

UNIVERSITÉ LIBRE DES PAYS DES GRANDS LACS

FACULTE DE SCIENCES ET TECHNOLOGIES

DEPARTEMENT DE GENIE ELECTRIQUE ET INFORMATIQUE



BP. 368 GOMA

www.ulpgl.net

**CONCEPTION ET IMPLÉMENTATION D'UNE
APPLICATION WEB PARTICIPATIVE DE
SIGNALEMENT DES INCIDENTS SÉCURITAIRES A
GOMA BASÉE SUR LA GÉOLOCALISATION**

Par **MAKENGU MUSAFIRI**

Travail présenté en vue de l'obtention du Diplôme de
Bachelor en Sciences de l'Ingénieur

Option : Génie Informatique

Directeur : Prof. **BARAKA Olivier MUSHAGE**

Encadreur : MSc. Yvette KALIMUMBALO

ANNEE ACADEMIQUE 2024 - 2025

Dédicace

À tous ceux qui ont cru en moi.

Epigraphe

« Le monde ne sera pas détruit par ceux qui font le mal, mais par ceux qui les regardent sans rien faire. »

Albert Einstein

Remerciements

La concrétisation de ce projet n'aurait pas été possible sans le soutien précieux de nombreuses personnes qui nous ont accompagnés à chaque étape. Nous commençons par rendre grâce à Dieu pour le don de la vie, son amour sans limites et sa protection bienveillante.

Nos remerciements les plus sincères vont à notre Directeur, le Professeur Baraka Mushage Olivier, ainsi qu'à notre encadreur, Msc. Yvette KALIMUMBALO, dont l'engagement et la disponibilité, malgré leurs obligations professionnelles chargées, ont été déterminants pour nous orienter, nous corriger et assurer la qualité de ce travail.

À nos chers parents, robert MUSAFIRI TOTO, sifa FAIDA CIROYI, MUSUZA MPARANYI Bertin, MUNYEREKANA MUSAFIRI aimée, janvier MUSHABISA, nous témoignons notre profonde gratitude pour leur soutien.

Enfin, une pensée chaleureuse va à tous nos amis et collègues pour leur amitié et les moments partagés. Une mention spéciale à VUNDE LUKENGU Gracien, KAZEINZELE CHIBANGU Célestin, MUGISA PANZA Emmanuel, AKSANTI BYALAHIRE François, ainsi qu'à toutes les personnes dont les noms ne figurent pas ici, mais dont l'appui a été d'une importance capitale.

MAKENGU MUSAFIRI Bénit

Résumé

Ce travail de recherche propose la conception et l'implémentation de « GomaSecure », une application web participative (Progressive Web App) basée sur la géolocalisation pour signaler les incidents sécuritaires dans la ville de Goma. Face à l'inefficacité et aux dangers des méthodes d'alerte traditionnelles comme les cris et les sifflets, qui manquent de précision géographique et de traçabilité, cette plateforme permet aux citoyens de signaler rapidement un danger (vol, incendie, agression) en y joignant des preuves multimédias (audio, photo, vidéo) et des coordonnées GPS exactes. Afin de garantir la fiabilité des alertes et d'éviter les fausses informations, le système s'appuie sur un mécanisme de validation à deux niveaux : une modération communautaire par les résidents locaux et une vérification hiérarchique par des utilisateurs de confiance désignés comme « Sentinelles », avant la prise en charge par les autorités. Développée avec des technologies modernes telles que React.js, TypeScript, Supabase (PostgreSQL/PostGIS) et Leaflet, l'application intègre également un mode SOS silencieux pour les urgences vitales, offrant ainsi aux forces de sécurité un outil centralisé et interactif pour améliorer la coordination et la rapidité des interventions.

Mots-clés : GomaSecure, Sécurité urbaine, Signalement participatif, Géolocalisation, Crowdsourcing, Progressive Web App (PWA), Validation communautaire, Goma.

Abstract

This research work proposes the design and implementation of “GomaSecure”, a participatory web application (Progressive Web App) based on geolocation to report security incidents in the city of Goma. Facing the inefficiency and dangers of traditional alert methods such as shouting and whistling, which lack geographical precision and traceability, this platform allows citizens to quickly report a danger (theft, fire, assault) by attaching multimedia evidence (audio, photo or video) and exact GPS coordinates. To ensure the reliability of alerts and avoid misinformation, the system relies on a two-level validation mechanism: community moderation by local residents and hierarchical verification by trusted users designated as “Sentinels”, before being handled by the authorities. Developed with modern technologies such as React.js, TypeScript, Supabase (PostgreSQL/PostGIS), and Leaflet, the application also integrates a silent SOS mode for vital emergencies, providing security forces with a centralized and interactive tool to improve coordination and response speed.

Keywords: GomaSecure, Urban security, Participatory reporting, Geolocation, Crowdsourcing, Progressive Web App (PWA), Community validation, Goma.

Table des matières

Dédicace.....	i
Epigraphe	i
Remerciements.....	ii
Résumé.....	iii
Table des matières	v
Liste des abréviations.....	ix
Liste des tableaux.....	xi
Liste des figures	xii
0. Introduction Générale	1
0.1. Contexte	1
0.2. Identification et formulation du problème	1
0.3. Questions de recherche.....	2
0.3.1. Questions complémentaires.....	2
0.4. Formulation des hypothèses.....	2
0.4.1. Hypothèses secondaires	3
0.5. Justification du choix du sujet et motivations	3
0.5.1. L’objectif général	4
0.5.2. Les objectifs opérationnels/spécifiques	4
0.6. Méthodologie et délimitation du travail.....	4
0.7. Structure du mémoire.....	5
Chapitre 1 Cadre théorique	7

1.1	Introduction.....	7
1.2	Contexte et enjeux.....	7
1.3	Présentation du système actuel de signalement à Goma.....	8
1.3.1	Coups de sifflet et sirènes	8
1.3.2	Alerte de proximité (cris) et communications téléphoniques	8
1.3.3	Limites globales du système actuel.....	9
1.3.4	Qu'est-ce qu'une PWA?	11
1.4	Le signalement participatif	11
1.4.1	Définition et Principe	11
1.4.2	Processus de validation communautaire et hiérarchique	12
1.4.3	Exemples de plateformes de signalement participatif	14
1.5	La citoyenneté numérique.....	17
1.5.1	Notions et concepts	17
1.5.2	Participation et compétences numériques.....	18
1.6	La géolocalisation	18
1.6.1	Technologies de géolocalisation	18
1.6.2	Système d'Information Géographique (SIG).....	19
1.6.3	Usage en sécurité publique	20
1.6.4	Impact attendu sur la sécurité communautaire.....	21
1.7	Conclusion partielle	21
Chapitre 2 Analyse et conception du système		22
2.1	Introduction.....	22
2.2	Analyse des besoins	22
2.2.1	Identification des acteurs	22
2.2.2	Besoins fonctionnels	23
2.2.3	Besoins non-fonctionnels.....	25
2.3	Diagramme de cas d'utilisation	26
2.3.1	Diagramme de cas d'utilisation de citoyen et de la sentinelle	26
2.3.2	Diagramme de cas d'utilisation d'administrateur	27

2.3.3	Documentation de différents cas d'utilisation	28
2.4	Diagramme de séquences.....	41
2.4.1	Authentification des utilisateurs	41
2.4.2	Réinitialiser mot de passe	42
2.4.3	Signaler un incident	43
2.4.4	Consulter signalement.....	44
2.4.5	Visualiser les Statistiques	45
2.4.6	Générer des Rapports	46
2.4.7	Gérer les utilisateurs	47
2.4.8	Consulter Signalement pour un administrateur.....	48
2.4.9	Déclenchement d'Alerte Silencieuse	49
2.5	Diagramme de classes.....	50
2.6	Conclusion partielle	51
Chapitre 3 Implémentation du système		52
3.1	Introduction.....	52
3.2	Outils et technologies de développement	52
3.3	Architecture du Système et Échanges de Données	53
3.3.1	Flux de Données Montant (Client vers Serveur)	54
3.3.2	Flux de Données Descendant et Synchronisation Temps Réel.....	54
3.4	Présentation des interfaces de l'application	54
3.4.1	Interface d'authentification.....	55
3.4.2	Interface d'inscription des citoyens	55
3.4.3	Interface de signalement d'incident.....	56
3.4.4	Interface de consultation des signalements.....	59
3.4.5	Interface de consultation des signalements pour administrateur	61
3.4.6	Interface de visualisation des statistiques	64
3.4.7	Interface de génération des rapports	65
3.4.8	Interface de gestion d'utilisation.....	65
3.4.9	Interface du déclenchement d'Alerte Silencieuse.....	68

3.5	Tests et validation du système	69
3.6	Conclusion partielle	70
	Conclusion générale.....	71
	Bibliographie.....	74
	Annexe A	78

Liste des abréviations

AML : Advanced Mobile Location (Localisation Mobile Avancée)

API : Application Programming Interface (Interface de Programmation d'Application)

BaaS : Backend as a Service (Backend en tant que Service)

CU : Cas d'Utilisation

DCU : Diagramme de Cas d'Utilisation

GPS : Global Positioning System

HTML: HyperText Markup Language

HTTP: HyperText Transfer Protocol

HTTPS : HyperText Transfer Protocol Secure

IA : Intelligence Artificielle

JS : JavaScript

JSON : JavaScript Object Notation

KPI : Key Performance Indicators (Indicateurs Clés de Performance)

OSINT : Open Source Intelligence

PNC : Police Nationale Congolaise

POST : Méthode de requête HTTP (utilisée pour l'envoi de données vers un serveur)

PWA : Progressive Web App (Application Web Progressive)

RDC : République Démocratique du Congo

REST : Representational State Transfer

RLS : Row Level Security (Sécurité au Niveau des Lignes)

SIG : Système d'Information Géographique

SMS : Short Message Service

SOS : Save Our Souls (Signal de détresse)

SQL : Structured Query Language

UI : User Interface (Interface Utilisateur)

UML : Unified Modeling Language (Langage de Modélisation Unifié)

URL : Uniform Resource Locator (Localisateur Uniforme de Ressource)

UX : User Experience (Expérience Utilisateur)

USSD : Unstructured Supplementary Service Data (Données de Service Supplémentaires Non Structurées)

Wi-Fi: Wireless Fidelity

Liste des tableaux

Tableau 2-1: Documentation de cas d'utilisation : "Créer un compte"	29
Tableau 2-2 : Documentation de cas d'utilisation : "s'authentifier"	30
Tableau 2-3: Documentation de cas d'utilisation : "réinitialiser mot de passe"	31
Tableau 2-4: Documentation de cas d'utilisation : "Signaler un incident"	31
Tableau 2-5: Documentation de cas d'utilisation : "Consulter signalement"	33
Tableau 2-6: Documentation de cas d'utilisation : "Visualiser les Statistiques"	35
Tableau 2-7: Documentation de cas d'utilisation : "Générer des Rapports"	36
Tableau 2-8: Documentation de cas d'utilisation : "Gérer les utilisateurs"	36
Tableau 2-9: Documentation de cas d'utilisation : "Consulter Signalement pour un administrateur"	38
Tableau 2-10: Documentation de cas d'utilisation : "Déclenchement d'Alerte Silencieuse"	39

