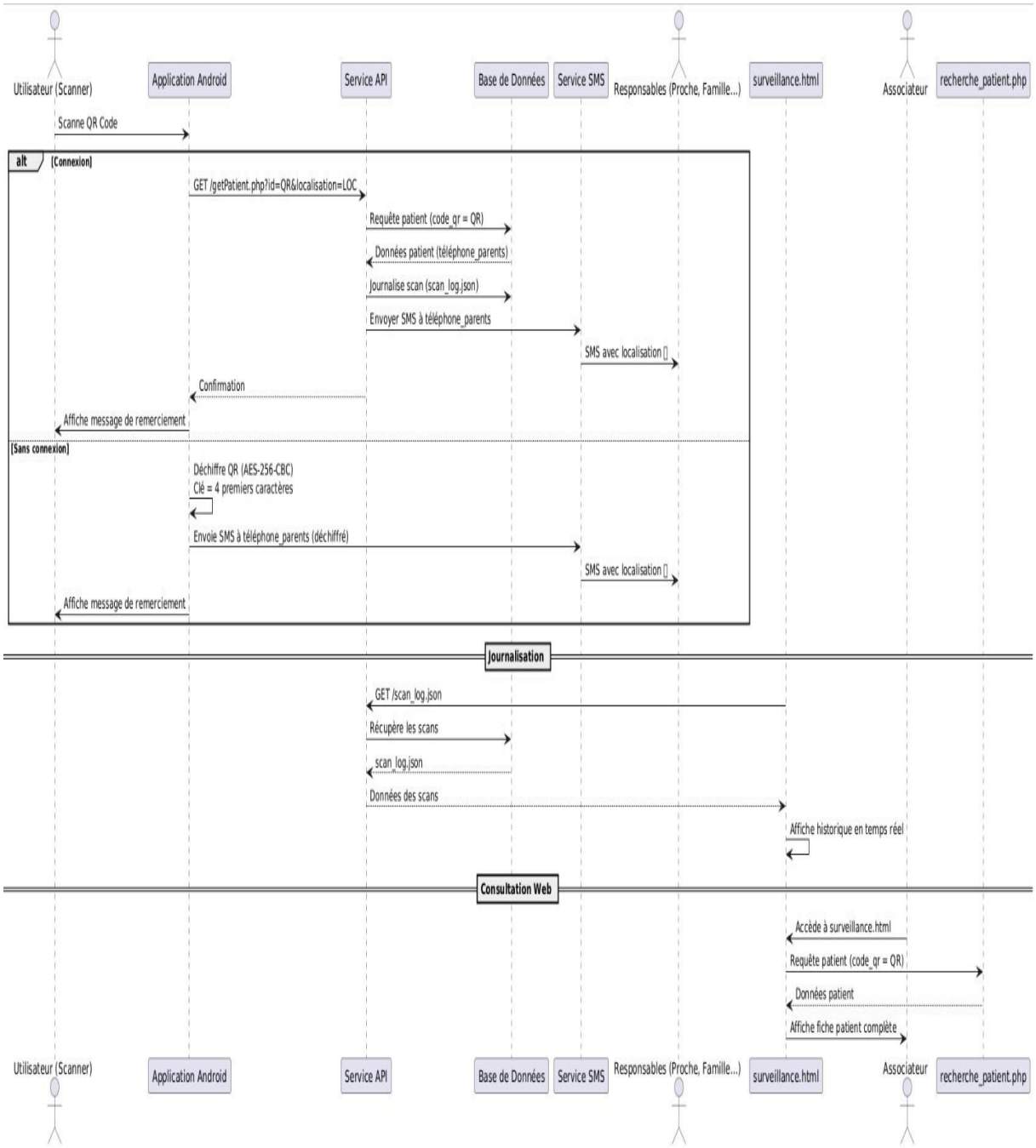


Figure 12 : Diagramme de séquence du flux d'information global .[50]

Le diagramme résume les échanges dynamiques entre les différents éléments clés du système (mobile, serveur, base de données, plateforme web) pendant le processus de détection d'un patient et de génération d'une alerte. L'accent est ainsi mis, à la fois sur les enchaînements d'appels et sur les temps de réponse conditionnant un traitement synchrone et sécurisé de l'information.

II.1.2.1 Déroulement du processus

De manière à bénéficier d'une prise en charge rapide et efficace lors de situations d'urgence, l'architecture du système intègre plusieurs étapes s'effectuant généralement de façon successive. La séquence des opérations effectuées par un utilisateur (aide-soignant, médecin ou citoyen) dans un mode d'usage habituel est la suivante :

1. Scan du QR Code

L'utilisateur scanne le QR code que porte l'utilisateur (aide-soignant, médecin ou citoyen) du Smartphone Androïde avec lequel il utilise l'application mobile pour scanner le QR code que porte le patient. Ce QR code contient des données sensibles chiffrées dont un identifiant patient ou un numéro de téléphone.

2. Déchiffrement AES

Le contenu du QR Code est déchiffré localement par l'algorithme AES en mode de fonctionnement CBC (Cipher Block Chaining) lui permettant d'extraire l'information nécessaire à la prise en charge : l'identifiant unique du patient ou le numéro de téléphone de son responsable.

3. Obtention de la géo localisation

L'application enclenche le service GPS du Smartphone pour déterminer le lieu où se trouve le patient.

4. Transfert de l'alerte

Si le réseau Internet est accessible, l'application :
- envoie une requête HTTP sécurisée à un script PHP (getPatient.php) qui interroge la base de données MySQL fournissant ainsi le dossier du patient ;
- fait un envoi immédiat d'un SMS au numéro de son proche ou responsable légal à qui une alerte est transmisse avec un message la précisant, ainsi que la position GPS du patient ;
- ou encore l'enregistrement de cet alerte par appel à une API REST vers le serveur Web pour archivage et visualisation en temps réel.

5. Affichage et journalisation

Le contenu de l'alerte est insérée dans la table trace de la base de données MySQL pour son suivi, puis afficher sur une carte dans l'interface Web surveillance.html par intégration de Google Maps.

6. Consultation Web

Les utilisateurs autorisés peuvent accéder à une interface permettant de consulter les fiches des patients, les historiques des alertes, et les traces de la géo localisation dans une interface (recherche_patient.php).

II.1.2.2 Comportement en mode déconnecté

Dans le but d'assurer la continuité de service régulier, même sans réseau, un mode hors ligne est développé au niveau du système pour permettre au terminal Androïde de fonctionner seul lorsqu'un accès au serveur n'est pas disponible. Dans ce cas, le déchiffrement du contenu du code QR est opéré localement sur le Smartphone, sans transmission vers une plateforme. Le numéro de téléphone du responsable est extrait des données décryptées qui permettent aussi d'envoyer directement un SMS contenant la position GPS du patient, obtenue via le module GPS intégré de l'appareil, sans avoir à faire d'appel Internet. Même si l'alerte n'est pas effectivement enregistrée au niveau du serveur et n'apparait donc pas sur la plateforme de supervision, l'application mobile offre à son utilisateur une vérification locale immédiate sur l'envoi ayant été opéré avec succès assurant ainsi un retour visuel, rapide et rassurant.

II.2 Gestion des données patients

II.2.1 Formulaire de saisie des coordonnées

La gestion des données concernant les patients démarre par la réalisation d'un formulaire de saisie ergonomique, structuré et sécurisé, accessible uniquement via une interface web pour les professionnels de santé ou les administrateurs identifiés et authentifiés, ayant pour but de recueillir l'ensemble des informations nécessaires à la bonne identification ainsi qu'au suivi du patient : les nom, prénom, adresse, numéro de téléphone du responsable à contacter, son nom, prénom et adresse, ainsi que la date d'enregistrement, générée automatiquement, ou manuellement lors de la création du dossier, tout comme chaque patient reçoit automatiquement un identifiant unique (UUID) pour garantir l'uniformité des enregistrements dans la base de données, et enfin, un code QR généré dynamiquement à partir des données chiffrées, et prêt à être imprimé sur un support vestimentaire. Ce formulaire intégré à la plateforme web n'est accessible qu'après authentification sécurisée, garantissant ainsi la confidentialité, sécurité, traçabilité et contrôle d'accès lors des opérations de saisie.

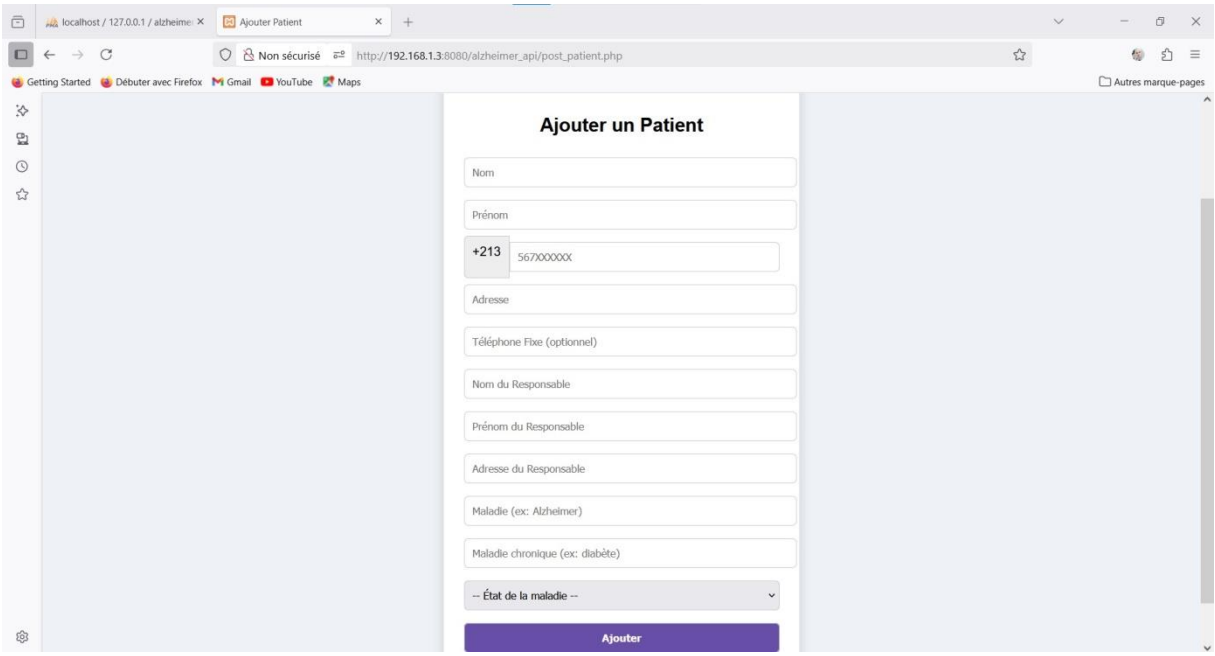


Figure 13: Interface de saisie des données patients .[51]

L'image montre un **formulaire web** utilisé pour **ajouter un patient**. Il contient plusieurs champs à remplir : le nom, le prénom, le numéro de téléphone, l'adresse du patient, ainsi que les informations d'un responsable (nom, prénom, adresse). En bas, il y a un bouton marqué "**Ajouter**" pour valider l'enregistrement.

II.2.2 Structure et sécurisation des données

Les informations recueillies à l'aide du formulaire de saisie sont conservées dans une base de données relationnelle conçue selon un schéma structuré garantissant la cohérence, l'intégrité et la traçabilité de l'information. Chaque champ (nom, prénom, adresse, téléphone du responsable, etc.) est typé de façon explicite (chaîne de caractères, date, identifiant unique) et fait l'objet de contraintes de non-nullité, d'unicité, et de validation anticipe le risque d'erreurs ou de doublons au moment de l'enregistrement. Un identifiant unique est généré de façon automatique pour chaque patient, ce qui permet de garantir que chaque état est individualisé.
Du point de vue de la sécurité, des mécanismes de chiffrement symétrique AES sont appliqués aux données sensibles, dont le numéro de téléphone du responsable. Ce chiffrement est effectué avant tout enregistrement dans la base, empêchant de fait toute lecture, non autorisée ou non, d'un accès à la base. En outre, un accès à la plateforme est strictement limité par une authentification fondée sur des rôles utilisateurs qui permettent des droits d'accès sélectifs et réservés, cuisine auprès des seuls administrateurs ou agents de santé habilités.
La totalité des actions réalisées (ajouts, modifications, suppressions) fait également l'objet d'une journalisation assurant ainsi la traçabilité complète des opérations et contribuant ainsi à l'atteinte des trois exigences de sécurité du système, à savoir la confidentialité, l'intégrité et la disponibilité des données.