Liste des figures

Figure 2-1: Diagramme de cas d'utilisation de citoyen et de la sentinelle	27
Figure 2-2: Diagramme de cas d'utilisation de l'administrateur	28
Figure 2-3: Diagramme de séquence du CU créer un compte et du CU s'authentifier	41
Figure 2-4: Diagramme de séquence du CU Réinitialiser mot de passe.....	42
Figure 2-5: Diagramme de séquence du CU signaler incident	43
Figure 2-6: Diagramme de séquence du CU Consulter signalement	44
Figure 2-7: Diagramme de séquence du CU Visualiser les Statistiques.....	45
Figure 2-8: Diagramme de séquence du CU Générer des Rapports	46
Figure 2-9: Diagramme de séquence du CU Gérer les utilisateurs.....	47
Figure 2-10: Diagramme de séquence du CU Consulter Signalement pour un administrateur	48
Figure 2-11: Diagramme de séquence du CU Déclenchement d'Alerte Silencieuse	49
Figure 2-12: Diagramme de classe du système.....	50
Figure 3-1: Interface d'authentification à la plateforme	55
Figure 3-2: Interface d'inscription des citoyens	56
Figure 3-3: Interface du formulaire de signalement d'incident	57
Figure 3-4: Interface d'incident signaler.....	58
Figure 3-5: Interface de consultation des signalements	60
Figure 3-6: Interface de consultation des signalements pour administrateur	62
Figure 3-7: Interface de validation pour administrateur	63
Figure 3-8: Interface de visualisation des statistiques	64
Figure 3-9: Interface de génération des rapports	65
Figure 3-10: Interface de gestions des utilisateurs.....	66
Figure 3-11: Interface profil d'utilisateur et attribution de rôle du sentinelle	67
Figure 3-12: Interface de notification de promotion d'un citoyen aux rang de sentinelle.....	67
Figure 3-13: Interface du déclenchement d'Alerte Silencieuse	68
Figure 3-14: Interface de visualisation d'alerte SOS par l'administrateur	69

0. Introduction Générale

0.1. Contexte

Dans un contexte urbain marqué par des défis sécuritaires croissants, la ville de Goma, en République Démocratique du Congo, fait face à des enjeux majeurs en matière de gestion des incidents sécuritaires. Entre conflits armés, criminalité urbaine (vols, agression, incendie, etc.) et catastrophes naturelles, l'absence de systèmes efficaces pour signaler, prioriser et répondre à ces situations en temps réel expose les populations à des risques accrus et retarde des interventions vitales. Le recours à une solution technologique innovante s'impose pour améliorer la rapidité, la précision et la coordination des réponses aux urgences.

Ce projet propose la conception et l'implémentation d'une **application web participative de signalement des incidents sécuritaires**, basée sur la géolocalisation et la collaboration communautaire. Inspirée par les principes des *Smart Cities*, cette plateforme vise à transformer chaque citoyen en acteur de sa propre sécurité, tout en fournissant aux autorités locales des outils de gestion des crises en temps réel. Contrairement aux applications existantes (comme Waze, limitées aux accidents routiers), notre solution couvre un spectre large d'incidents (vols, agressions, incendies, etc.) et intègre un mécanisme de **validation communautaire** pour garantir la fiabilité des alertes.

0.2. Identification et formulation du problème

La situation sécuritaire de la ville de Goma est préoccupante : la ville enregistre un taux élevé d'incidents (vols, agressions, incendies, etc.) et repose sur des mécanismes de signalement traditionnels (cris, sifflets, etc.) peu efficaces. Le manque de coordination entre les acteurs de la sécurité et la méfiance croissante de la population aggravent cette situation. La situation actuelle révèle l'absence d'un système intégré permettant un signalement rapide et géolocalisé des incidents, une mobilisation coordonnée des acteurs de sécurité et une remontée d'informations fiables. Cette lacune technologique et organisationnelle se traduit par des

retards d'intervention, une allocation inefficace des ressources et une incapacité à établir des données fiables pour la prévention. L'absence d'une plateforme numérique participative adaptée au contexte local constitue un frein majeur à l'amélioration de la sécurité publique à Goma, justifiant la conception d'une solution technologique innovante.

0.3. Questions de recherche

Comment concevoir une application web participative de signalement des incidents sécuritaires à Goma pour améliorer significativement l'efficacité et la rapidité des interventions ?

0.3.1. Questions complémentaires

Afin de préciser le cadre d'analyse et d'opérationnaliser la question principale, les questions complémentaires suivantes sont formulées :

1. Quelles sont les limites des systèmes actuels de signalement des incidents sécuritaires à Goma (appels téléphoniques, cris, sifflets, etc.) ?
2. Quel type d'architecture et quelles fonctionnalités une application web participative devrait-elle intégrer pour être efficace en contexte de crise sécuritaire ?
3. Quel mécanisme de validation communautaire permettrait d'assurer la fiabilité des informations transmises ?

0.4. Formulation des hypothèses

L'hypothèse principale est qu'une telle application, dotée de géolocalisation automatique, d'un système de catégorisation des urgences et d'un mécanisme de validation collaborative, permettrait d'améliorer significativement la rapidité et l'efficacité des interventions. Elle optimiserait ainsi le traitement des alertes et la coordination entre les différents acteurs de la sécurité.

0.4.1. Hypothèses secondaires

Pour étayer et opérationnaliser l'hypothèse principale, les hypothèses secondaires suivantes sont formulées :

1. Les systèmes actuels de signalement présentent des lacunes en termes de centralisation, de rapidité de diffusion et de couverture géographique.
2. Une architecture technique basée sur une API REST, intégrant une cartographie interactive des incidents, une catégorisation automatique des signalements et des notifications en temps réel, constituerait une solution adaptée au contexte local.
3. Un mécanisme de validation à deux niveaux (auto-évaluation collaborative par les citoyens suivie d'une validation officielle par les administrateurs) renforcerait la fiabilité des informations transmises, en limitant les fausses alertes tout en instaurant la confiance des utilisateurs.

0.5. Justification du choix du sujet et motivations

Ce sujet va d'abord répondre à un besoin concret qui est l'absence d'outils numériques locaux permettant un signalement collaboratif et géolocalisé des incidents sécuritaires. Les dispositifs d'alerte traditionnels restent insuffisants pour traiter les enjeux complexes de sécurité urbaine. Par ailleurs, les concepts de **citoyenneté numérique** [1] et de **crowdsourcing sécuritaire** [2] montrent que les habitants peuvent contribuer activement à la gestion des risques via des plateformes numériques. En garantissant l'anonymat et la fiabilité des signalements, on peut encourager l'engagement citoyen sans exposer les lanceurs d'alerte à des représailles.

Au final, ce mémoire vise à favoriser une gestion communautaire des crises par une approche technologique accessible, inclusive et contextualisée, améliorant la résilience sécuritaire de la ville de Goma.

Énoncé des objectifs de recherche

0.5.1. L'objectif général

L'objectif général de ce travail est de **concevoir et implémenter une application web participative de signalement des incidents sécuritaires à Goma**, intégrant un système de géolocalisation précise et de validation communautaire, afin d'optimiser la collecte, la vérification et la transmission des données d'urgence vers les autorités compétentes.

0.5.2. Les objectifs opérationnels/spécifiques

Pour atteindre cet objectif, les objectifs spécifiques suivants ont été définis :

- **Analyser** les besoins des différentes parties prenantes (citoyens et les forces de l'ordre qui sont les administrateurs) à travers l'étude des systèmes existants dans des contextes similaires.
- **Modéliser** l'architecture fonctionnelle du système en définissant les cas d'utilisation principaux (UML) et les flux de données, en tenant compte des contraintes techniques spécifiques au contexte de Goma.
- **Développer** les composants clés de l'application : notamment le module de signalement (avec géolocalisation automatique), le mécanisme de validation collaborative, le tableau de bord analytique pour les administrateurs (avec cartographie interactive) et le système de notifications en temps réel.

0.6. Méthodologie et délimitation du travail

Ce projet utilise une approche méthodologique structurée qui combine plusieurs méthodes et techniques de recherche. L'objectif est de garantir que l'application développée réponde réellement aux besoins de sécurité à Goma tout en étant techniquement fiable.

La recherche suit principalement deux méthodes scientifiques. La méthode analytique permet de décomposer le système complexe de sécurité en éléments simples pour mieux comprendre les problèmes actuels. La méthode expérimentale guide le développement par essais successifs, avec des prototypes testés et améliorés progressivement.

Pour recueillir les informations nécessaires, plusieurs techniques sont employées. L'observation directe sur le terrain aide à comprendre comment fonctionnent actuellement les signalements d'incidents.

Le développement technique utilise la méthode Agile, avec des cycles de travail courts qui permettent d'avancer pas à pas et de s'adapter rapidement aux retours des utilisateurs. Cette approche assure que l'application évolue en fonction des besoins réels plutôt que de suivre un plan rigide établi au départ.

Des tests rigoureux sont prévus à chaque étape pour vérifier que l'application fonctionne correctement. Des tests techniques contrôlent la performance et la sécurité, tandis que des tests pratiques avec des utilisateurs évaluent la facilité d'utilisation.

Cette méthodologie équilibrée assure que le projet reste ancré dans la réalité du terrain tout en respectant les standards techniques les plus exigeants. Elle permet de créer une application qui soit à la fois techniquement solide et véritablement utile pour les habitants de la ville de Goma.

0.7. Structure du mémoire

Hormis l'introduction et la conclusion générales, la présente recherche s'articule autour de trois chapitres fondamentaux qui structurent notre démarche méthodologique :

- **Chapitre 1. Cadre théorique**

Ce chapitre pose les bases conceptuelles du projet en analysant la problématique de l'insécurité urbaine à Goma et en explorant les notions de villes intelligentes (Smart Cities) et de sécurité participative.

- **Chapitre 2. Analyse et Conception du système**

Ce chapitre traduit les besoins du terrain en solutions logicielles, en modélisant l'architecture de GomaSecure, les flux de données et les interactions entre les différents acteurs (citoyens, sentinelles, autorités) à l'aide du langage UML.

- **Chapitre 3. Implémentation du système**

Ce chapitre détaille la réalisation technique et concrète de l'application, mettant en lumière le choix des technologies modernes (React, Supabase, PWA) et présentant les interfaces finales de la plateforme déployée.

Cette organisation reflète la progression logique de notre étude, allant des fondements conceptuels à la mise en œuvre concrète de la solution mobile proposée pour la sécurité à Goma.

Chapitre 1 Cadre théorique

1.1 Introduction

Ce premier chapitre établit les bases théoriques et contextuelles nécessaires au développement d'un système participatif de signalement des incidents sécuritaires dans la ville de Goma. Il met en lumière la vulnérabilité sécuritaire persistante de la ville et les mécanismes actuels d'alerte communautaire (sirènes, sifflets, cris), qui, bien qu'utiles, restent limités en termes de précision, rapidité et de traçabilité. Ces insuffisances justifient la mise en place d'une solution numérique plus efficace et confidentielle.

Le chapitre présente ensuite les concepts de crowdsourcing sécuritaire et de citoyenneté numérique, qui démontrent la capacité des citoyens à contribuer activement à la gestion des incidents. Les notions de géolocalisation et de validation communautaire sont également présentées afin de cadrer les principes techniques et collaboratifs qui orienteront la future solution.

Ainsi, cette analyse constitue le socle méthodologique pour orienter la conception et l'implémentation du prototype, en s'assurant que la solution technologique réponde de manière pragmatique aux réalités sécuritaires et sociotechniques de la ville de Goma.

1.2 Contexte et enjeux

Dans une ville comme Goma, marquée par une instabilité politique persistante, des incidents sécuritaires fréquents, des catastrophes récurrentes, l'absence d'un dialogue direct entre la population et les autorités limite considérablement la rapidité et l'efficacité des interventions. Dans ce contexte, de nouvelles technologies participatives basées sur le numérique et la géolocalisation offrent des leviers pour améliorer la transparence et la réactivité face aux incidents de sécurité.

Le cadre institutionnel et technologique actuel de Goma demeure en développement : la pénétration du téléphone mobile dépasse 50 % de la population en RDC, mais seulement un quart des habitants ont un accès régulier à Internet [3]. Cette fracture numérique impose de

concevoir une application robuste (locale, peu consommatrice de données) et accessible. À ceci s'ajoute la confiance du public envers les autorités qui est limitée en raison de la défaillance de la coordination antérieure des interventions et d'une méfiance persistante envers les forces de l'ordre. Il est donc essentiel de garantir l'anonymat et la fiabilité des signalements afin d'encourager la participation citoyenne active et durable.

1.3 Présentation du système actuel de signalement à Goma

Face à une insécurité récurrente, la population de Goma s'appuie principalement sur des **coups de sifflet** et des **cris d'alerte ou appels vocaux**, dispositifs traditionnels dont l'efficacité opérationnelle reste limitée par leur nature essentiellement sonore et informelle.

1.3.1 Coups de sifflet et sirènes

Concrètement, un habitant en danger souffle dans un sifflet, une trompette artisanale, produisant un bruit fort et strident. Ce son est aussitôt entendu par les voisins proches qui le répètent à leur tour, propageant ainsi l'alerte dans tout le quartier. Par exemple, lors d'une récente poussée d'insécurité nocturne (avril 2025), il a été rapporté que « dès 20 heures, le quartier Ndosho a résonné de coups de sifflet et de sons de trompette » pour tenter de dissuader les malfaiteurs [4]. Des initiatives locales formalisent aussi ce procédé : en 2022, le chef de quartier de Himbi a distribué 400 sifflets, 3 sirènes et 4 vuvuzelas aux responsables de base afin de renforcer ces alertes communautaires [5]. Le bourgmestre de Goma a même appelé, en décembre 2021, tous les habitants à se munir d'un sifflet pour prévenir rapidement les forces de l'ordre en cas de danger [6]. Ces témoignages montrent la solidarité de voisinage forte, mais aussi l'aspect rudimentaire de ce système.

1.3.2 Alerte de proximité (cris) et communications téléphoniques

Un autre moyen traditionnel est l'alerte par la voix. Lorsqu'un témoin d'un crime comme un vol ou une agression s'en rend compte, il peut crier « Au voleur ! » ou « À l'aide ! » pour attirer l'attention du voisinage. Ces cris sont transmis par propagation acoustique : chaque habitant

situé à portée peut les répercuter. Les sources indiquent que ces appels reposent sur la réactivité des habitants : par exemple, Radio Okapi note que « des cris d'alerte ont fusé à travers le quartier, témoignant d'une montée de la tension » dans le quartier lors des incidents signalés [4] [7].

Pour pallier la limite de la distance, la population se tourne vers les appels vocaux d'urgence ou les messages dans des groupes WhatsApp citoyens. Cependant, cette méthode se heurte à des défis structurels critiques. Par appel téléphonique, la principale barrière est l'absence d'un adressage urbain précis à Goma : la victime perd de précieuses minutes à tenter de décrire son emplacement exact (« à côté de la boutique rouge, 3ème avenue »), ce qui retarde l'intervention. Quant aux groupes WhatsApp, bien qu'ils permettent de diffuser l'information massivement, l'information y est non structurée, difficilement exploitable par les autorités (pas de base de données ni de dashboard), et laisse une porte grande ouverte à la propagation rapide de fausses alertes et de rumeurs incontrôlables.

En définitive, bien que ces méthodes orales et téléphoniques soient les plus utilisées par défaut, leur manque de précision spatiale, de structuration et de lien direct avec un système centralisé des autorités montre leurs limites critiques en situation d'urgence vitale.

1.3.3 Limites globales du système actuel

Ces procédés traditionnels présentent plusieurs faiblesses majeures :

- **Manque de précision géographique** : Les alertes sonores (sifflets ou cris) ne donnent qu'une indication très vague de l'emplacement. Les récits des incidents identifient seulement le quartier (par exemple Ndosho [4]), car les voisins entendent le signal sans pouvoir localiser précisément l'origine du bruit. Aucun outil de géolocalisation ou de repérage précis n'est associé à ces alertes, si bien que les secours guidés par le son restent dans l'incertitude sur le lieu exact de l'événement. De plus, le message vocal est souvent imprécis : il signale un problème sans en préciser la nature exacte (vol à main armée, incendie, etc.).

- **Lenteur et dépendance humaine** : La transmission de l'alerte s'effectue par relais voisin-à-voisin. Ce mode informel peut prendre du temps et échouer si certains habitants dorment, sont absents ou ne réagissent pas au bruit. C'est pour pallier cette lenteur que des dispositifs tels que les sifflets et les sirènes sont aujourd'hui distribués officiellement aux responsables locaux [5], soulignant que sans ces outils la propagation de l'alerte était trop aléatoire et lente.
- **Absence de traçabilité** : Ces alertes restent un acte ponctuel sans aucun enregistrement. Aucun journal d'alerte (horodatage, localisation, nature du signal) n'est conservé. Les sources consultées (reportages de presse et annonces officielles) ne font état d'aucune archive ni de suivi formel des incidents signalés, ce qui empêche tout bilan ou analyse a posteriori [8].
- **Risque pour les citoyens** : L'alerte est publique et bruyante, ce qui met en danger le témoin. En criant ou en soufflant dans un sifflet, la victime ou le témoin indique sa position aux malfaiteurs, enfin, la personne qui crie s'expose elle-même au danger en se signalant de façon évidente. Les articles relatent d'ailleurs des incidents tragiques à Goma où la population, en panique, a commis des erreurs (lynchages, etc.), ce qui traduit la dangerosité de ce système non protégé [8].
- **Manque de coordination institutionnelle** : Il n'existe pas de canal officiel pour recevoir directement ces signaux communautaires. Les autorités n'ont pas de centre de réception pour les alertes artisanales, qui leur parviennent au mieux par le bouche-à-oreille. À ce propos, le président du Conseil communal de la jeunesse de Goma note que les numéros verts distribués à la population « n'ont fait aucune suite favorable car [ils] ne sont pas joignables lorsque la population fait face à des menaces » [6] [8]. Autrement dit, aucun système centralisé n'est en place : la réaction dépend uniquement de la veille spontanée des voisins et gardiens locaux.

Ces limites structurelles (imprécision, lenteur, absence d'archives, exposition du lanceur d'alerte et manque de relais officiel) motivent clairement la recherche d'un système de signalement modernisé, capable de localiser précisément les incidents, de diffuser rapidement les alertes et de conserver un historique exploitable des événements.

La pertinence technique de la PWA devient une nécessité stratégique lorsqu'on la projette dans le contexte de la ville de Goma.

1.3.4 Qu'est-ce qu'une PWA?

Une Progressive Web App (PWA) est une application Web développée avec les standards du Web, mais offrant une expérience utilisateur proche de celle d'une application native [9]. Autrement dit, c'est d'abord un site web (HTML/CSS/JS) accessible par URL, mais conçu de telle sorte qu'il peut être installé sur l'appareil de l'utilisateur et s'exécuter comme une appli classique [10]. L'un de ses avantages majeurs est sa portée universelle : une PWA utilise un code source unique multiplateforme et peut être utilisée (par n'importe qui, n'importe où, sur n'importe quel appareil) [10]. Une fois installée, une PWA apparaît avec une icône sur l'écran d'accueil et s'ouvre en mode autonome (plein écran), sans l'interface du navigateur. Nous expliquerons, au cours de ce travail, pourquoi nous avons privilégié la PWA plutôt que l'application mobile pour la première version de notre système.

Dans cette perspective, le recours au signalement participatif apparaît comme une approche innovante et adaptée.

1.4 Le signalement participatif

1.4.1 Définition et Principe

Le signalement participatif (ou crowdsourcing en contexte sécuritaire) se définit comme une méthode interactive de collecte de données ou d'informations auprès d'un grand nombre de

personnes, généralement par Internet [2]. Il repose sur la contribution volontaire des citoyens pour signaler des incidents (criminalité, violences, alertes urgentes, etc.) via une plateforme numérique. Appliqué à la sécurité urbaine, ce système permet aux citoyens de fournir des comptes rendus « de première main » (photos, vidéos, audios, textes, géolocalisation) sur des risques et incidents, contribuant ainsi à une meilleure connaissance de la situation en temps réel [2] [11]. Dans ce modèle, les usagers jouent le rôle de « capteurs humains » sur le terrain.

Les plateformes participatives exploitent souvent les smartphones pour géolocaliser précisément chaque incident signalé et alerter automatiquement les autorités locales [11]. Le déploiement de telles plateformes suppose cependant de relever plusieurs défis : la qualité et la fiabilité des données collectées (contrôle des faux reports), le traitement en temps réel par les opérateurs, et le respect de la vie privée des contributeurs [11]. La recherche montre notamment qu'un des principaux freins est l'absence de mécanismes de gestion de la confiance dans les données fournies par des amateurs [11]. Sans système de modération ou de validation (par des modérateurs), les autorités hésitent à se fier entièrement aux informations communautaires.

1.4.2 Processus de validation communautaire et hiérarchique

Les systèmes participatifs de signalement d'incidents combinent généralement deux niveaux de vérification. D'abord, les alertes sont filtrées par la communauté elle-même (sentinelles locales qui sont les utilisateurs de confiance) via des confirmations croisées et des votes (par ex. un bouton « Je confirme » par un ou plusieurs témoins proches). Ce « filtre citoyen » renforce la crédibilité initiale du signalement [12]. Ensuite, les informations validées par les sentinelles sont transmises à un niveau supérieur (administrateurs, services de police ou autorités locales) pour une revue formelle.

1.4.2.1 Processus de validation communautaire et basé sur la réputation

Les plateformes mettent en outre en place des mécanismes de **confiance** et de **réputation** pour évaluer la fiabilité des contributeurs [13]. Chaque utilisateur se voit attribué un score de réputation qui évolue selon la fiabilité de ses signalements passés, influençant ses droits pour passer d'un utilisateur simple (citoyen) à modérateur (par ex. accès prioritaire à la publication ou capacités de modération). Les usagers de confiance peuvent ainsi signaler directement et jouer un rôle de modération, alors que les nouveaux venus doivent accumuler des validations pour être crédibles. De plus, les votes communautaires (« Je confirme (liker) »/« Je démens (disliker) ») font office de filtre de qualité initial: plus un incident est confirmé (liker) par les voisins, plus il est jugé sérieux et prioritaire [12]. Dans le volontariat humanitaire, on observe qu'«une grande quantité de données issues du public est ensuite croisée par d'autres volontaires pour évaluer la gravité de la demande d'aide ou de secours formulées par les populations affectées par une crise» [14]. Ce double mécanisme (score individuel + vote collectif) affine la sélection des alertes avant l'escalade.

1.4.2.2 Processus de validation par les autorités (administrateurs)

La seconde phase fait intervenir des acteurs plus spécialisés (coordinateurs, autorités, services d'urgence, etc.) pour valider les signalements les plus critiques ou ambigus. En somme, la littérature met en avant un modèle hybride où la réactivité initiale de la foule est couplée à la rigueur des vérifications des modérateurs, maximisant à la fois la rapidité d'intervention et la confiance dans l'information diffusée [14] [15].

1.4.2.3 Bénéfices attendus du système

Ce mécanisme de réputation et de double validation présente plusieurs avantages stratégiques [16] :

- ❖ **Fiabilisation des signalements** : en mettant d'abord à contribution des utilisateurs de confiance, le système filtre les fausses alertes, doublons et contenus malveillants

avant diffusion large. Les contributions frauduleuses ou inexactes voient rapidement leur origine neutralisée par le vote majoritaire des citoyens ou rejeter par une sentinelle.

- ❖ **Renforcement de la confiance publique** : la transparence du processus (critères de réputation, niveaux utilisateurs, marqueurs « validé / rejeté ») montre à tous que l'information est validée de façon objective. Cette traçabilité renforce la crédibilité de la plateforme auprès des utilisateurs et des autorités.
- ❖ **Apprentissage collectif** : le système de score joue un rôle d'éducation numérique. Les utilisateurs voient leur réputation augmenter avec la fiabilité de leurs contributions, ce qui les incite à adopter des comportements responsables. En récompensant publiquement la rigueur et la pertinence, on encourage une communauté plus engagée et avisée.