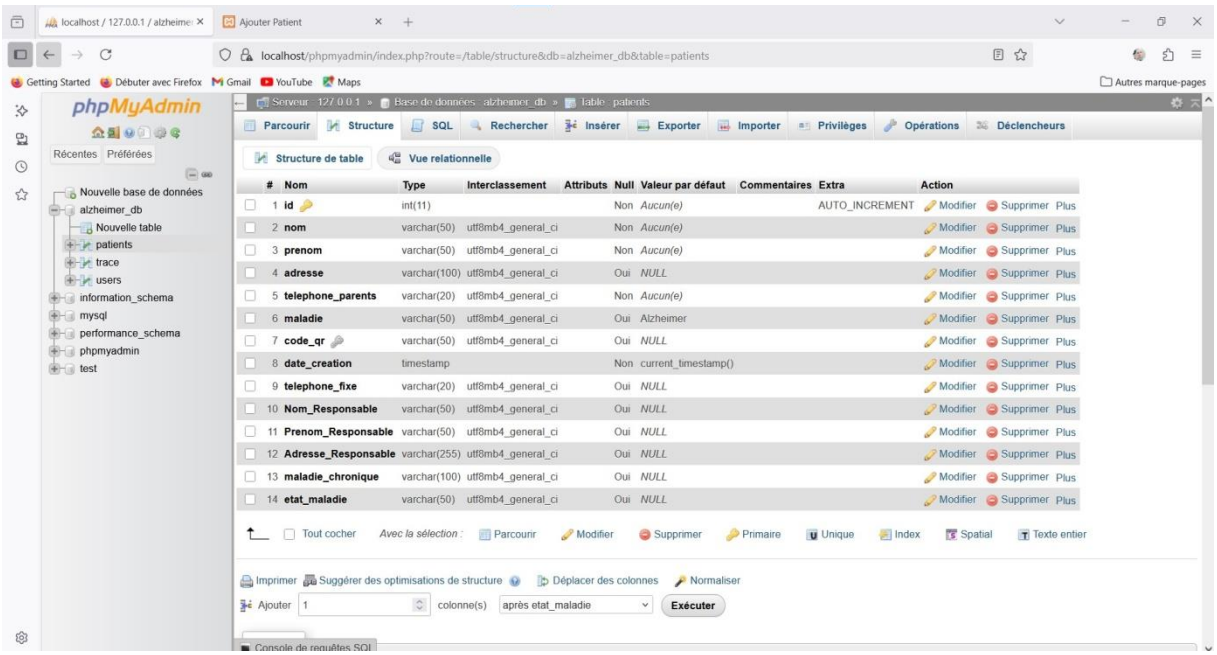


Figure 14: Structure de la table patients dans la base de données alzheimer_db .[52]

Dans le contexte de l'affichage dans phpMyAdmin de la table `patients`, l'ensemble de leurs champs est indispensable à l'identification, à la localisation, à la prise en charge et à l'accompagnement des patients atteints d'Alzheimer, ces champs étant les suivants : informations privées (nom, prénom, adresse personnelle), coordonnées personnelles des aidants et des proches, code QR (qui est unique) servant d'accès au profil du patient, sachant que des contraintes telles que l'unicité du code QR ainsi que le recours à la méthode de chiffrement AES sont à garantir bien évidemment dans le souci d'assurer la confidentialité et la fiabilité des données.

II.3 Chiffrement AES

II.3.1 Choix de l'algorithme et de ses paramètres

Pour veiller à la confidentialité des données personnelles sensibles des patients, telles que leur identité ou leurs contacts d'urgence, notre choix s'est porté sur l'algorithme AES (Advanced Encryption Standard), connu pour sa solidité. AES a été utilisé dans notre solution en mode CBC (Cipher Block Chaining) qui renforce la sécurité en liant chaque bloc chiffré à son prédécesseur. La clé de chiffrement sera simplement une chaîne de caractères « courte », par exemple 7K92, qui sera hachée avec SHA-256 pour produire une clé AES de 256 bits. Le chiffrement CBC a également besoin d'un vecteur d'initialisation (IV) au hasard de 16 octets, généré dynamiquement à chaque opération de chiffrement. Le IV est en effet essentiel pour

éviter qu'une même clé et un même message donnent le même résultat chiffré.

- Exemple 1 :

Texte à chiffrer : ID=125 ; Nom=Ali ; Tel=0550123456

Clé courte : 7K92 → SHA-256 → Clé AES : e26a...d9fe (32 octets)

IV généré : a3b1c9d5627890ff33aa12bc7689eac4

Texte chiffré (hex) : a3b1c9d5627890ff33aa12bc7689eac4b9f06e24f2...

II.1.1 Intégration de la clé dans la chaîne cryptée

Dans le cadre de la simplification du déchiffrement côté application mobile, la clé de taille limitée utilisée pour générer la clé AES est récupérée depuis la chaîne cryptée en ajoutant la courte clé, qui pourra (par exemple, 7K92) être ajoutée au début de la chaîne cryptée, suivie de la chaîne chiffrée codée en Base64. Chaque QR code devient alors autonome, sans nécessité de faire appel à une base de données externe permettant de retrouver la clé. Lors de la lecture du code QR, l'application extrait cette clé, la transforme via SHA-256 en clé AES, puis déchiffre le reste de la chaîne selon le mode utilisé. Le niveau de sécurité est garanti tant que la clé de petite taille reste assez difficile à deviner et que le système n'est pas exposé.

- Exemple 2 :

Clé courte : 7K92

Donnée chiffrée (encodée Base64) : U2FsdGVkX1+ZZ9N2HQyHAbS4P3...

Chaîne finale stockée dans le QR code : 7K92U2FsdGVkX1+ZZ9N2HQyHAbS4P3...

L'application :

Extrait les 4 premiers caractères : 7K92

Génère la clé AES

Déchiffre la suite : U2FsdGVkX1+ZZ9N2...

II.4 Génération du QR code

II.4.1 Contenu du QR code

Le QR code que l'on génère renferme les informations permettant d'identifier le patient, mais d'une manière sécurisée. En effet, les données à caractère personnel (l'identifiant unique du patient, le nom ou le téléphone de son référent) sont d'abord parées d'un chiffrement via l'algorithme AES, avec une clé secrète de 128 bits. Dorénavant, cette chaîne chiffrée est codée sous forme de QR code, ou bien pour réaliser le déchiffrement côté mobile, une partie de la clé AES peut être glissée directement dans la chaîne chiffrée comme elle pourrait aussi être reconstituée d'un algorithme partagé.

- Exemple 3 :

Données initiales : id=12345 ; nom=LABANI ; tel=+213774779227

Clé AES : Xf93z!qP4L9tYw

Chaîne chiffrée (AES/ECB) : D7F9A4B...ZK1U==

Contenu du QR : D7F9A4B...ZK1U==#Xf93z!

Figure 15 : Exemple de *QR code contenant les données cryptées et la clé intégrée* .[53]

II.4.2 Impression sur vêtement (contraintes matérielles

et lisibilité)

Une fois le QR code créé, il est nécessaire de l'imprimer sur les vêtements du patient de manière pérenne, lisible et durable. Cela nécessite le choix minutieux de certains matériaux dont les qualités sont adaptées, tel que le tissu, qui doit être clair et uni, dépourvu de motifs qui viendraient perturber la lecture du code par un lecteur optique. Les travaux d'impression doivent recourir à des procédés durables tels que l'impression par transfert thermique ou la broderie numérique, afin de garantir la pérennité du code malgré l'influence du lavage et de l'usure. Le QR code devra aussi être de taille suffisamment importante pour permettre une lecture sans encombre, même en mouvement, en basse lumière, et d'une résolution minimale de 300 dpi permettant ainsi une lecture correcte.

- Exemple d'application :

Taille minimale recommandée : 20 × 20 cm

Techniques d'impression : transfert thermique ou broderie numérique

Types de vêtements : pull, casquette, t-shirt

Emplacements : poitrine, dos ou manche , devant de casquette .

Cette méthode permet aux passants, aux aidants et donc aussi aux professionnels de santé de scanner rapidement le code, y compris à distance raisonnable du patient, et ainsi d'accéder aux informations nécessaires à la prise en charge du patient.

Figure 16: Exemple d'un vêtement (pull) et casquette avec un QR code . [54]

Conception du système

Figure 17 : T-shirt du patient intégrant un QR code personnalisé avec logo, imprimé pour assurer l'identification et la lisibilité en milieu extérieur. [55]

II.5 Application mobile

L' application mobile (RANI MAAK) constitue l' interface technologique du système en mettant en relation le citoyen , le patient et le serveur . Elle permet de scanner le QR Code du patient , de déchiffrer les données qui le sécurisent , d' alerter les agents en cas de besoin et de transmettre les informations récupéré es à la plateforme centrale. Une fois le QR Code d é codé , l' ensemble des opérations fonctionne automatiquement , sans intervention humaine .

II.5.1 Scan du QR code et extraction des données

Le processus débute par le scan du code QR porté par le patient (intégré dans le vêtement). Ce code a été généré à partir des informations personnelles du patient (identifiant, numéro du tuteur, etc.) préalablement chiffrées à l'aide de l'algorithme AES.L'application utilise la bibliothèque ZXing ("Zebra Crossing") qui permet un scan rapide et fiable à l'aide de la caméra du téléphone. Une fois le QR code détecté, il est décodé en une chaîne de caractères représentant les données chiffrées.

Exemple de contenu extrait :

WSIUV71PSFNat95fq3VzWHFQZS9QVmCp0J/jUADvmJlPxqI=

Ces données ne sont pas exploitables sans le processus de déchiffrement qui suit.

II.5.2 Déchiffrement avec la clé extraite

Les données intégrées sont dans le code QR apparaissant dans une version chiffrée selon l' algorithme AES-128 en mode CBC (Chaining Block of Ciphers) . Le choix de l' AES comme chiffre pour le contenu QR est pertinent du fait de la sécurité mise en avant par ce chiffre symétrique largement répandu . L'application contient en local une clé secrète soit codée en dur (dans les premiers prototypes), soit envoyée é e de manière sécurisée par la plateforme lors de l' installation . Une fois les données extraites du code QR , l' application applique le déchiffrement via l' algorithme AES avec une initialisation vectorielle (IV) récupérée ou fixée .

Résultat du déchiffrement :

ID=1234 ; TEL= +213772444417; NOM= Benyahia ; PRENOM= Abdelkader

Les données ainsi obtenues sont analysées et exploitées immédiatement pour le processus d'alerte.

II.5.3 Envoi du message d'alerte au responsable

Une fois le QR code du patient scanné et les données correctement déchiffrées, l'application déclenche automatiquement une alerte destinée au responsable (parent, tuteur ou proche), selon les conditions de connectivité du Smartphone. Deux scénarios sont prévus :

1. Mode hors ligne (absence de connexion Internet)

Lorsque le téléphone n'est pas connecté au réseau, l'application affiche localement un message d'alerte en arabe, comprenant les coordonnées GPS du patient. Par exemple :

تم العثور على المريض في الموقع
34.8605671,0.1553248

Ce message peut être lu et transmis manuellement par l'utilisateur à un tiers (famille, autorité ou soignant), ce qui permet d'agir même en l'absence de réseau mobile ou Wi-Fi.

2. Mode connecté (avec réseau disponible)

Lorsque l'appareil est connecté à Internet ou au réseau mobile, l'application utilise l'API SMS d'Androïde (SmsManager) pour envoyer automatiquement un message d'alerte au numéro de téléphone du responsable, contenant les données suivantes :

Alerte : votre patient Benyahia Abdelkader a été localisé.
Localisation actuelle : 34.8605671,0.1553248
Veuillez venir le récupérer rapidement.