1.4.3 Exemples de plateformes de signalement participatif

Plusieurs initiatives illustrent concrètement les deux modes de validation participative évoqués : communautaire et hiérarchique. Par exemple, la plateforme électorale ukrainienne Elect.UA avait pour objectif de surveiller en temps réel l'intégrité des scrutins nationaux. Elle distinguait explicitement deux catégories de contributeurs : d'une part, des observateurs officiels dont les signalements des incidents étaient automatiquement validés ; d'autre part, le grand public, pour lequel chaque rapport devait faire l'objet d'un protocole de confirmation rigoureux [17]. Ce dispositif hybride assure qu'une part de confiance est accordée aux acteurs légitimes (observateurs officiels), tandis que les contributions externes sont vérifiées avec plus de précaution.

D'autres projets misent principalement sur la validation par la communauté. Ainsi, City.Risks, initiative soutenue par l'Union européenne, propose une plateforme collaborative où chaque citoyen, via son smartphone, partage en temps réel des informations critiques avec les autorités. Dans ce cas, l'information circule horizontalement et n'est considérée comme fiable que si

plusieurs utilisateurs indépendants signalent le même événement. De même, la plateforme Ushahidi : consacrée à la cartographie participative des crises, recommande de ne déclarer un signalement « vérifié » que s'il est confirmé par au moins deux sources distinctes (par exemple, deux SMS provenant de numéros différents ou un témoignage accompagné d'une photo/vidéo) [18]. Ce mode de validation communautaire par recoupement multiple renforce la fiabilité et la crédibilité des données diffusées.

En complément de ces modèles, l'application américaine Citizen, qui diffuse en continu des alertes de sécurité met en lumière l'importance d'une validation rigoureuse pour éviter la désinformation. Lors d'une fausse alerte sur Manhattan, Citizen a rappelé qu' <envoyer une fausse alerte sur un attentat terroriste pourrait littéralement générer une panique>, soulignant ainsi la nécessité d'une vérification systématique de chaque signalement [19]. La diffusion incessante d'alertes peut accroître l'anxiété des utilisateurs (comme l'a montré l'expérience de l'application Citizen) et provoquer des comportements indésirables, tels que le profilage géographique de certains quartiers. Cette expérience souligne donc l'importance de concevoir ces plateformes avec un accent sur la confiance, la qualité de l'information et la protection des usagers.

Concernant l'aspect technologique, L'étude de ces plateformes participatives met en évidence une prédominance des architectures natives ou hybrides, souvent lourdes à déployer.

Elect.UA et City.Risks reposent sur des écosystèmes complexes couplant applications mobiles natives et infrastructures cloud, exigeant des terminaux performants [20].

Ushahidi, bien qu'en transition vers l'hybride via Ionic, et Citizen, exclusivement native, imposent le passage obligatoire par les magasins d'applications (Google Play, App Store).

Cette approche traditionnelle présente des frictions majeures, elle nécessite des développements distincts par système d'exploitation (coûteux en maintenance), impose des téléchargements initiaux volumineux et rend les mises à jour dépendantes de la validation des stores d'applications.

Ce constat s'inscrit dans le phénomène mondial de la “Fatigue des Apps”: la majorité des utilisateurs ne téléchargent désormais plus aucune nouvelle application mobile par mois, se limitant aux réseaux sociaux essentiels [21]. À Goma, cette réticence est amplifiée par la précarité matérielle, avec des smartphones d'entrée de gamme dont le stockage (8Go ou 16Go) est souvent saturé, installer une application de sécurité oblige l'utilisateur à sacrifier des photos ou des outils essentiels [22]. La difficulté d'installer une application dissuade les gens de le faire, ce qui fait qu'elle reste très peu utilisée.

Plus critique encore est la gestion du cycle de vie des applications. Dans un environnement où les coûts des données mobile est prohibitif (représentant une part significative du revenu journalier), les utilisateurs désactivent quasi-systématiquement les mises à jour automatiques. Conséquence, une application native installée risque de ne jamais être mise à jour. Sans mise à jour, l'application devient vite dépassée et vulnérable, privant ainsi les utilisateurs des dernières nouveautés et d'une protection efficace.

Face à ces limites, la PWA (Progressive Web App) se positionne comme une solution de convergence. Contrairement aux applications natives qui exigent une installation lourde, ou aux sites web classiques inopérants totalement sans réseau, la PWA tire parti du meilleur des deux mondes, Une seule base de code fonctionne sur tous les terminaux (Android, iOS, Desktop), éliminant la fragmentation technologique, fonctionne hors ligne via des service workers, Elle est accessible via une simple URL, contournant les barrières à l'entrée des stores d'applications [23].

Néanmoins, ces contraintes ne signifient pas un rejet définitif du natif. Au contraire, la PWA est vue comme une première étape adaptée à l'environnement de la ville de Goma (faible connectivité, terminaux modestes, etc.). Un déploiement ultérieur d'applications Android/iOS est prévu pour intégrer des fonctionnalités critiques non réalisables en PWA (par exemple accéder à tous les capteurs et boutons physiques du téléphone). La PWA sert ainsi de solution légère, rapidement disponible et évolutive, avant le développement d'une version native plus riche.

Au final, qu'il s'agisse de validation officielle par des observateurs ou de vérification collaborative entre citoyens, ces plateformes de signalement donnent aux habitants un rôle actif dans la vie publique. Elles offrent aux citoyens les moyens de signaler, recouper et partager des informations en temps réel grâce aux outils numériques, incarnant ainsi une citoyenneté numérique concrète et responsable. En impliquant directement les utilisateurs dans la collecte et la fiabilité de l'information de sécurité, ces systèmes participatifs posent les bases d'un engagement civique renouvelé par le numérique : La thématique que nous aborderons dans la section suivante sur la citoyenneté numérique.

1.5 La citoyenneté numérique

1.5.1 Notions et concepts

La citoyenneté numérique désigne la capacité et la responsabilité d'un individu à participer activement à la vie de la société via les technologies digitales [1]. Selon Karen Mossberger et al., les citoyens numériques sont ceux « qui utilisent Internet de manière régulière et efficace », c'est-à-dire pour s'engager dans la société, la politique et l'action publique [1]. Autrement dit, être citoyen numérique revient à exercer ses droits et devoirs civiques (informer, débattre, signaler, collaborer) sur les plateformes en ligne, tout en respectant les règles de sécurité et d'éthique numérique.

La citoyenneté numérique est aussi vue comme une performativité : elle s'exprime non pas seulement par la présence en ligne, mais par les actes. Dans les sociétés actuelles, « les actes numériques deviennent des moyens importants par lesquels les citoyens créent et incarnent leur rôle dans la société » [24]. Appliqué à notre contexte, cela signifie que la plateforme de signalement doit offrir aux citoyens un moyen concret de “prendre part” à la sécurité locale. Les principes fondamentaux incluent la transparence de l'information, la protection de la vie privée (par ex. possibilité d'anonymat) et la facilité d'usage, afin de favoriser l'engagement le

plus large possible. Par exemple, l'initiative européenne de citoyenneté numérique recommande de placer les personnes « au centre de la transformation numérique » [1], ce qui implique de concevoir des interfaces accessibles et inclusives pour tous (y compris non-informaticiens).

1.5.2 Participation et compétences numériques

Au-delà des définitions théoriques, la citoyenneté numérique passe par l'éveil et la formation des utilisateurs. Dans notre cas d'usage, il s'agit d'expliquer aux habitants de la ville de Goma comment signaler un incident en ligne, quels types d'informations sont utiles (photos, vidéos, audio, localisation, descriptif), et comment protéger leurs données personnelles (ne fournir que ces éléments nécessaires, recours à l'anonymat). Les compétences numériques de base (utilisation d'un smartphone, d'Internet) doivent être considérées : bien que la pénétration mobile soit moyenne, les campagnes de sensibilisation (par radio, télévision, réseaux sociaux) peuvent renforcer la confiance dans l'outil. En synthèse, la citoyenneté numérique appliquée ici se traduit par l'autonomisation des citoyens dans le monitoring de leur sécurité et leur interaction constructive avec les institutions [1] [24]. Dans cette logique de responsabilisation et d'efficacité opérationnelle, la géolocalisation constitue un levier technologique essentiel, en ce qu'elle permet de situer avec précision les incidents signalés et d'optimiser la coordination des interventions.

1.6 La géolocalisation

1.6.1 Technologies de géolocalisation

La géolocalisation désigne l'ensemble des techniques permettant de déterminer la position géographique précise d'un appareil (smartphone, tablette) via GPS, Wi-Fi ou réseaux cellulaires [25]. D'après Estes, la géolocalisation « utilise les données acquises à partir d'un appareil personnel pour identifier ou décrire la position physique réelle de l'utilisateur » [25].

Avec la généralisation des smartphones (plus de 2,5 milliards d'utilisateurs dans le monde) et la prolifération des applications mobiles, les services basés sur la localisation sont devenus omniprésents. Ils reposent sur la collecte de données actives (GPS) ou passives (adresse IP, stations de base) pour obtenir une précision souvent inférieure à quelques dizaines de mètres, adaptée aux usages urbains.

Dans notre application, la géolocalisation joue un rôle clé : chaque signalement d'incident est automatiquement associé à des coordonnées GPS, ce qui permet de l'afficher sur une carte et d'alerter les services concernés à proximité. Cet usage améliore considérablement la vitesse d'identification des lieux critiques. En France, par exemple, des applications d'urgence comme AML (Advanced Mobile Location) intègrent des systèmes similaires pour guider les secours vers le lieu exact d'un accident. En outre, la géolocalisation peut servir à filtrer ou regrouper les rapports redondants (plusieurs signaux de la même catégorie dans un rayon de 50) et à produire des statistiques par quartier. Pour transformer ces coordonnées brutes en une véritable aide à la décision, il est nécessaire de les intégrer au sein d'un Système d'Information Géographique (SIG), capable de centraliser l'intelligence territoriale de notre plateforme.

1.6.2 Système d'Information Géographique (SIG)

Un SIG est un système informatique dédié aux données géographiques. Il “intègre, stocke, analyse et affiche l'information géographique” afin de représenter le monde sous forme de cartes interactives [26] [27]. Concrètement, un SIG combine des bases de données spatiales (vecteurs, images raster, attributs thématiques) avec des logiciels spécialisés permettant de manipuler ces données. Les logiciels de SIG fournissent des outils pour stocker, analyser et afficher toutes les informations géographiques [28], tandis que les données elles-mêmes (points, lignes, polygones géoréférencés) doivent être correctement coordonnées pour assurer la cohérence des analyses [28]. L'interface principale est souvent une carte multi-couches thématiques : chaque couche représente un type de données (routes, bâtiments, densité de population, etc.) que l'on peut superposer. Au final, l'objectif du SIG est de créer des cartes

dynamiques et lisibles qui supportent les requêtes spatiales et facilitent la compréhension de phénomènes localisés [27].

En matière de sécurité publique, les SIG jouent un rôle clé dans la connaissance de la situation et l'aide à la décision. Ils permettent de visualiser en temps réel des incidents géolocalisés et de repérer des tendances spatiales (points chauds, trajectoires d'évacuation, etc.), ce qui optimise l'allocation des ressources d'intervention. Des études soulignent qu'avec un SIG les services de police "peuvent comprendre où et quand le crime se produit afin de déployer leurs ressources plus efficacement" [29]. De même, les responsables d'urgence utilisent les SIG pour planifier la réponse aux catastrophes (gestion des sinistres, interventions en zone à risque, etc.) en combinant données géographiques et analyse spatiale. En somme, les SIG fournissent aux acteurs de la sécurité des outils de visualisation et d'analyse puissants pour prévenir, protéger et atténuer les menaces. Pour comprendre comment cette technologie peut révolutionner la gestion des incidents de la ville de Goma, il convient d'analyser plus spécifiquement les modalités de son usage en sécurité publique.

1.6.3 Usage en sécurité publique

Les systèmes de signalement participatif utilisent la géolocalisation pour fournir un contenu contextuel. Comme cité plus haut, l'application CitiSafe affiche les incidents « en temps réel avec la localisation marquée sur la carte » [30]. De même, le projet CITY.RISKS souligne l'importance de la géolocalisation pour l'anonymat et la sécurité. Bien que la technologie indique la position, la plateforme permet aux citoyens de collaborer « de manière principalement anonyme » [20] afin de préserver la vie privée. Cela illustre un compromis essentiel : l'adresse GPS est vitale pour l'efficacité des secours, mais elle doit être gérée selon des protocoles transparents.

Dans les études académiques sur la sûreté urbaine, l'apport de la géolocalisation est reconnu pour « améliorer la connaissance de la situation » (situation awareness) et accélérer la réponse aux incidents [2]. Par exemple, après des catastrophes naturelles, l'analyse en temps réel des

localisations de signalements permet de cartographier les zones les plus touchées et de guider les opérations de secours (crowdsourcing en mobilisation des populations). Au bilan, la géolocalisation fournit une dimension spatiotemporelle indispensable : elle précise où et quand un incident se produit, ce qui est critique pour la planification des interventions et la visualisation des données de sécurité.

1.6.4 Impact attendu sur la sécurité communautaire

À long terme, ce modèle devrait améliorer la perception de sécurité dans la ville de Goma. En rapprochant citoyens et autorités autour d'un dispositif transparent, on renouvelle la confiance mutuelle : chaque habitant devient à la fois informateur, validateur et bénéficiaire des alertes sécuritaires. Cette "vigilance partagée" s'appuie sur l'intelligence collective de la communauté ; chacun veille sur son voisin et sur son quartier. De telles approches participatives s'inscrivent dans l'esprit des "villes intelligentes collaboratives", où la technologie sert à renforcer la gouvernance locale et la cohésion sociale. En co-construisant la sécurité, les habitants de la ville de Goma se sentent davantage écoutés et impliqués, ce qui peut contribuer à une meilleure acceptation des mesures de sécurité et à une réduction du sentiment d'insécurité. En somme, le système de validation hiérarchisé devient plus qu'un simple outil technique : c'est un levier sociotechnique pour renforcer la gouvernance locale, la réactivité des services et la cohésion communautaire par la participation citoyenne.

1.7 Conclusion partielle

Ce chapitre constitue le fondement progressif du projet. Il est parti d'un constat contextuel précis (les limites des systèmes traditionnels à Goma) pour construire une réponse conceptuelle structurée autour du crowdsourcing, de la citoyenneté numérique, de la géolocalisation et d'un modèle de validation hybride. Sur la base de ces exigences, le chapitre suivant abordera la phase d'analyse et conception du système, en définissant l'architecture technique et les choix méthodologiques.

Chapitre 2 Analyse et conception du système

2.1 Introduction

Ce chapitre explore les fondements nécessaires à la mise en œuvre d'un système de signalement des incidents basé sur la géolocalisation et adapté au contexte de Goma. Il couvre l'analyse des besoins et la modélisation du système, tout en mettant en avant les solutions envisagées pour répondre aux défis identifiés.

2.2 Analyse des besoins

L'analyse des besoins est une étape clé du développement logiciel. Elle permet de définir précisément ce que le système doit faire pour répondre aux attentes des utilisateurs et aux contraintes du projet. Une bonne définition des besoins guide toutes les phases suivantes, de la conception aux tests, et contribue à la réussite du projet en limitant les risques et en garantissant la qualité finale de l'application.

2.2.1 Identification des acteurs

L'analyse des besoins exige une identification rigoureuse des parties prenantes, chacune apportant des attentes spécifiques au système. Pour notre plateforme de signalement, les acteurs principaux sont :

- **Citoyens** : Les citoyens sont les résidents de la ville de Goma qui utilisent l'application pour signaler des incidents et consulter les informations liées à la sécurité dans leur Zone. Ils participent également à la validation communautaire des signalements en réagissant aux incidents proches de leur position à travers un système de vote simple (like ou dislike)
- **Sentinelles** : Les sentinelles sont également des résidents de Goma, sélectionnés sur la base de leur fiabilité. Elles disposent des mêmes fonctionnalités que les citoyens pour signaler et consulter les incidents, mais assument en plus un rôle de modération. Leur

mission consiste à examiner les signalements, vérifier leur cohérence, éviter les doublons et contribuer à la validation des informations avant leur transmission aux autorités.

- **Administrateurs** : Les administrateurs qui sont aussi les autorités représentent les acteurs institutionnels du système. Elles reçoivent les signalements confirmés ou escaladés par le système afin de planifier et coordonner les interventions nécessaires. Leur rôle est d'assurer une prise en charge opérationnelle des incidents signalés sur le terrain.

2.2.2 Besoins fonctionnels

Les besoins fonctionnels décrivent les fonctions que doit offrir le système [31]. Ils sont énoncés sous forme d'actions à l'infinitif, correspondant aux services attendus. Le système doit permettre :

❖ Authentification des utilisateurs

Pour garantir la sécurité des données, chaque utilisateur (citoyen, sentinelle, administrateurs) doit se connecter avec un identifiant unique (à l'instar de son adresse mail) et un mot de passe, avec une option de récupération de ce dernier en cas d'oubli.

❖ Signaler et géolocaliser un incident

Permettre la création rapide d'alertes incluant une description textuelle, la catégorisation de l'incident et l'ajout de preuves multimédias (photo, audio, vidéo). Le système doit assurer la géolocalisation automatique du terminal tout en garantissant l'anonymat du lanceur d'alerte pour sa protection.

❖ Notification et communication

Envoyer automatiquement des notifications aux différents acteurs : un accusé de réception au citoyen ayant soumis le signalement, une alerte aux sentinelles et aux autorités, ainsi qu'une demande de confirmation aux citoyens voisins du lieu de l'incident (rayon ≤ 200 mètres).

❖ **La validation et la modération des signalements**

Une sentinelle peut consulter les signalements soumis, et décider de les valider ou les rejeter avant transmission aux autorités.

Il convient également de préciser qu'à la phase initiale de l'utilisation du système, avant la nomination officielle des premières sentinelles, ce rôle sera attribué par défaut à des personnes reconnues localement, telles que le chef de quartier ou le chef d'avenue. Le système reposera alors sur leur validation, ainsi que sur un mécanisme de modération collective permettant à chaque citoyen d'approuver (like) ou de désapprouver (dislike) un signalement. C'est sur la base de la pertinence des interventions et sur véracité de ses signalements qu'un citoyen se verra attribué le rôle de la sentinelle.

❖ **Visualisation, consultation et analyse**

Afficher les incidents et leurs statuts sur un tableau de bord intégrant une carte interactive, des tableaux et des graphiques. Consulter la carte publique des incidents pour permettre aux citoyens d'être informés des alertes dans leur zone. Filtrer, trier et rechercher les signalements selon différents critères (date, type, gravité, statut de validation) pour faciliter l'analyse historique et opérationnelle, Consulter l'historique complet des signalements.

❖ **Gestion des utilisateurs**

Le système offre à l'administrateur la possibilité d'attribuer les rôles, de modifier ou de supprimer des comptes utilisateurs, assurant ainsi une gestion centralisée des informations. Les

administrateurs peuvent mettre à jour les informations des sentinelles, telles que leurs spécialités, afin de garantir que les recommandations soient toujours pertinentes.

2.2.3 Besoins non-fonctionnels

Les besoins non-fonctionnels définissent les qualités et contraintes du système, souvent décrites par la norme ISO 25010 [32]. Voici les points clés :

- ❖ **Adéquation fonctionnelle** : le système doit fournir précisément les fonctionnalités spécifiées [32]. Chaque cas d'usage doit être pris en charge par un formulaire approprié et une réponse dédiée.
- ❖ **Performance et efficience** : l'application doit être rapide et économe en ressources [32] La RDC compte environ 53 millions d'abonnements mobiles (51,4% de la population) mais seulement 27,2% d'utilisateurs Internet [33]. Il est donc crucial de minimiser la consommation de données et de prévoir un mode hors-ligne pour stocker temporairement les signalements en l'absence de réseau. Les temps de réponse (chargement de carte, envoi d'alerte) doivent rester faibles même sur des smartphones bas de gamme et réseaux lents.
- ❖ **Compatibilité** : l'application doit fonctionner sur un large éventail d'appareils. À minima, une version Android (réseau 3G/4G) est indispensable pour toucher la majorité des utilisateurs.
- ❖ **Utilisabilité et accessibilité** : l'interface doit être **intuitive et universelle** [32] Les icônes et textes utilisés doivent être clairs [20], des libellés en langue locale. Des tests utilisateur et des campagnes de formation (via radios, television) aideront à garantir que même les non-informaticiens puissent se servir aisément de l'application. L'ergonomie doit aussi tenir compte des personnes vulnérables (contraste des couleurs, taille de police ajustable) pour être accessible au plus grand nombre.
- ❖ **Fiabilité** : le système doit être robuste et stable [32]. Des tests unitaires et de charge doivent être effectués régulièrement pour détecter les erreurs. En cas de bug ou de perte

de connexion, l'utilisateur doit recevoir un message clair. Une administration technique minimale doit exister pour garantir une haute disponibilité, surtout en période de crise.

- ❖ **Sécurité et confidentialité** : la protection des données et la résistance aux attaques sont critiques [32] Toutes les communications doivent être chiffrées (HTTPS). Les comptes utilisateurs doivent être protégés par une authentification forte.
- ❖ **Maintenabilité et transférabilité** : le code doit être conçu de façon modulaire et documentée [32]. Ceci permet d'ajouter facilement de nouvelles fonctionnalités (ex. modules d'alerte pandémique ou météo) et de faire évoluer l'application sans repartir de zéro.

2.3 Diagramme de cas d'utilisation

Les diagrammes de cas d'utilisations (DCU) sont des diagrammes UML utilisés pour une représentation du comportement fonctionnel d'un système logiciel [34]. Le cas d'utilisation correspond à un ensemble d'actions réalisées par le système en interaction avec les acteurs en vue d'une finalité. L'ensemble des cas d'utilisation permet ainsi de décrire les exigences fonctionnelles d'un système en adoptant le point de vue et le langage de l'utilisateur final [35]

2.3.1 Diagramme de cas d'utilisation de citoyen et de la sentinelle

Ce diagramme présente les fonctionnalités principales accessibles aux citoyens et aux sentinelles. Le citoyen peut signaler un incident (avec catégorisation, description et médias), consulter les incidents, la carte interactive et l'historique, recevoir des notifications, et confirmer les signalements à proximité via des votes. La sentinelle hérite de toutes les fonctionnalités du citoyen à part le vote et dispose en plus de droits de modération : elle peut valider, rejeter un signalement. L'authentification est requise pour accéder aux cas d'usage sécurisés.