Ce message est généré dynamiquement à partir :
des données contenues dans le QR code (nom, prénom du patient),
et de la position GPS en temps réel, obtenue via le Fused Location Provider.

Ce système garantit une réactivité immédiate et une assistance rapide, en s'adaptant aux conditions du terrain (connecté ou non). Il assure ainsi une protection renforcée des patients atteints de la maladie d'Alzheimer, notamment lorsqu'ils se retrouvent désorientés hors de leur environnement sécurisé.

L'envoi de SMS s'effectue silencieusement (sans intervention utilisateur) grâce à SmsManager, à condition que les permissions SMS aient été acceptées lors de l'installation de l'application.

Figure 18 : Exemples de messages d'alerte envoyés automatiquement – Mode hors ligne et mode connecté . [56]

II.5.4 Mise à jour et affichage de l'alerte sur la plateforme

Quand l' alerte se déclenche , depuis l'application mobile, selon que le terminal est soit en mode connecté é , soit en mode non connecté é , les données d' alerte sont traitées et pré envoyées différemment , et ces deux cas de figure au niveau de l' état de la connexion Internet font varier directement le traitement de données .

Chapitre 2

Conception du système

1. En mode en ligne (Wi-Fi ou données mobiles activés)

Conjointement avec la transmission du SMS au responsable, l' application mobile , au travers d' une API sécurisée , transmet au serveur les données données identifiant le patient, la date
et l' heure de l' incident ainsi que ses coordonnées géographiques , informations qui sont centralisées dans le serveur .
La plateforme web, notamment via la page (`surveillance.php`), interroge la base de données en temps réel pour récupérer les informations liées au patient. Elle affiche ensuite l'ensemble des données pertinentes dans l'interface dédiée au journal des scans patients , permettant un suivi détaillé de chaque alerte émise.

2. En mode hors ligne (Wi-Fi et données mobiles désactivés)

Lorsqu'elle fonctionne sans connexion Internet , l' application ne peut offrir qu'un mode local . Après scan du QR code et déchiffrement des données via l' algorithme AES,
l' application envoie automatiquement une alerte SMS au numéro de téléphone identifié dans le contenu du code. Or , aucune mise à jour ne peut être envoyée vers la plateforme web, faute de connexion avec le serveur. L' alerte ne figure alors pas dans l' interface en ligne, et rien n'est pas é dans la base de données distante . Ce mode assure bien que l' alerte soit transmise à la personne d' é signée , mais ne permet pas un suivi global sur la plateforme.

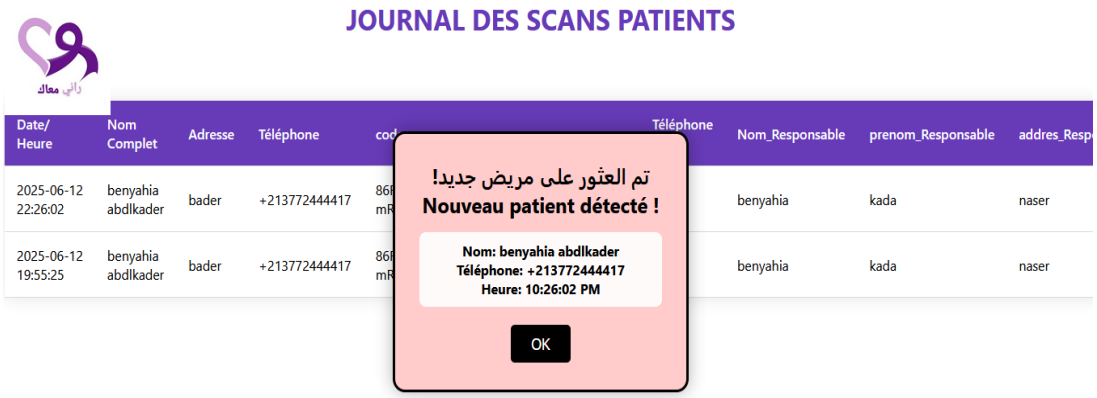


Figure 19 : Exemple d'affichage d'une alerte dans le journal des scans des patients . [57]

II.6 Système de géo localisation

II.6.1 Méthode de localisation utilisée

Le système de géo localisation de l'application mobile permet de déterminer précisément la position géographique du patient en temps réel. Pour cela, elle pense aux services de localisation disponibles sur le Smartphone, qui croise les signaux du système de géo localisation par satellite GPS (Global Positioning System), les réseaux Wi-Fi aux alentours et les antennes de téléphonie mobile. Ce fonctionnement de la géo localisation hybrides augmentent la précision de ses résultats, y compris dans les milieux urbains denses ou dans les zones faiblement couvertes par la géo localisation satellitaire.
Dès que le code QR a été scanné, l'application enclenche automatiquement le service de localisation pour obtenir les coordonnées latitude-longitude de l'appareil. Celles-ci sont alors utilisées pour construire une alerte annonçant la position en temps réel du patient, apportant ainsi aux proches du patient une information sur sa situation en cas d'urgence nécessitant une réponse rapide.
D'après Zandbergen & Barbeau (2011) le croisement de plusieurs sources de localisation permet un gain significatif en termes de précision pour les endroits où les signaux GPS sont atténués ou perturbés.

II.6.2 Transmission de la position à la plateforme

Une fois que les coordonnées GPS ont été obtenues, elles sont automatiquement intégrées dans le SMS d'alerte à remettre à la plateforme serveur. Ces données sont envoyées via une requête HTTP sur une API, en même temps que le SMS du service de secours.
L'identifiant du patient, la date-heure et la position sont stockés dans la base de données.
La plateforme peut ainsi lire ces éléments puis les afficher au sein de son interface de suivi en temps réel et surtout permettre aux responsables concernés d'agir effectif et rapidement pour apporter leur secours à un patient en difficulté.

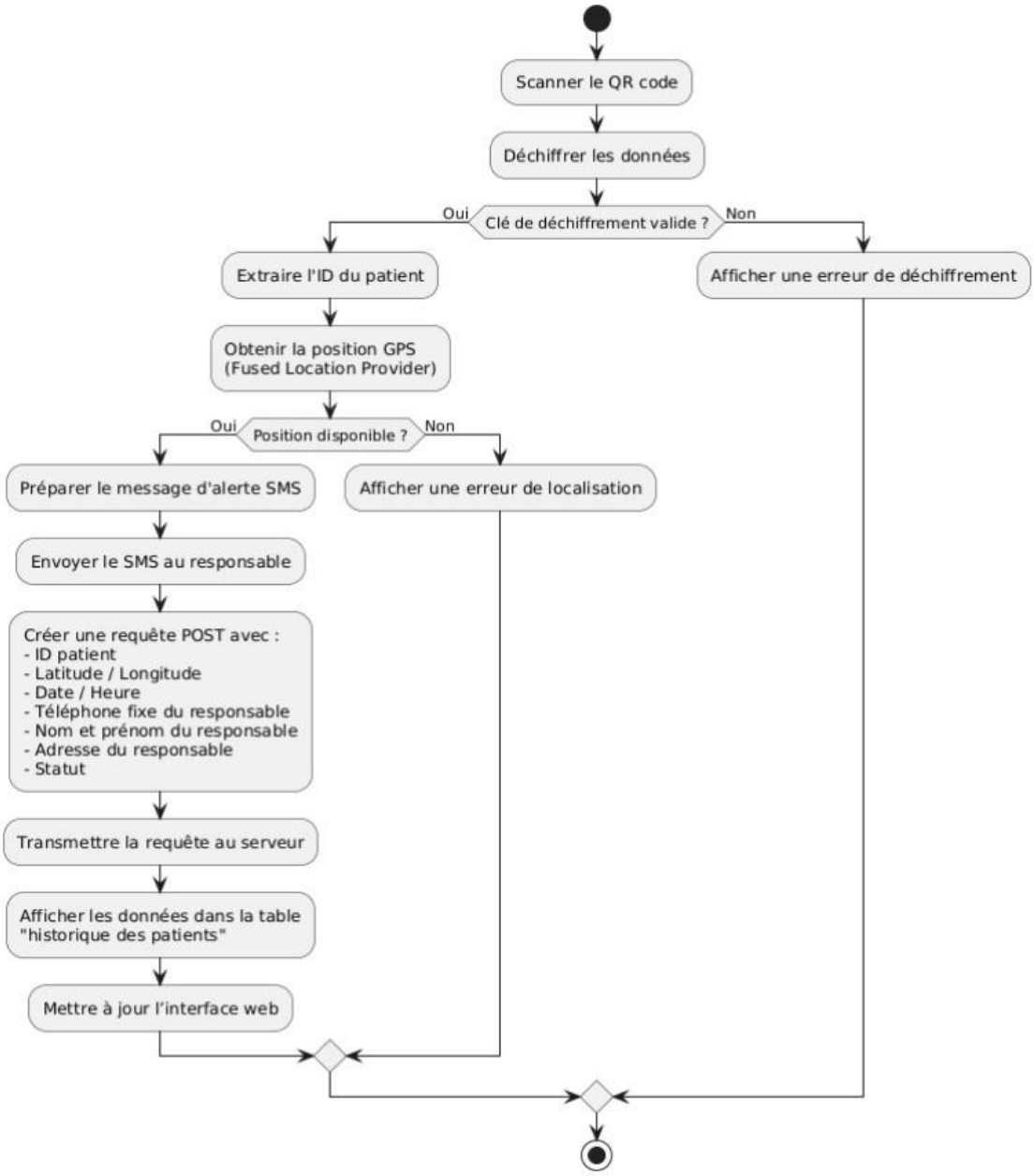


Figure 20 : Diagramme d'activité de la transmission de la position du patient à la plateforme . [58]

Chapitre3.Réalisation technique

Chapitre 3

Réalisation technique

III.1 Développement de l'application web

III.1.1 Technologies utilisées

Le développement de l'application Web a été accompli avec des technologies modernes permettant la performance, l'accessibilité, la sécurité et l'évolutivité dans divers environnements. Ce choix est dû à leur fiabilité, leur accessibilité et leur grande diffusion dans le champ professionnel du développement Web, ces dernières permettant un cadre rigoureux et adaptable au développement, la maintenance et l'évolution du système.

1.PHP (version 8.0) : Langage de programmation côté serveur

Le langage PHP a été utilisé pour le développement des interfaces côté serveur, dans le cadre de la gestion de la logique métier, de l'implémentation des opérations de chiffrement AES,
de la création des API REST, ainsi que de la manipulation de la base de données MySQL. PHP est l'un des langages le plus utilisé dans le développement web, grâce à sa syntaxe simple, sa rapidité d'exécution et sa compatibilité avec de nombreux serveurs web. La version 8.0 présente des améliorations intéressantes par rapport à des versions antérieures, telles que le typage fort, les attributs (annotations) et une meilleure gestion des erreurs [59] .

2.MySQL :Système de gestion de base de données

Le système de gestion de base de données relationnelle (SGBDR) choisi pour les données sensibles était MySQL. En effet, ce système s'est imposé comme la solution la plus cohérente et pertinente pour le stockage de données (informations de patients, utilisateurs, historiques
de géo localisation, etc.) en raison de sa performance, de sa sécurité et de sa compatibilité avec PHP. Ainsi, trois tables principales ont été utilisées pour les données projetées vers le tableau de bord : patients, users et trace. Pour une gestion efficace de ces données, le langage SQL permet d'effectuer des requêtes structurées [60] .

3.HTML5, CSS3, JavaScript ES6 : Les Technologies front-end

Le développement de l'interface utilisateur utilise les normes actuelles du développement Web. HTML5 structure les pages avec une sémantique éclairée, CSS3 assure une mise en page responsive, et JavaScript ES6 dynamise l'interactivité (contrôles côté client, animations, interactions AJAX). De ce fait, ces technologies garantissent la compatibilité avec les navigateurs récents et la bonne expérience utilisateur sur l'ensemble des supports

(ordinateurs, tablettes, smartphones) [61] .

4.API REST :Connexion entre les composants

La connexion entre l'application mobile de type Android et le serveur de type Web s'effectue via des API RESTful. Ces dernières sont réalisées avec PHP et permettent d'échanger des données via le protocole HTTP (GET, POST). Ainsi, après avoir scanné un QR code, l'application mobile envoie une requête au serveur qui déchiffre le contenu puis retourne les informations du patient. Cette architecture est simple, efficace et respecte les standards du WEB moderne [62] .