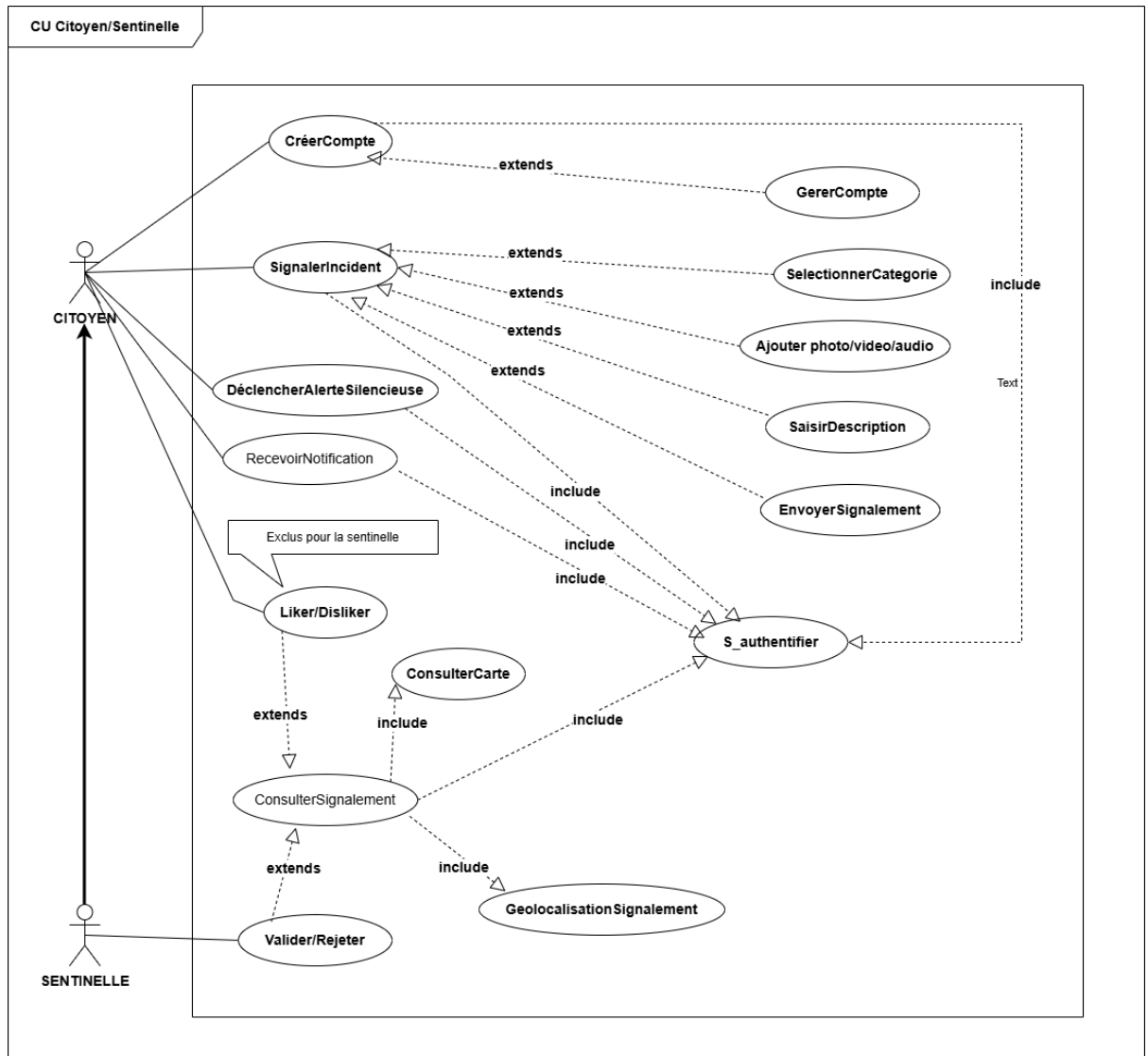


Figure 2-1: Diagramme de cas d'utilisation de citoyen et de la sentinelle

2.3.2 Diagramme de cas d'utilisation d'administrateur

Ce diagramme illustre les actions réservées à l'administrateur. Il peut gérer les comptes utilisateurs (modification, suppression), consulter les signalements avec des actions spécifiques (validation, rejet, résolution), visualiser les statistiques sous forme de tableaux de bord et générer des rapports exportables. Comme pour les autres acteurs, l'authentification est nécessaire pour accéder à ces fonctionnalités. Ces actions permettent à l'administrateur de superviser le système, d'analyser les données et d'assurer la modération globale.

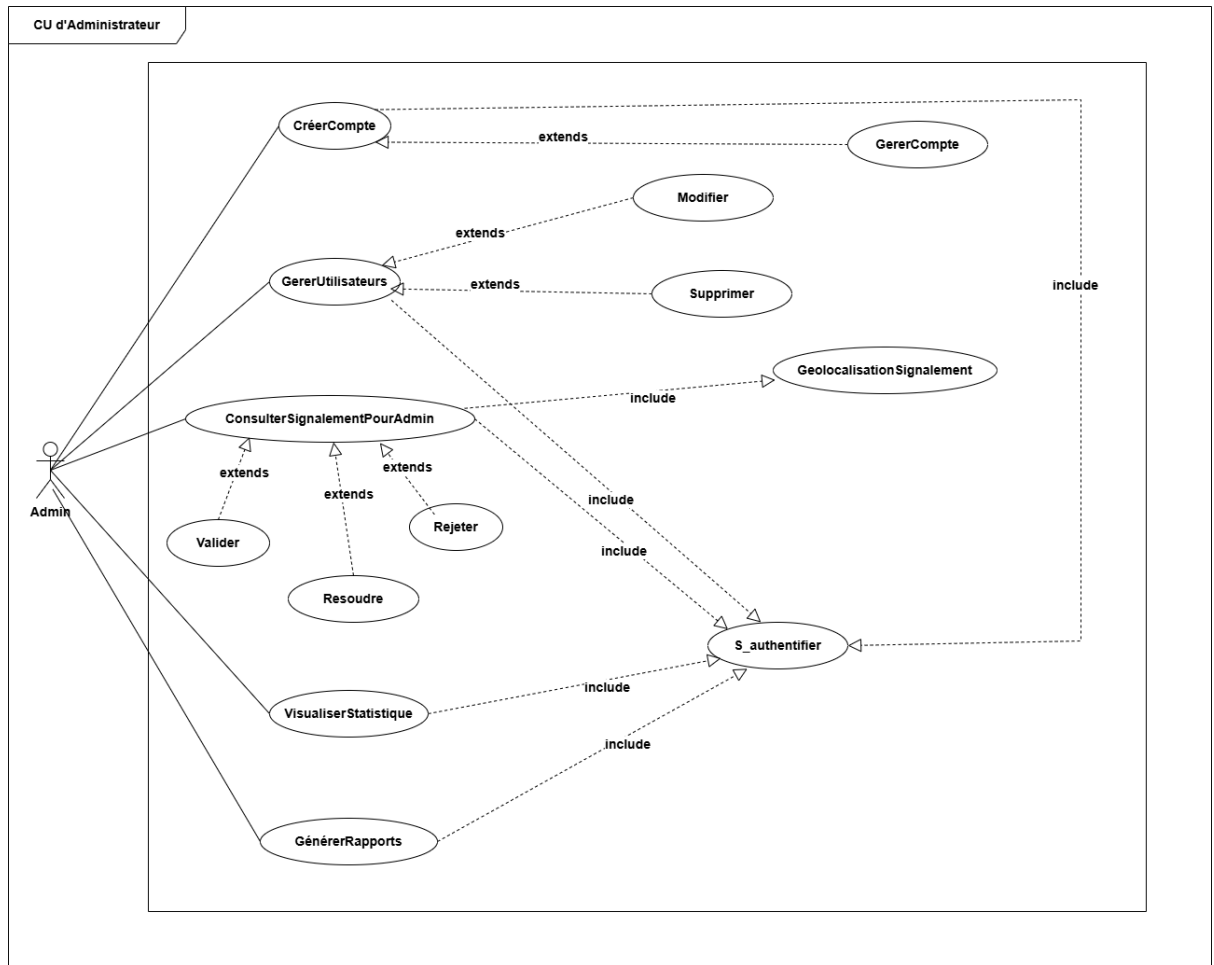


Figure 2-2: Diagramme de cas d'utilisation de l'administrateur

2.3.3 Documentation de différents cas d'utilisation

Notre plateforme propose plusieurs fonctionnalités principales, dont chacune est décrite en détail à travers un cas d'utilisation. La documentation qui suit présente ces cas d'utilisation en explicitant clairement les interactions entre les utilisateurs et le système pour atteindre des objectifs précis

2.3.3.1 Cas d'utilisation (Créer un compte)

Ce cas d'utilisation décrit la procédure permettant à un nouvel utilisateur de rejoindre la plateforme afin de bénéficier des services de sécurité collaborative.

Tableau 2-1: Documentation de cas d'utilisation : "Créer un compte"

ID	CU-01
Nom	Créer un compte
Description	Permet aux nouveaux utilisateurs (Citoyens) de s'inscrire sur la plateforme.
Acteur principal	Tous
Acteur secondaire	Aucun
Préconditions	L'utilisateur doit avoir accès à la page d'inscription.
Enchaînement principal	1) Le CU démarre lorsque l'utilisateur clique sur le bouton "s'inscrire". 2) Il remplit le formulaire (nom, e-mail, téléphone, mot de passe, quartier). 3) Le système vérifie l'unicité de l'email. 4) Le système crée le compte avec le rôle par défaut "Citoyen". 5) Un e-mail de confirmation est envoyé.
Post condition	Le compte est créé avec statut "Citoyen" et l'utilisateur peut se connecter.
Alternatif	Si les informations sont invalides, un message d'erreur est affiché.

2.3.3.2 Cas d'utilisation (S'authentifier)

Ce cas d'utilisation décrit la procédure d'authentification qui garantit l'accès sécurisé aux fonctionnalités selon le profil de l'utilisateur (Citoyen, Sentinelle ou Administrateur).

Tableau 2-2 : Documentation de cas d'utilisation : "s'authentifier"

ID	CU-2
Nom	S'authentifier
Description	Permet à un utilisateur (Citoyen, Sentinelle, Administrateur) d'accéder aux fonctionnalités sécurisées de la plateforme en vérifiant son identité.
Acteur principale	Tous
Acteur secondaire	Aucun
Préconditions	1. L'utilisateur doit posséder un compte actif dans le système. 2. L'application est lancée et l'utilisateur est sur l'écran de connexion.
Enchaînement principal	1) Le CU démarre lorsque l'utilisateur saisit ses identifiants (e-mail ou téléphone et mot de passe). 2) L'utilisateur clique sur le bouton "Se connecter". 3) Le système récupère le compte associé et vérifie la correspondance du mot de passe (via un mécanisme de hachage). 4) Le système génère un jeton de session (Token) correspondant au rôle de l'utilisateur. 5) L'utilisateur est redirigé vers l'interface principale selon son rôle.
Post condition	L'utilisateur est authentifié et sa session est active.
Alternatif	A1. Identifiants incorrects : Si l'e-mail ou le mot de passe est erroné, le système affiche le message : " l'e-mail ou le mot de passe invalides" et l'accès est refusé. A2. Compte suspendu : Si l'administrateur a banni l'utilisateur, un message indique : "Votre compte a été suspendu pour non-respect des règles.

2.3.3.3 Cas d'utilisation (réinitialiser mot de passe)

Ce cas d'utilisation décrit le processus qui permet de restaurer l'accès à un compte en cas d'oubli des identifiants, via une vérification par courrier électronique.

Tableau 2-3: Documentation de cas d'utilisation : "réinitialiser mot de passe"

ID	CU-03
Nom	Réinitialiser mot de passe.
Description	Permet aux utilisateurs de réinitialiser leur mot de passe en cas d'oubli.
Acteur principal	Tous
Acteur secondaire	Aucun
Préconditions	L'utilisateur doit avoir déjà créé un compte auparavant
Enchaînement principal	1) Le CU démarre lorsque l'internaute clique sur le bouton mot de passe oublié. 2) L'utilisateur accède à la section "Mot de passe oublié". 3) Il entre son e-mail pour recevoir un lien de réinitialisation. 4) Le système envoie un e-mail avec les instructions. 5) L'utilisateur clique sur le lien et entre un nouveau mot de passe. 6) Le système valide et met à jour le mot de passe.
Post condition	Le mot de passe est réinitialisé et l'utilisateur peut se connecter avec ses nouvelles informations.
Alternatif	Si l'e-mail est invalide ou non trouvé, un message d'erreur est affiché.