5. PHP QR Code :Génération de QR Codes

Pour mettre en place la génération de QR codes, la bibliothèque open source PHP QR Code a été intégrée dans ce projet. Elle permet de générer dynamiquement des images PNG à partir des données chiffrées et propose des paramètres de personnalisation (taille du code, niveau de correction d'erreur, marges) qui permettent leur adaptation à différents supports tels que les vêtements [63].

6. Chiffrement AES 128 bits : Sécurisation

Le système repose sur un chiffrement symétrique de type AES (Advanced Encryption Standard) 128 bits. Cette technique permet de sécuriser les données sensibles (identifiant du patient) encodées dans les QR codes. L'algorithme AES est reconnu dans le monde entier pour sa robustesse face aux attaques cryptographiques et pour garantir la confidentialité des informations qui y sont transmises [64] .

7. Environnement de développement – Outils utilisés

Plusieurs outils ont été mobilisés pour mettre en œuvre le développement et les tests. L'éditeur principal a sans nul doute été Visual Studio Code (VS Code) et ses extensions PHP, SQL et HTML. XAMPP a permis de simuler un environnement local Apache/PHP/MySQL pour le développement.

III.1.2 Implémentation du chiffrement AES

La sécurité des données sensibles au sein de notre système repose sur l'utilisation de l'algorithme AES (Advanced Encryption Standard), dans sa version AES-256-CBC, un standard recommandé par le NIST (National Institute of Standards and Technology) et largement utilisé dans des systèmes sécurisés gouvernementaux, bancaire et médical [65].

Le chiffrement est fait via le mode CBC (Cipher Block Chaining) qui introduit du chaînage entre blocs permettant d'atteindre une sécurité supérieure à celle offerte par le mode ECB (Electronic Code Book). En effet, pour le mode CBC, un vecteur d'initialisation (IV) unique est utilisé pour chacune des opérations de chiffrement ce qui rend impossible la réalisation d'attaques par répétition ou d'analyses statistiques, et ce même si les données d'entrée sont identiques [66].

III.1.3 Génération et personnalisation des QR codes

Dans un souci de repérage rapide et sécurisé des patients souffrants de la maladie d'Alzheimer, chaque fiche patient est affectée à un QR code d'identification qui contient ses données chiffrées et qui est ensuite imprimé sur un objet porté par le patient, au choix, une casquette , un T-shirt personnalisé, dont la fonction est d'assurer son identification et sa localisation en cas de perte ou d'errance.

- Génération des QR code

La génération des QR code est effectuée côté serveur via la bibliothèque PHP QR Code, une bibliothèque open-source permettant de produire des QR codes au format image (PNG, SVG) [1]. Chaque QR code contient une chaîne de caractères encodée en Base64 résultant d'un chiffrement AES-256-CBC des données sensibles (ID, téléphone…).

-Personnalisation des QR codes

En vue de favoriser la lisibilité et d'inscrire le QR code dans une identité visuelle choisie :
Le logo de l'application RANI MAAK peut être intégré au centre du QR code .
Les couleurs du QR peuvent être adaptées (ex. : fond blanc, motif mouve) au fond du support textile tout en garantissant la lisibilité.
La taille sera choisie en fonction des supports physiques (minimum recommandé : 20 x 20 cm).
Ces personnalisations sont effectuées à l'aide d'outils tiers comme QR Code Studio ou par le

biais de scripts JavaScript (si traitement client-side) tout en conservant un taux de lecture élevés.

-Sécuité et authenticité

La spécificité à chantier code QR est ajoutée même pour chaque casier, au moment du chiffrement, sera généré un IV aléatoire, et ainsi la réédition (changement de t-shirt ou de mise à jour de données) génère automatiquement un nouveau QR code, ce qui rend impossible la production ou la falsification par un tiers.

III.2 Développement de l'application mobile

L'élaboration de l'application mobile apparaît comme une partie fondamentale du système proposé, conçu pour renforcer la sécurité des patients souffrant de la maladie d'Alzheimer. Cette application à partir de l'environnement Androïde, permet la lecture d'un QR code encrypté, la géo localisation de l'utilisateur et la transmission automatique d'un message d'alerte à un proche. L'ambition est de proposer une solution intuitive, sécurisée et efficace, opérationnelle en situation critique.

III.2.1 Technologies utilisées

Les prises de décisions quant aux technologies utilisées ont porté leur choix sur des outils reconnus pour leur fiabilité, leur compatibilité avec les systèmes procédant du monde d'Androïde, mais également en phase avec les besoins exprimés par le projet :

1-Android Studio : représente le cadre de développement intégré idoine pour les applications Android, prôné par Google. Le développement ne peut se faire en dehors du cadre IntelliJ IDEA, car il se fonde sur cette plateforme établie en bon père de famille, et offre l'ensemble des outils nécessaires à la conception, au débogage, à l'émulation, à la compilation et à la publication d'une application Android [67]. Il intègre également le système de build Gradle et l'éditeur de code intelligent qui va bien, sans oublier l'émulateur d'applications, sans compter l'intégration de bibliothèques tierces (ex : ZXing pour les QR codes, ou Google Location Services pour la géolocalisation). Son interface invitante et ses outils de profiling permettront le suivi des performances de son application mobile au petit oignon.

2-Java : Le langage Java a été le choix de base pour le développement natif de l'application Android. Il est totalement pris en charge par Android Studio, a de bonnes capacités de gestion

des threads (favorables aux tâches asynchrones, comme l'accès réseau ou la géolocalisation) et est bien documenté dans une large communauté, à travers de multiples bibliothèques [68].

3-ZXing (Zebra Crossing) :ZXing est une bibliothèque open source développée elle aussi en Java, destinée à la génération et à la lecture de codes-barres 1D/2D, donc de QR codes. En étant intégrée à l'application à l'aide d'un Intent personnalisé, elle permet le scan rapide et fiable des QR codes chargés de données chiffrées [69].

4-L'API Google Location Services : Cette API fournie par Google donne accès aux informations de localisation, c'est-à-dire d'où proviennent la localisation du patient précise à la « cartographie » du lieu grâce à la combinaison de plusieurs sources : GPS, Wi-Fi, antennes de téléphonie mobile, etc. Elle permet de récupérer en temps réel la position du patient avec un maximum de précision. La localisation ainsi récupérée est intégrée tant dans le message d'alerte que dans l'enregistrement dans la base de données distante [70].

5-SmsManager Android : La classe SmsManager est utilisée pour automatiser l'envoi du message d'alerte. L'application peut donc envoyer un SMS de façon programmée, sans intervention manuelle. Ceci est très important pour les situations d'urgence, où le patient n'est plus en mesure d'agir [71].

6-Connexion vers serveur de stockage distant (PHP/MySQL) :
L'application mobile échangera avec la base de données à distance via des requêtes HTTP envoyées à des scripts PHP, étant eux-mêmes hébergés sur un serveur, celui-ci étant lui-même connecté à une base de données (MySQL) qui est la seule interface vers le stockage distant. Dans cette couche appelée backend se trouve l'organisation, le stockage des alertes envoyées, les authentifications pour accéder à l'interface administrateur et à l'historique, …

III.2.2 Fonctionnalités Clés

La création de l'application RANI MAAK vise à fournir à ses utilisateurs un ensemble suffisant de fonctions nécessaires à la sécurité des patients Alzheimer, tout en assurant la facilité de son utilisation et l'efficacité dans un cadre critique. Les fonctionnalités principales mises en œuvre sont :

1-Lire des QR codes encryptés. À l'aide de la bibliothèque ZXing, l'utilisateur peut scanner un code QR prêté au patient. Le code à QR code est censé transporter des informations sensibles (ID, numéro de contact) aussi encryptées en AES-256.

2-Déchiffrement local sécurisé des données. Une fois scanné le QR code, l'application procède par l'algorithme AES (Advanced Encryptions Standard) en mode CBC au déchiffrement des données localement, ce qui assure la confidentialité des données .
3-Récupération de la position GPS : L'application sollicite le service de localisation du Smartphone (GPS, Wifi, antennes cellulaires) afin d'obtenir la position géographique du patient avec précision .

4-Envoi automatique d'un SMS d'alerte : Un message contenant la position courante et le lien Google Maps est automatiquement envoyé au numéro de téléphone du tuteur/parent. Il permet de réagir rapidement en cas de fugue ou perte.
5-Archivage sur une plateforme serveur des alertes : En parallèle, les informations relatives à l'événement (ID patient, heure, position) sont transmises à un serveur distant en PHP/MySQL pour archivage et consultation ultérieure.

III.3 Base de données et plateforme d'alerte

III.3.1 Modèle de données

Le modèle de la base de données de l'application repose sur trois tables principales, étroitement interconnectées afin de garantir la cohérence de l'information, mais également le suivi des événements critiques. La table **patients** contient des informations relatives aux personnes suivies, leurs identifiants, mais également le QR code chiffré contenant les coordonnées du contact d'urgence à prévenir en cas de situation critique. La table **users** concerne la gestion des comptes administrateurs ou des tuteurs accédant à la plateforme web ; des identifiants, noms d'utilisateur et mots de passe y sont stockés sous forme hachée afin d'assurer un accès sécurisé. Enfin, la table **trace** répond au besoin systémique de la surveillance en tant qu'historique des alertes générées par l'application mobile. Chacune des lignes qui composent cette table intègre l'identification du patient concerné, ses coordonnées géographiques (latitude et longitude) exactes, la date et l'heure de l'alerte, et un champ statut. Ce champ est particulièrement important dans le dispositif de suivi du traitement de l'alerte, en ce sens que l'alerte générée automatiquement par l'application, est inscrite sur l'événement avec un statut "en_attente", puis ce statut est requalifié à "réalisée" lorsque l'intervenant, administrateur de l'application, a pris, par l'interface web consultée, en charge l'alerte. Ce mécanisme contribue donc à contrôler la réactivité des intervenants, permet de réaliser des statistiques sur ce qui est pris en charge dans des délais, tout en permettant la traçabilité de chaque éventuelle intervention.

III.3.2 Gestion des alertes et des localisations

Le processus de gestion des alertes s'effectue dans le cadre de l'interface entre l'application mobile et le serveur distant. Quand un patient est géolocalisé via le scan du QR code, l'application se charge de : récupérer les coordonnées GPS du patient, déchiffrer les données du QR, puis de générer et transmettre automatiquement un SMS d'alerte au contact d'urgence en lui communiquant la position GPS du patient. La QR et les données (id patient,

position, horodatage) sont également envoyées sur le serveur via un script php pour stockage dans la table trace, avec le statut “en attente”.

Cette interface web permet aux administrateurs de consulter les alertes en temps réel. Ainsi, lorsque l’alerte est prise en charge, l’administrateur a la possibilité de changer le statut de l’alerte à « réalisée ». Cela garantit une réactivité efficace dans le cadre d’un suivi rigoureux et d’une traçabilité à chaque étape des situations difficiles à traiter.

III.4 Intégration et tests

III.4.1 Tests unitaires et fonctionnels

Des tests unitaires ont été effectués sur chaque module Java de l’application mobile : lecture de QR code, déchiffrement AES, envoi de SMS, accès GPS, communication avec l’API serveur. Les tests fonctionnels ont été réalisés à partir de cas d’usage réels, simulant des scénarios d’alerte avec des patients fictifs, et en milieu urbain. Tous les modules ont répondu de façon cohérente et rapide (<3 secondes entre le scan et l’envoi de l’alerte).

III.4.2 Tests d’ergonomie et d’usage

Une série d’évaluations ergonomiques a eu lieu avec des utilisateurs non techniques (25 à 65 ans). Les objectifs étaient de mesurer la facilitation de l’accès, la lisibilité de l’interface (taille et contraste des textes) et le taux de succès sans aide. Le taux de succès mesuré est de 94% avec des remarques favorables sur la simplicité du processus et le temps pris pour effectuer l’opération. Quelques ajustements sur la taille des boutons et la lisibilité du message ont été réalisés.

Conclusion Générale

IV CONCLUSION GENERALE:

En conclusion, ce projet de fin d'études a permis de mettre en place une solution innovante et sécurisée de prise en charge des patients atteints de la maladie d'Alzheimer. En effet, grâce à une base de données robuste, un chiffrement symétrique efficace de type AES, l'intégration de QR codes au sein des vêtements des patients, et le déploiement d'une application mobile permettant de scanner, localiser et transmettre, le système peut répondre aux enjeux de surveillance et d'alerte en situation d'urgence. Cette solution technologique permet d'offrir un cadre fiable pour sécuriser la vulnérabilité des personnes tout en préfigurant une réponse efficace de leurs proches ou des professionnels de santé.

Néanmoins, plusieurs orientations de progrès peuvent être envisagées. En dépit d'une bonne sécurisation actuelle des données sensibles par le chiffrement AES, l'adoption future d'un chiffrement asymétrique du type RSA ou ECC permettrait une gestion plus sécurisée des clés de chiffrement , notamment lors de leur transport. De même, le recours à des méthodes de géo localisation hybrides (qui combinent GPS, Wifi et réseaux de téléphonie mobile) pourrait permettre d'améliorer la précision de la localisation, notamment en milieu urbain dense ou dans les zones mal couvertes. Enfin, la création d'une version multiplateforme (incluant iOS) de l'application mobile, et l'exploration de technologies complémentaires telles que les QR Codes dynamiques ou les balises NFC pourraient encore renforcer la robustesse et l'adaptabilité du dispositif.

Pour finir, au-delà de ses caractéristiques techniques, le projet comporte un fort potentiel d'impact social. Il offre une réponse concrète, adaptée aux enjeux de santé publique : la protection des patients présentant des troubles cognitifs. Il facilite l'identification immédiate des individus, alerte en temps réel les référents et permet enfin une localisation précise, contribuant à apaiser les familles et à améliorer la vie du patient. Ce dispositif pourrait aussi, à terme, permettre la prise en charge d'autres publics en situation de vulnérabilité, tels que les enfants autistes, ou les personnes âgées isolées, en devenant un vecteur d'innovation pour la sécurité, la santé, la solidarité.

Annexe

V Annexe

2-Outils de développement et liens d'installation

Android Studio

Environnement de développement officiel pour Android. Il permet de concevoir, tester et compiler des applications Android . Lien de l'installation :

https://developer.android.com/studio

Java JDK

Kit de développement Java utilisé pour coder l'application

Mobile Android. Lien de l'installation :

https://www.oracle.com/java/technologies/javase-downloads.html

PHP

Langage de programmation côté serveur pour gérer la communication avec la base de données.

https://www.php.net/downloads.php

Annexe

XAMPP

Serveur local regroupant Apache, MySQL, PHP et phpMyAdmin. Permet de tester le backend en local.

https://www.apachefriends.org/fr/index.html

MySQL Workbench

Outil graphique de conception, requêtage et gestion de la base de données MySQL.

https://dev.mysql.com/downloads/workbench/

Visual Studio Code

Éditeur de code léger et extensible pour le développement PHP, JavaScript et HTML.

https://code.visualstudio.com/

2-Outil de Conception des Diagrammes UML

PlantUML

Outil en ligne gratuit permettant de créer des diagrammes UML à partir d'un langage texte simple.

https://www.plantuml.com/plantuml/uml

3-Logos utilisés dans le projet

-Logo officiel de l'application RANI MAAK

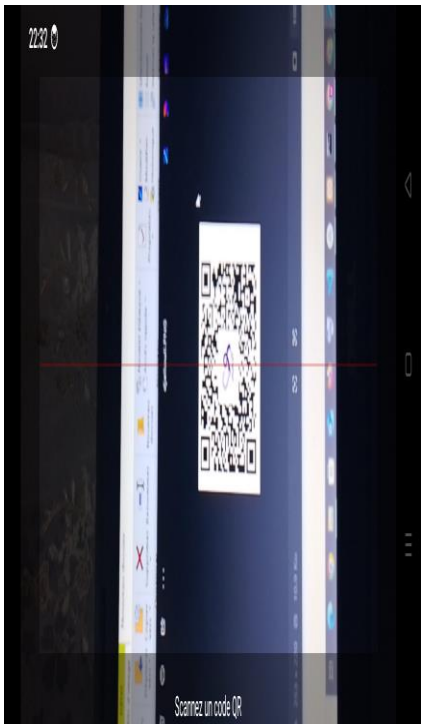
-Logo symbolique de QR Code

4-Captures d’écran des interfaces (Prototype)

1-Interfaces de l’application mobile “RANI MAAK”