2.3.3.4 Cas d'utilisation (signaler un incident)

Il s'agit de la fonctionnalité cœur du système, permettant de remonter une alerte géolocalisée enrichie de preuves multimédias vers la communauté proche et les autorités.

Tableau 2-4: Documentation de cas d'utilisation : "Signaler un incident"

ID	CU-04
Nom	Signaler un incident

Description	Permet à un citoyen de signaler un incident dans sa zone.
Acteur principal	Citoyen et sentinelle
Acteur secondaire	Aucun
Préconditions	- Le citoyen est connecté. - La géolocalisation du mobile est activée (pour associer l'incident à des coordonnées). - L'appareil ne doit pas utiliser de logiciel de simulation de position (Mock Location).
Enchaînement principal	1. Le citoyen clique sur l'option "Signalement (+)" dans l'application. 2. Vérification d'intégrité : Le système vérifie la validité du signal GPS. 3. Il choisit le type d'incident (vol, agression, incendie, braquage, etc.) dans la liste. 4. Il saisit une description textuelle et peut ajouter des preuves (photo, audio, vidéo). 5. Le citoyen ou la sentinelle appuie sur "Envoyer Signalement". 6. Le système enregistre le signalement dans la base de données et l'inscrit pour validation par la communauté locale. 7. Le citoyen reçoit une confirmation d'envoi.
Post condition	L'incident est soumis à une validation collaborative locale et transmis aux autorités.
Alternatif	- A1 : Géolocalisation désactivée. Si le GPS n'est pas disponible, l'application demande au citoyen de l'activer. - A2 : Pas de connexion internet: Si le mobile est hors ligne, L'utilisateur peut appeler le numéro d'urgence des autorités. Lorsque les autorités reçoivent l'appel, elles peuvent entrer le numéro de téléphone dans leur base de données pour retrouver l'adresse et les informations de l'appelant. - A3 : Info incomplète. Si le citoyen ne fournit pas les informations obligatoires (type ou description), le système refuse la soumission et indique les champs manquants. - A4 : Détection de Triche (Anti-Spoofing). Si le système détecte une position falsifiée (Mock Location) : la soumission est bloquée, l'incident n'est pas créé et une notification d'avertissement est envoyée à l'utilisateur. - A5 : En Situation critique, Le signalement peut se faire selon le cas d'utilisation CU-10

2.3.3.5 Cas d'utilisateur (Consulter signalement)

Ce cas d'utilisation permet l'affichage des détails d'un incident et déclenche les actions de modération communautaire (like/dislike) pour le citoyen ou de validation (valider/rejeter) pour la sentinelle.

Tableau 2-5: Documentation de cas d'utilisation : "Consulter signalement"

ID	CU-05
Nom	Consulter signalement
Description	Permet à un citoyen de confirmer ou infirmer un incident après avoir reçu une notification, via un système de vote simple (Like/Dislike) et pour la sentinelle de valider ou rejeter un incident.
Acteur principal	Citoyen/Sentinelle
Acteur secondaire	Aucun
Préconditions	1. La localisation est activée 2. L'appareil est connecté à Internet 3. Le système a détecté que l'utilisateur se trouve à $\leq 200m$ d'un incident signalé
Enchaînement principal	1. CU démarre lorsque le système détecte qu'un nouvel incident a été signalé dans un rayon de $\leq 200m$ de la position actuelle de l'utilisateur (Citoyen ou Sentinelle). 2. Le système envoie une notification push sur l'appareil de l'utilisateur avec le message : "Incident signalé près de vous". 3. Le citoyen ou la sentinelle clique sur la notification. 4. L'application s'ouvre automatiquement 5. Le système redirige l'utilisateur vers la carte interactive, qui se centre automatiquement sur les coordonnées de l'incident. 7. L'utilisateur clique sur le marqueur de l'incident sur la carte. 8. Le système affiche une fenêtre contextuelle (pop-up) résumant l'événement avec : • Type d'incident • La distance exacte par rapport à l'utilisateur • Le temps écoulé depuis le signalement 9. L'utilisateur clique sur le bouton "Détails" depuis cette fenêtre contextuelle. 10. Le système ouvre la page détaillée de l'incident et affiche les options spécifiques selon le profil de l'utilisateur:

	▪ Si l'utilisateur est un Citoyen : Le système propose les options de vote : - Like : "Temoin". - Dislike : "fausse alerte" ▪ Si l'utilisateur est une Sentinelle : Le système propose les options de modération : - Valider - Rejeter 10. L'utilisateur sélectionne l'une des options proposées pour évaluer ou modérer l'incident.
Post condition	1. Incident modéré pou citoyen et incident valider ou rejeter pour sentinelle. 2. Lorsqu'une sentinelle valide un signalement, le système marque l'incident comme « validé ». En cas de rejet, l'incident est identifié comme « rejeté », indiquant un possible faux signalement. Dans tous les cas, qu'un signalement soit validé ou rejeté par la sentinelle, il est systématiquement transmis aux autorités. Cette transmission permet aux administrateurs d'effectuer une analyse globale et de procéder à l'archivage des incidents, y compris ceux considérés comme faux signalements.
Alternatif	A1 : Si l'utilisateur s'est éloigné de la zone du signalement +200m (Contrainte GPS) Le bouton de vote est désactivé. Et pour la sentinelle c'est pareil aussi, le boutons de valider et rejeter seront désactivé. A2 : Délai expiré. Si aucune sentinelle n'a valider ou rejeter un signalement dans un petit délai prédéfini (ex: 3 minutes), le cas est pris en charge automatiquement (transmis directement aux administrateurs).

2.3.3.6 Cas d'utilisation (Visualiser les Statistiques)

Ce cas d'utilisation offre à l'administrateur une vision analytique et cartographique de la criminalité pour une meilleure aide à la décision.

Tableau 2-6: Documentation de cas d'utilisation : "Visualiser les Statistiques"

ID	CU-06
Nom	Visualiser les Statistiques
Description	Permet à l'administrateur de consulter en temps réel les indicateurs clés de performance (KPI), les tendances criminelles par heure, mois ou année, par quartier (Heatmap) et l'activité des utilisateurs via un tableau de bord interactif.
Acteur principale	Administrateur
Acteur secondaire	Aucun
Préconditions	- L'administrateur est authentifié. - Des données d'incidents sont présentes dans la base de données.
Enchaînement principal	1. L'administrateur accède au menu "Tableau de Bord". 2. Le système affiche la vue globale par défaut de la Totalité des incidents. La carte thermique des heures à risque et zone à risque). 3. L'administrateur peut appliquer des filtres par (Période : " ", Zone : " ", Type : " ", Statut : " "). 4. Le système met à jour dynamiquement les graphiques et la carte interactive. 5. L'administrateur peut survoler une zone spécifique pour voir les détails précis de ce quartier.
Post condition	L'administrateur a pris connaissance de la situation sécuritaire actuelle sans extraire de document.
Alternatif	A1 : Aucune donnée : Si les filtres sélectionnés ne correspondent à aucun incident, le système affiche un graphique vide avec la mention "Aucune donnée pour cette période/zone/statut/etc.

2.3.3.7 Cas d'utilisation (Générer des Rapports)

Ce cas d'utilisation permet l'extraction de données traitées sous format documentaire pour le compte-rendu officiel auprès des instances supérieures.

Tableau 2-7: Documentation de cas d'utilisation : "Générer des Rapports"

ID	CU-07
Nom	Générer des Rapports
Description	Permet à l'administrateur de créer et télécharger des documents officiels (PDF) synthétisant les incidents et les interventions pour une période donnée, afin de les transmettre à la hiérarchie ou aux autres autorités.
Acteur principale	Administrateur
Acteur secondaire	Aucun
Préconditions	- L'administrateur est authentifié. - La fonctionnalité de visualisation (CU-06) fonctionne.
Enchaînement principal	1. L'administrateur accède au module "Rapports". 2. Il sélectionne le type de rapport (ex: "Rapport Mensuel de Sécurité", "Performance des Sentinelles", "Incidents par Quartier"). 3. Il définit la plage de dates 4. Il clique sur " Télécharger PDF ". 5. Le système compile les données, crée le fichier et lance le téléchargement.
Post condition	Un fichier est stocké localement sur la machine de l'administrateur.
Alternatif	A1 : Échec de génération. Si le volume de données est trop important ou si une erreur serveur survient, le système notifie : "Erreur de génération, Veuillez réduire la plage de dates et réessayer"

2.3.3.8 Cas d'utilisation (Gérer les utilisateurs)

Ce cas d'utilisation offre aux administrateurs les outils nécessaires pour modifier, suspendre ou supprimer les profils des citoyens, des sentinelles au sein de la plateforme.

Tableau 2-8: Documentation de cas d'utilisation : "Gérer les utilisateurs"

ID	CU-08
Nom	Gérer les utilisateurs
Description	Permet à l'administrateur de gérer les comptes des utilisateurs (citoyens et sentinelles).

Acteur principale	Administrateur
Acteur secondaire	Aucun
Préconditions	L'administrateur doit être authentifié.
Enchaînement principal	1) Le CU démarre lorsque l'administrateur accède à la section "gestion des utilisateurs". 2) Il consulte la liste des utilisateurs. 3) Il peut bannir, attribuer un rôle de sentinelle à un citoyen tout comme retrogarder aussi. 4) Le système affiche une liste de citoyens classés par critère (score de fiabilité, etc.). 5) L'administrateur consulte les profils et l'historique d'un candidat (nombre de rapports confirmés/démentis, taux d'accord avec consensus, etc.). 6) L'administrateur clique sur Nommer Sentinelle pour le candidat sélectionné. 7) Le système met à jour le rôle du citoyen en "Sentinelle" et lui envoie une notification de promotion.
Post condition	1. Les informations des utilisateurs sont mises à jour dans la base de données. 2. Le citoyen choisi est promu au rang de Sentinelle. Il dispose désormais des privilèges de validation d'incidents (voir CU-05). Une notification est envoyée pour l'informer du nouveau statut.
Alternatif	A1 : Candidat refuse. Si le citoyen décline le rôle (préférence ou indisponibilité), le système enregistre le refus et le rôle précédent reste actif. A2 : Pas de candidat fiable. Si aucun citoyen n'atteint les seuils de confiance, l'administrateur remet le processus en attente et collecte plus de données (par ex. attendre plus de signalements/votes). A3: Si une modification échoue, un message d'erreur est affiché.

2.3.3.9 Cas d'utilisation (Consulter Signalement pour un administrateur)

Ce cas d'utilisation décrit la prise en charge opérationnelle d'un incident par l'administrateur dès lors qu'il est validé par une sentinelle ou escaladé automatiquement.