Interface1

Interface2

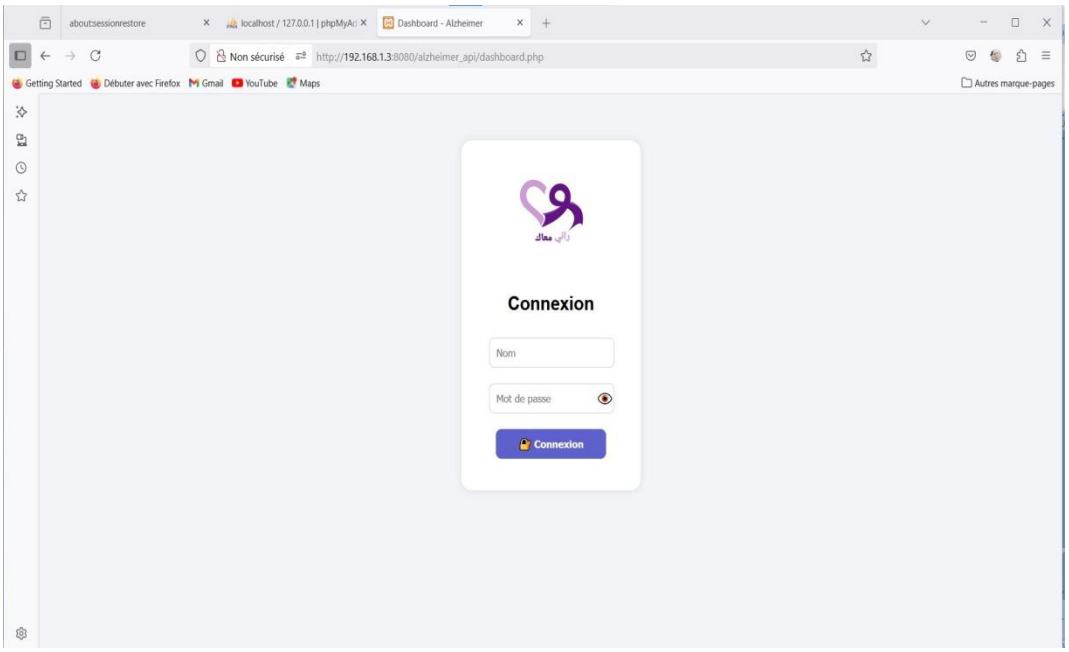


Interface3

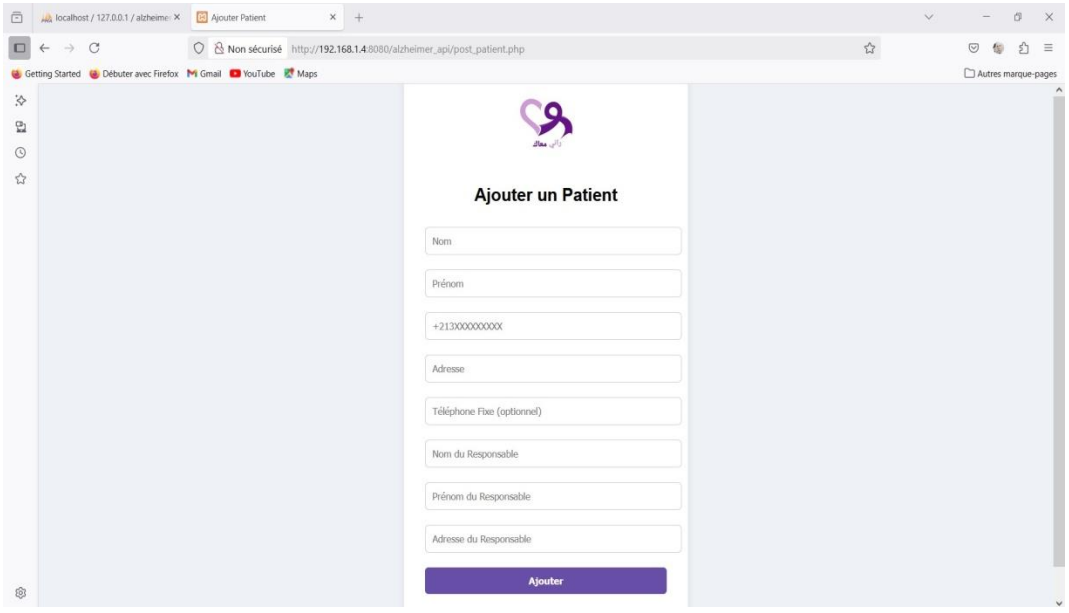
Interface4

Interface5

2-Interfaces de la plateforme web

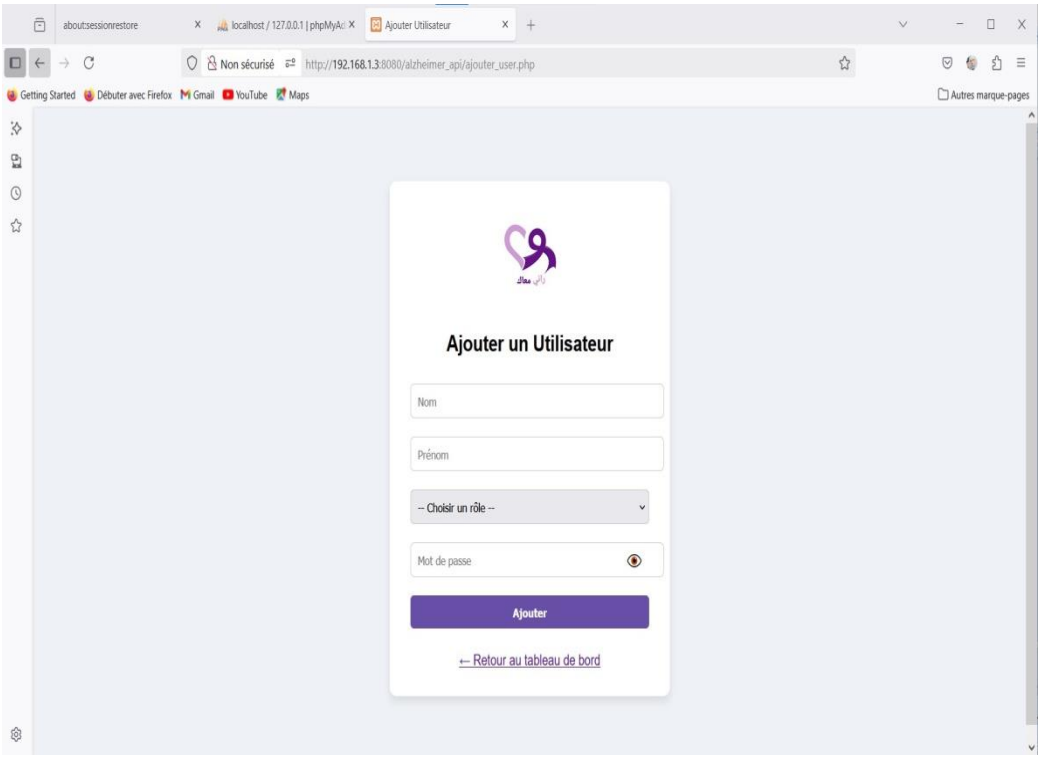


Interface pour établir la connexion pour accéder a d'autre page

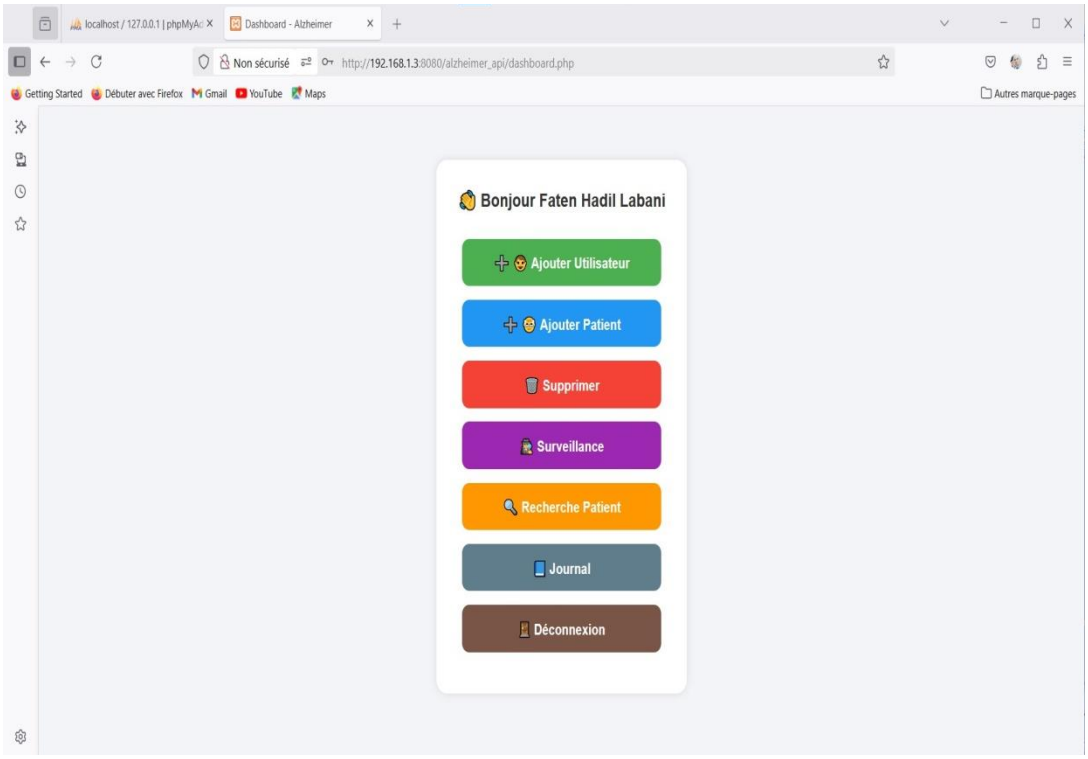


Interface pour ajouter un patient

Annexe

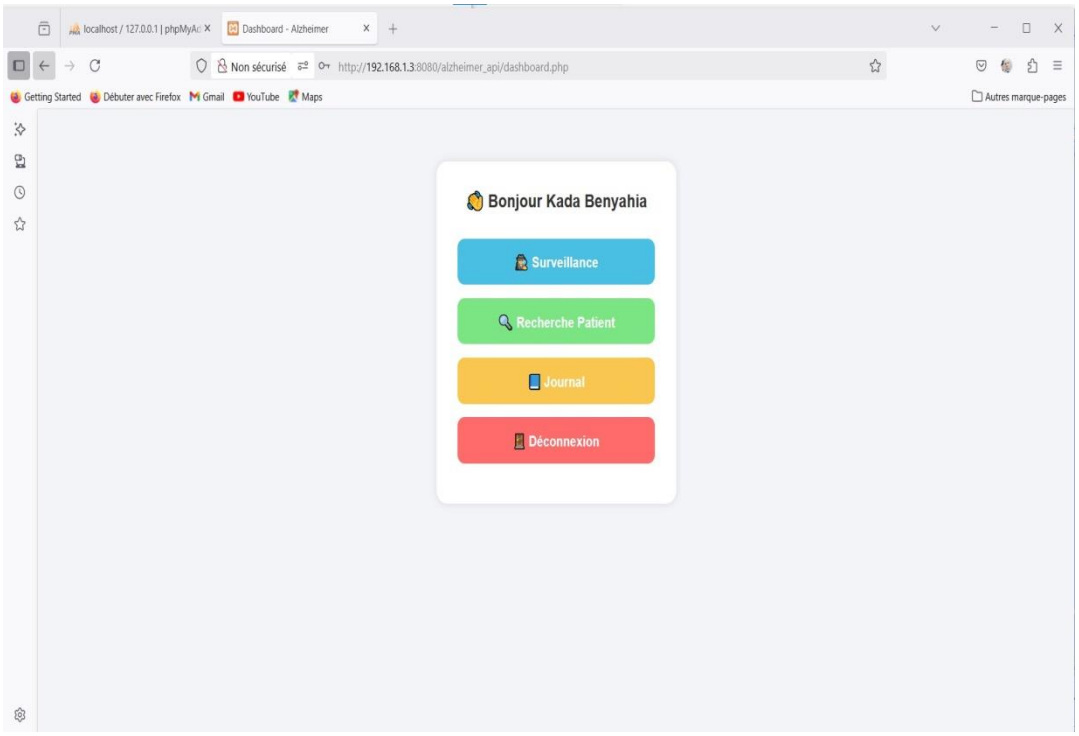


Interface pour ajouter un utilisateur Admin ou Associateur

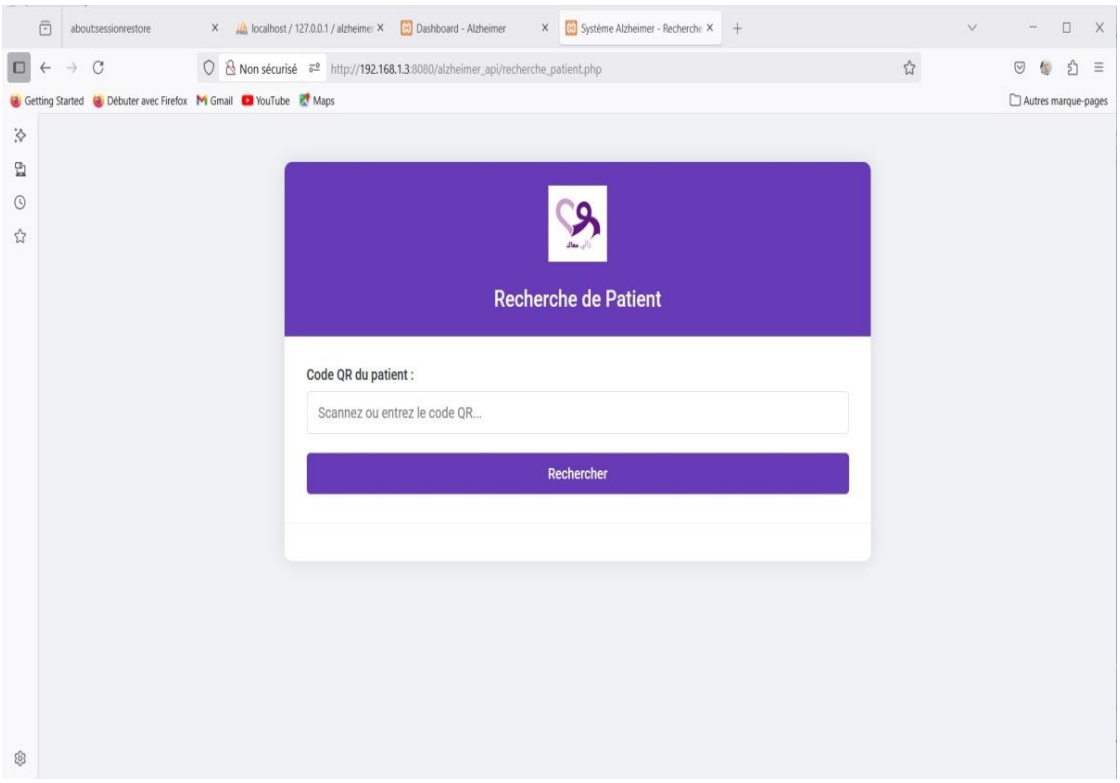


Interface de tableaux de bord de utilisateur Admin

Annexe

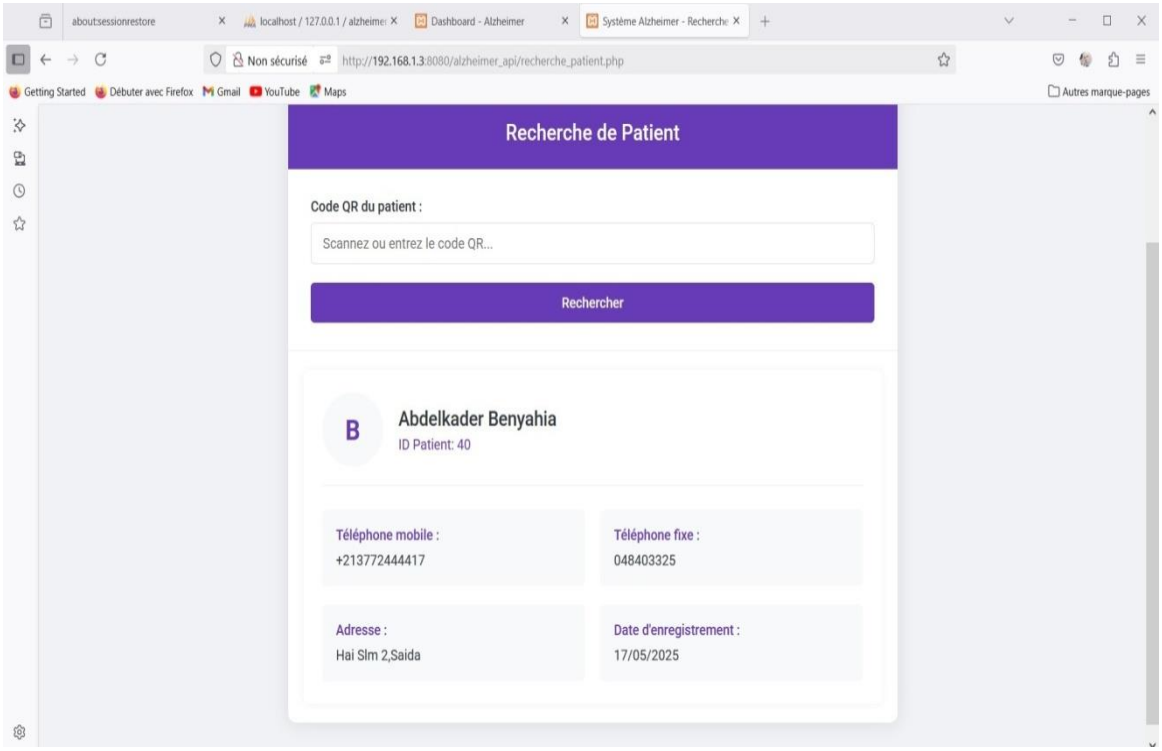


Interface de tableaux de bord de utilisateur Associateur

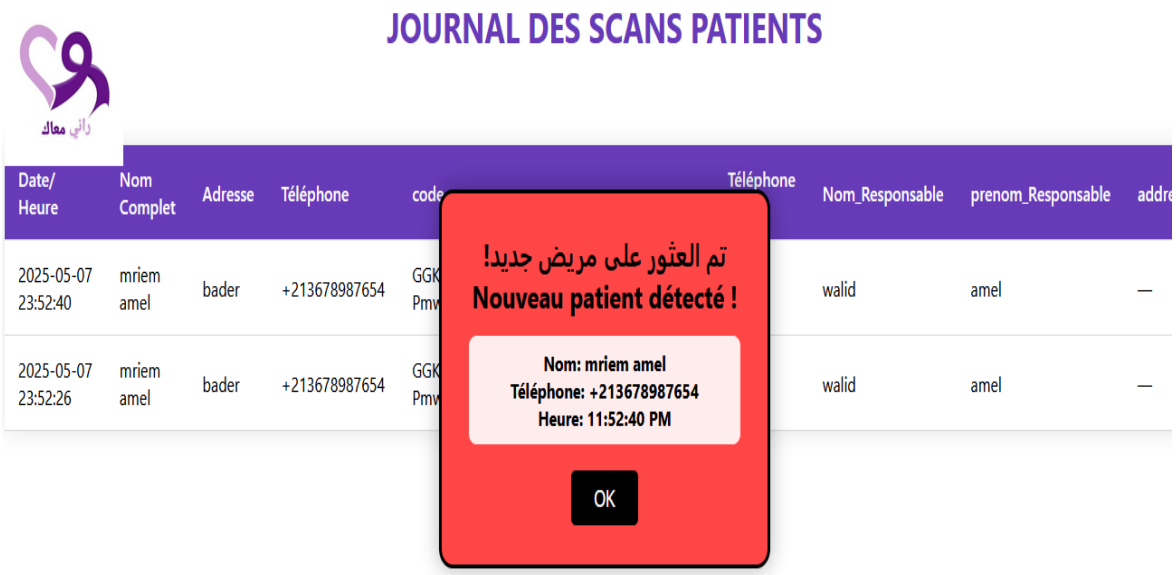


Interface pour rechercher un patient

Annexe



Interface pour rechercher un patient avec ces informations



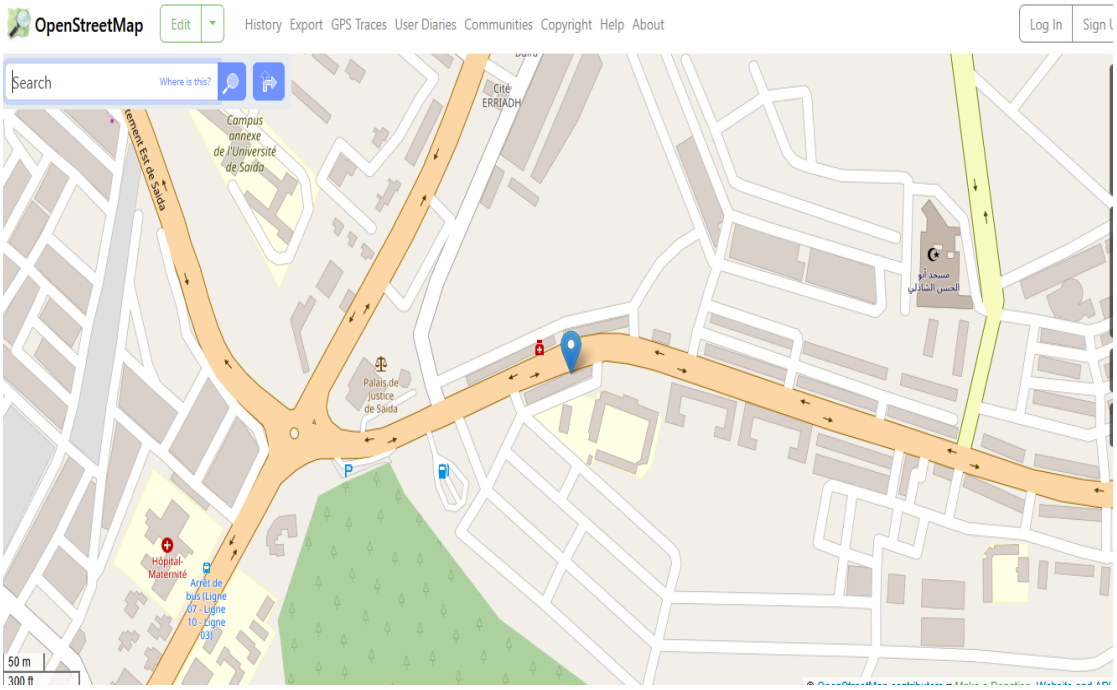
Interface de journal des scans patients

Annexe

JOURNAL DES SCANS PATIENTS

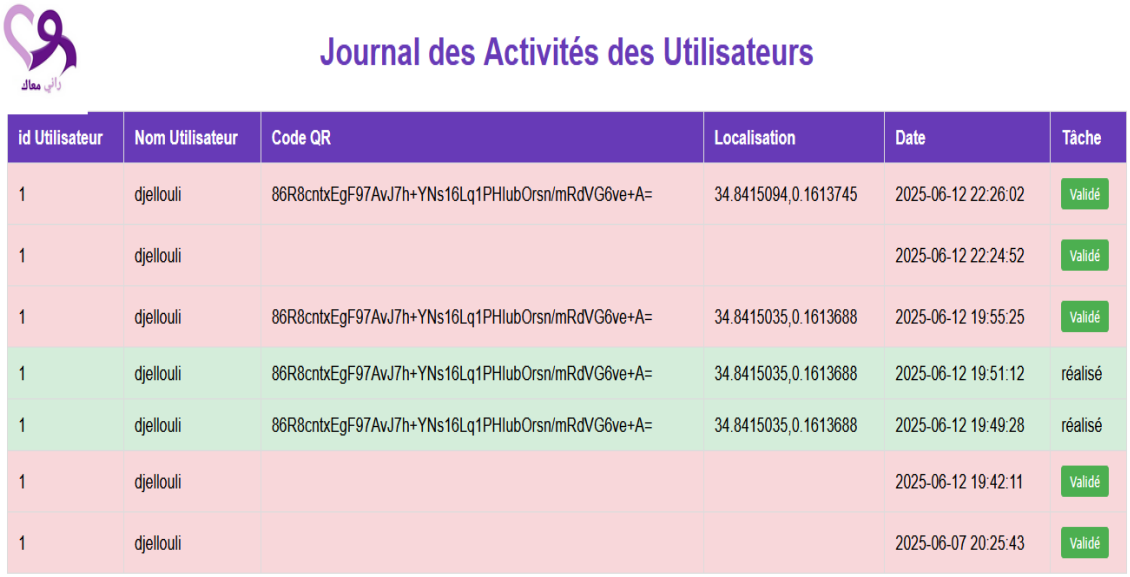
esse	Téléphone	code_qr	Téléphone Fixe	Nom_Responsable	prenom_Responsable	addres_Responsable	Localisation	Actions
er	+213772444417	86R8cntxEgF97AvJ7h+YNs16Lq1PHIubOrsn/mRdVG6ve+A=	—	benyahia	kada	naser	Voir la carte	Validé
er	+213772444417	86R8cntxEgF97AvJ7h+YNs16Lq1PHIubOrsn/mRdVG6ve+A=	—	benyahia	kada	naser	Voir la carte	Validé

Interface de journal des scans patients



Interface de localisation sur google map

Annexe



Journal des Activités des Utilisateurs

id Utilisateur	Nom Utilisateur	Code QR	Localisation	Date	Tâche
1	djellouli	86R8cntxEgF97AvJ7h+YNs16Lq1PHlubOrsn/mRdVG6ve+A=	34.8415094,0.1613745	2025-06-12 22:26:02	Validé
1	djellouli			2025-06-12 22:24:52	Validé
1	djellouli	86R8cntxEgF97AvJ7h+YNs16Lq1PHlubOrsn/mRdVG6ve+A=	34.8415035,0.1613688	2025-06-12 19:55:25	Validé
1	djellouli	86R8cntxEgF97AvJ7h+YNs16Lq1PHlubOrsn/mRdVG6ve+A=	34.8415035,0.1613688	2025-06-12 19:51:12	réalisé
1	djellouli	86R8cntxEgF97AvJ7h+YNs16Lq1PHlubOrsn/mRdVG6ve+A=	34.8415035,0.1613688	2025-06-12 19:49:28	réalisé
1	djellouli			2025-06-12 19:42:11	Validé
1	djellouli			2025-06-07 20:25:43	Validé

Interface de journal des activités des utilisateurs pour

Garantir la traçabilité

Références bibliographiques

VI. REFERENCES BIBLIOGRAPHIQUES

[1] Commission Européenne. *Règlement Général sur la Protection des Données (RGPD)*. 2016. https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32016R0679

(consulté le 1 juin 2025).

[2] U.S. Department of Health & Human Services. *Health Insurance Portability and Accountability Act (HIPAA)*. 1996. https://www.hhs.gov/hipaa/index.html

(consulté le 1 juin 2025).

[3] Organisation mondiale de la santé (OMS). *Démence*. Fiche d'information, 2022. https://www.who.int/fr/news-room/fact-sheets/detail/dementia (consulté le 1 juin 2025).

[4] Daemen, J., & Rijmen, V. *The Design of Rijndael: AES - The Advanced Encryption Standard*. Springer, 2002. (consulté le 1 juin 2025).

[5] ISO/IEC 27799:2016 — Health informatics — Information security management in health. (consulté le 1 juin 2025).

[6] Union européenne, "Règlement (UE) 2016/679 – RGPD," 2016. (consulté le 1 juin 2025).

[7] U.S. Department of Health & Human Services, *Health Insurance Portability and Accountability Act of 1996 (HIPAA).* (consulté le 2 juin 2025).

[8] CNIL (Commission Nationale de l'Informatique et des Libertés). (s.d.). Passer à l'action en 4 étapes - RGPD. [Illustration]. Consulté le 14 juin 2025, depuis : https://www.cnil.fr/fr/rgpd-par-ou-commencer (consulté le 14 juin 2025).

[9] Règlement (UE) 2016/679 du Parlement européen et du Conseil, 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel (RGPD), https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32016R0679

(consulté le 2 juin 2025).

[10] CNIL. (2023). Le principe de minimisation des données, https://www.cnil.fr/fr/minimisation-des-donnees. (consulté le 2 juin 2025).

[11] CNIL. (2022). *La sécurité des données personnelles*, https://www.cnil.fr/fr/securite.

(consulté le 2 juin 2025).

[12] FasterCapital. (s.d.). *Exporter vos données HIPAA en 4 étapes* [Infographie]. Disponible sur : https://fastercapital.com/fr (consulté le 2 juin 2025).

[13] CNIL. (2021). *Le principe de minimisation des données*. https://www.cnil.fr(consulté le 2 juin 2025).

Références bibliographiques

[14] HL7 International. (2022). *FHIR Overview.* https://www.hl7.org/fhir/overview.html(consulté le 3 juin 2025).

[15] U.S. Department of Health and Human Services (HHS). (2020). HIPAA Security Rule. https://www.hhs.gov/hipaa/for-professionals/security/index.html (consulté le 3 juin 2025).

[16] ISO/IEC 27002:2022. *Information security, cybersecurity and privacy protection — Code of practice for information security controls*. (consulté le 3 juin 2025).

[17] Menezes, A., van Oorschot, P., & Vanstone, S. *Handbook of Applied Cryptography*, CRC Press, 1996. (consulté le 4 juin 2025).

[18] Daemen, J., & Rijmen, V. (2002). *The Design of Rijndael: AES—The Advanced Encryption Standard*. Springer. (consulté le 4 juin 2025).

[19] Stallings, W. (2020). *Cryptography and Network Security: Principles and Practice* (8th ed.). Pearson. (consulté le 5 juin 2025).

[20] NIST, *Announcing the Advanced Encryption Standard (AES)*, FIPS PUB 197, 2001. (consulté le 6 juin 2025).

[21] Malekal. *Chiffrer un disque ou systèmes de fichiers : quelles différences ?* [en ligne]. Malekal.com, 2023. Disponible sur : https://www.malekal.com/chiffrer-un-disques-ou-systemes-fichiers-differences/ (consulté le 6 juin 2025).

[22] Paar, C., & Pelzl, J. *Understanding Cryptography*, Springer, 2009. (consulté le 6 juin 2025).

[23] Denso Wave Incorporated. (2020). *QR Code Essentials*. https://www.qrcode.com

(consulté le 7 juin 2025).

[24] ISO/IEC 18004:2015. *Information technology — Automatic identification and data capture techniques — QR Code bar code symbology specification.* (consulté le 7 juin 2025).

[25] European Union Agency for Cybersecurity (ENISA). (2021). *Guidelines for securing sensitive health data transmission.* https://www.enisa.europa.eu (consulté le 7 juin 2025).

[26] Daemen, J., & Rijmen, V. (2002). *The Design of Rijndael: AES — The Advanced Encryption Standard*. Springer. (consulté le 7 juin 2025).

[27] NIST. (2001). Federal Information Processing Standards Publication 197 (FIPS PUB 197): Specification for the Advanced Encryption Standard (AES). (consulté le 8 juin 2025).

[28] Abdul-Jabbar, S. S., & Farhan, A. K. (2023). *Secure QR-Code Generation in Healthcare*. ResearchGate. Lien (consulté le 8 juin 2025).

[29] Lin, C. et al. (2021). *QR Code Applications in Healthcare: A Review*. Journal of Medical Systems, 45(3). (consulté le 8 juin 2025).

Références bibliographiques

[30] L. Dupont. (2020). *QR Codes in Emergency Medicine: Rapid Identification Tools*. Revue Médecine Urgence. (consulté le 9 juin 2025).

[31] ISEE Corporation. *Site officiel – Solutions de sécurité, identification et alertes médicales par QR Code*. [en ligne]. Disponible sur : https://www.isee-corporation.com (consulté le 14 juin 2025). (consulté le 9 juin 2025).

[32] ICE Medical Cards. (2023). www.icemedicalcards.com (consulté le 9 juin 2025).

[33] Commission européenne. (2021). *EU Digital COVID Certificate*. ec.europa.eu

(consulté le 10 juin 2025).

[34] Commission européenne. *Certificat numérique COVID de l'UE*. [en ligne]. Bruxelles : Union européenne, 2021. Disponible sur : https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/safe-covid-19-vaccines-europeans/eu-digital-covid-certificate_fr (consulté le 10 juin 2025).

[35] Takahashi, Y., & López, M. (2023). *QR-Based Tracking for Alzheimer's Patients: Case Studies in Japan and Spain*. HealthTech Journal, 12(4). (consulté le 10 juin 2025).

[36] **SafeBandd.** (2024). *Code QR de sport bracelet – Bracelet d'identification personnel avec QR code à scanner*. Etsy. https://www.etsy.com/fr/listing/1777147214/code-qr-de-sport-bracelet (consulté le 10 juin 2025).

[37] B. Nguyen et al. (2022). *Location-Based Health Monitoring Systems for Elderly Care*. IEEE Communications Surveys & Tutorials. (consulté le 11 juin 2025).

[38] European GNSS Agency. (2021). *GNSS User Technology Report*. www.gsa.europa.eu

(consulté le 11 juin 2025).

[39] A. Rahman, M., & Huang, Y. (2020). *GSM-based Positioning Techniques for Low-Infrastructure Areas*. Mobile Networks Journal, 18(2). (consulté le 11 juin 2025).

[40] S. Amiri, & Chikhaoui, B. (2019). *Indoor Positioning Using Wi-Fi Fingerprinting: Challenges and Solutions* Sensors, 19(20). (consulté le 11 juin 2025).

[41] Google. (2021). *Fused Location Provider API Documentation*. developers.google.com

(consulté le 11 juin 2025).

[42] Alert1. *On-the-Go with Fall Detection Medical Alert Pendant*. [en ligne], consulté le 12 juin 2025.

Références bibliographiques

[43] Mauldin, T. R., Canby, M. E., Metsis, V., Ngu, A. H. H., & Rivera, C. C. (2018). *SmartFall: A smartwatch-based fall detection system using deep learning*. *Sensors*, 18(10), 3363. https://doi.org/10.3390/s18103363 (consulté le 12 juin 2025).

[44] Custódio da Silva, A., Rodrigues, W. de S., Gonçalves, B. P., da Cruz, M. A., Gomes, R. P., & de Alencar, D. B. (2020). *Locator Bracelet with QR Code for Elderly People with Alzheimer's*. *International Journal of Advanced Engineering Research and Science (IJAERS)*, 7(6), 81-86. ijaers.com (consulté le 12 juin 2025).

[45] Emish, M., Haroon, N., & Iqbal, R. (2023). *Real-Time Health Monitoring using mHealth Apps: A Review on Privacy and Compliance Challenges*. *Computers in Biology and Medicine*, 155, 106579. https://doi.org/10.1016/j.compbiomed.2023.106579 (consulté le 12 juin 2025).

[46] Ehn, M., et al. (2021). *Safety in elder care through geofencing and location tracking: User experience of digital monitoring*. *BMC Geriatrics*, 21, 611. https://doi.org/10.1186/s12877-021-02586-y (consulté le 13 juin 2025).

[47] Labani Faten Hadil, Architecture d'un système mobile de géo localisation et d'alerte pour patients Alzheimer utilisant QR code et chiffrement AES, Production personnelle dans le cadre du mémoire de Master 2 en Réseaux Informatiques et Systèmes Distribués, Université de Dr. Moulay Taher, 2025. (consulté le 13 juin 2025).

[48] Labani Faten Hadil, Modélisation UML du système d'assistance Alzheimer à base de QR code et géo localisation – Diagramme de cas d'utilisation, Production personnelle dans le cadre du mémoire de Master 2 en Réseaux Informatiques et Systèmes Distribués, Université Dr. Moulay Taher , 2025. (consulté le 14 juin 2025).

[49] Labani Faten Hadil et Djelloli nour el houda , Modélisation orientée objet de l'application mobile Alzheimer – Diagramme de classes UML, Réalisation personnelle dans le cadre du mémoire de fin d'études, Master 2 Réseaux Informatiques et Systèmes Distribués, Université Dr. Moulay Taher , 2025. (consulté le 14 juin 2025).

[50] Labani Faten Hadil et Djelloli nour el houda, Modélisation dynamique du système Alzheimer – Diagramme de séquence illustrant l'échange global d'informations entre les composants, Production personnelle dans le cadre du mémoire de Master 2 Réseaux Informatiques et Systèmes Distribués, Université Dr. Moulay Taher , 2025. (consulté le 14 juin 2025).

[51] Labani Faten Hadil , *Interface graphique de saisie des données des patients Alzheimer – Réalisation côté application Web sécurisée*, Réalisation personnelle dans le cadre du mémoire de Master 2 Réseaux Informatiques et Systèmes Distribués, Université Dr. Moulay Taher , 2025. (consulté le 14 juin 2025).

[52] Labani Faten Hadil , Conception de la base de données alzheimer_db – Structure de la table patients, Réalisation personnelle dans le cadre du mémoire de Master 2 Réseaux Informatiques et Systèmes Distribués, Université Dr. Moulay Taher , 2025. (consulté le 14 juin 2025).

Références bibliographiques

[53] Encodage sécurisé des informations patients – Exemple de QR code avec données chiffrées et clé intégrée (AES-256-CBC), Réalisation personnelle dans le cadre du mémoire de Master 2 en Réseaux Informatiques et Systèmes Distribués, Université Dr. Moulay Taher ,2025. (consulté le 14 juin 2025).

[54] Labani Faten Hadil, Illustration d'un support physique pour QR code – Exemple de pull et casquette adaptés aux patients Alzheimer, Conception personnelle dans le cadre du mémoire de Master 2 Réseaux Informatiques et Systèmes Distribués, Université Dr. Moulay Taher ,2025. (consulté le 14 juin 2025).

[55] Labani Faten Hadil et Djelloli nour el houda , *Prototype de t-shirt personnalisé pour patients Alzheimer – Intégration d'un QR code chiffré avec logo pour une identification rapide en milieu extérieur*, Réalisation personnelle dans le cadre du mémoire de Master 2 en Réseaux Informatiques et Systèmes Distribués, Université Dr. Moulay Taher, 2025. (consulté le 14 juin 2025).

[56] Labani Faten Hadil et Djelloli nour el houda , Système d'alerte pour patients Alzheimer – Exemples de messages SMS envoyés automatiquement en mode hors ligne et connecté, Conception personnelle dans le cadre du mémoire de Master 2 en Réseaux Informatiques et Systèmes Distribués, Université Dr. Moulay Taher , 2025. (consulté le 14 juin 2025).

[57] Labani Faten Hadil et Djelloli nour el houda , *Système de traçabilité des alertes – Exemple d'enregistrement d'un scan de patient dans le journal des événements*, Réalisation personnelle dans le cadre du mémoire de Master 2 en Réseaux Informatiques et Systèmes Distribués, Université Dr. Moulay Taher , 2025. (consulté le 14 juin 2025).

[58] Labani Faten Hadil, Modélisation du processus de géo localisation – Diagramme d'activité décrivant la transmission de la position du patient à la plateforme de surveillance, Réalisation personnelle dans le cadre du mémoire de Master 2 en Réseaux Informatiques et Systèmes Distribués, Université Dr. Moulay Taher , 2025. (consulté le 14 juin 2025).

[59] Larose, D. (2021). *Programmation PHP 8: Principes de base, programmation orientée objet, bonnes pratiques et nouveautés*. Éditions ENI. (consulté le 15 juin 2025).

[60] Paul DuBois. (2020). *MySQL, 5th Edition: The Definitive Guide to Using, Programming, and Administering MySQL 8*. O'Reilly Media. (consulté le 15 juin 2025).

[61] Freeman, E., & Robson, E. (2018). *Head First HTML and CSS (2nd Edition)*. O'Reilly Media. (consulté le 15 juin 2025).
Flanagan, D. (2020). *JavaScript: The Definitive Guide (7th Edition)*. O'Reilly Media.

(consulté le 15 juin 2025).

[62] Masse, M. (2011). *REST API Design Rulebook: Designing Consistent RESTful Web Service Interfaces*. O'Reilly Media. (consulté le 15 juin 2025).

Références bibliographiques

[63] Mikowski, M., & Powell, J. C. (2013). *Single Page Web Applications: JavaScript end-to-end*. Manning Publications. (consulté le 15 juin 2025).
(Contient des exemples de bibliothèques de génération dynamique, dont les QR codes).

[64] National Institute of Standards and Technology (NIST). (2001). *Advanced Encryption Standard (AES)*. FIPS Publication 197.
https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf (consulté le 16 juin 2025).

[65] National Institute of Standards and Technology (NIST). (2001). *Advanced Encryption Standard (AES)*. FIPS Publication 197.
https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf (consulté le 16 juin 2025).

[66] Stallings, W. (2017). *Cryptography and Network Security: Principles and Practice* (7th ed.). Pearson Education.
(Chapitre sur les modes de fonctionnement des algorithmes de chiffrement symétrique, notamment CBC vs ECB) (consulté le 16 juin 2025).

[67] Google Developers. (2023). *Android Studio User Guide*. Google Inc.
https://developer.android.com/studio/ (consulté le 16 juin 2025).

[68] Eckel, B. (2017). *Thinking in Java* (4th ed.). Prentice Hall. (consulté le 16 juin 2025).

[69] ZXing Project. (2022). *Zebra Crossing (ZXing) – Official GitHub Repository*.
https://github.com/zxing/zxing (consulté le 16 juin 2025).

[70] Google Developers. (2023). *Location APIs - Fused Location Provider*.
https://developer.android.com/training/location (consulté le 16 juin 2025).

[71] Android Developers. (2023). *Sending SMS with SmsManager*.
https://developer.android.com/reference/android/telephony/SmsManager (consulté le 16 juin 2025).

ملخص

يقدّم هذا المشروع تطبيق راني معك على نظام أندرويد، لتعزيز السلامة الشخصية. يسمح التطبيق بمسح رموز QR المشفرة، فك تشفير معلومات الاتصال في حالات الطوارئ، تحديد الموقع الجغرافي وإرسال رسائل نصية تلقائية. كما يُسجل التنبيهات على خادم PHP/MySQL. أظهرت التجارب فعاليته في الاستجابة السريعة للطوارئ.

الكلمات المفتاحية: راني معك، تطبيق أندرويد، السلامة الشخصية، رمز QR، تشفير AES، تحديد الموقع، رسالة SMS

Abstract

This Project introduces RANI MAAK, an Android application that enhances personal safety by enabling users to scan encrypted QR codes, decrypt emergency contact details, capture GPS location, and send automated SMS alerts. It also logs incidents to a remote PHP/MySQL server. Combining AES encryption, geolocation, and QR scanning, the app proves effective in real-world tests for quick emergency response.

Keywords: RANI MAAK, Android app, safety, QR code, AES, geolocation, SMS

Résumé

Ce projet présente RANI MAAK, une application Androïde visant à renforcer la sécurité personnelle. Elle permet de scanner des QR codes chiffrés, de décrypter les contacts d'urgence, d'obtenir la position GPS en temps réel et d'envoyer des alertes SMS automatiques. Un système d'enregistrement distant via PHP/MySQL est aussi intégré. Les tests confirment son efficacité en situation d'urgence.

Mots-clés : RANI MAAK, application Androïde, sécurité personnelle, QR code, chiffrement AES, géo localisation, SMS