Tableau 2-9: Documentation de cas d'utilisation : "Consulter Signalement pour un administrateur"

ID	CU-9
Nom	Consulter Signalement pour un administrateur
Description	Permet à l'administrateur de recevoir, consulter et prendre en charge les signalements qui lui sont transmis par le système (soit par escalade automatique suite à l'absence de validation locale, soit par urgence critique)
Acteur principale	Administrateur
Acteur secondaire	Aucun
Préconditions	- L'administrateur est authentifiée sur la plateforme - Un incident a été signalé (CU-04). - Un incident a été validé par une Sentinelle ou a été escaladé automatiquement par le système (Aucune sentinelle n'a validé ou rejeté l'incident dans le délai configurable, danger de mort imminent).
Enchaînement principal	1. Le système notifie l'autorité qu'un nouveau signalement est disponible (notification push) et visible sur la carte. 2. L'administrateur accède à la liste des "Incidents entrants". 3. Elle sélectionne le signalement pour consulter les détails complets [description, localisation précise, photos/audio, statut de validation, la personne qui l'a signalé, et la sentinelle qui l'a validé s'il y a lieu. Si le signalement a été fusionné avec d'autres (les signalements de même catégorie situés dans un rayon de 50 mètres afin d'éviter les doublons), on ajoute également la liste de toutes les personnes concernées par ces signalements associés]. 4. L'administrateur change le statut de l'incident en "Validé" s'il était "En attente" pour en accuser réception, et en "Résolu" s'il était déjà "Validé" après l'intervention. 5. Le système enregistre l'heure de prise en charge pour les statistiques.
Post condition	L'incident passe au statut "resolu". Les citoyens concernés peuvent être notifiés que les secours sont informés.

Alternatif	A1 : Rejet pour Fausse Alerte. Si après analyse des preuves (médias), l'autorité juge que l'alerte est infondée, elle peut clore l'incident avec le motif "Fausse Alerte".
------------	--

2.3.3.10 Cas d'utilisateur (Déclenchement d'Alerte Silencieuse)

Ce mode d'urgence extrême est conçu pour les situations où la victime ne peut pas manipuler son téléphone, permettant un suivi discret et immédiat.

Tableau 2-10: Documentation de cas d'utilisation : "Déclenchement d'Alerte Silencieuse"

ID	CU-10
Nom	Déclenchement d'Alerte Silencieuse
Description	Permet à une victime sous contrainte (braquage, kidnapping) de lancer une alerte de « Priorité » sans manipuler l'écran, via une combinaison physique, tout en capturant des preuves audios et la localisation.
Acteur principale	Citoyen/sentinelle
Acteur secondaire	Aucun
Préconditions	1. L'application est installée et configurée. 2. Le "Mode Discret" a été paramétré au préalable. 3. L'utilisateur a signé numériquement le "Contrat de Responsabilité" (acceptation des sanctions en cas d'abus de ce type d'alerte). 4. Aucun média ne doit être en cours d'exécution sur le téléphone afin d'éviter que l'alerte ne soit déclenchée par erreur, notamment lors d'une tentative d'augmentation du volume 5. Les permissions (Micro, GPS en arrière-plan) sont accordées.
Enchaînement principal	1. Le CU permet à l'utilisateur de déclencher un signalement juste en appuyant 3 fois sur le bouton volume de son smartphone 2. Le système prévoit un délai de 5 secondes durant lequel l'utilisateur peut annuler le signalement. Passé ce délai, le signalement s'active automatiquement et est confirmé par une courte vibration haptique de 0,5 seconde, sans allumer l'écran du téléphone 3. Le système active le GPS et démarre l'enregistrement "Audio Furtif" le micro reste ouvert durant tout le temps d'intervention.

	4. Le système compile les données et les envoie avec le tag "DANGER DE MORT". 5. Le système active le tracking de la position en temps réel
Post condition	1. Les autorités reçoivent une alerte critique immédiate avec la position et le flux audio. Le téléphone de la victime reste en apparence éteint/verrouillé. 1. Gestion des Abus (Post-incident). Si l'autorité classe l'alerte comme "Fausse Alerte Volontaire" : - 1ère fois : Suspension du compte (30 jours) + Avertissement. - 2ème fois : Bannissement définitif (Blacklist Device ID) + Transmission dossier à la justice.
Alternatif	Signalement normal CU-04.

2.4 Diagramme de séquences

Les diagrammes de séquences sont la représentation graphique des interactions entre les acteurs et le système selon un ordre chronologique dans la formulation Unified Modeling Language [36].

2.4.1 Authentification des utilisateurs

Pour l'authentification des utilisateurs, le diagramme décrit comment un utilisateur peut créer un compte et se connecter au système. Le système vérifie l'unicité de l'email lors de la création et valide les identifiants lors de l'authentification.

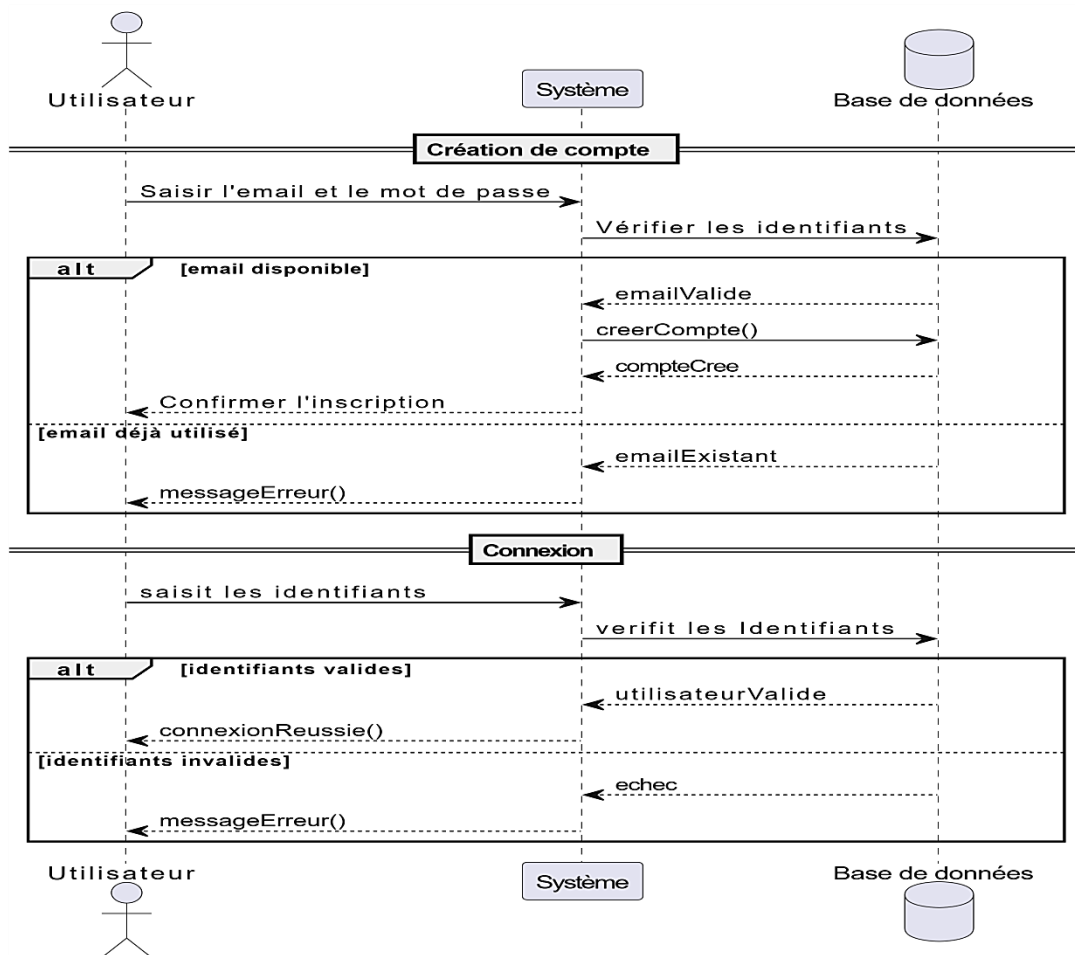


Figure 2-3: Diagramme de séquence du CU créer un compte et du CU s'authentifier

2.4.2 Réinitialiser mot de passe

Ce diagramme de séquence modélise les interactions dynamiques du système lors de la procédure de changement de mot de passe.

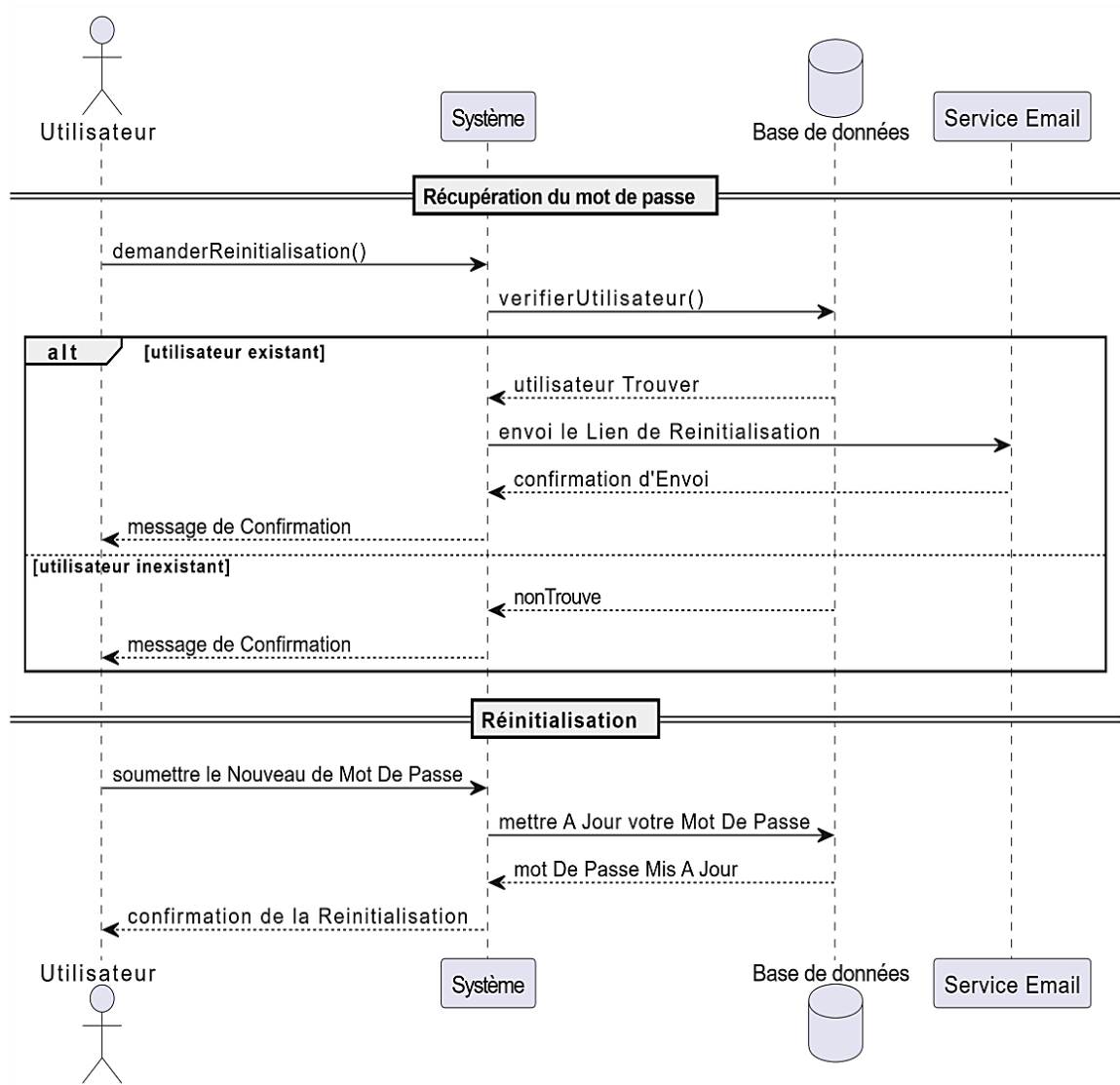


Figure 2-4: Diagramme de séquence du CU Réinitialiser mot de passe

2.4.3 Signaler un incident

Le diagramme décrit comment un citoyen ou une sentinelle peut soumettre un incident via l'application. Le système récupère automatiquement la position géographique de l'utilisateur, enregistre les informations fournies ainsi que les médias associés, puis place l'incident en attente de validation.

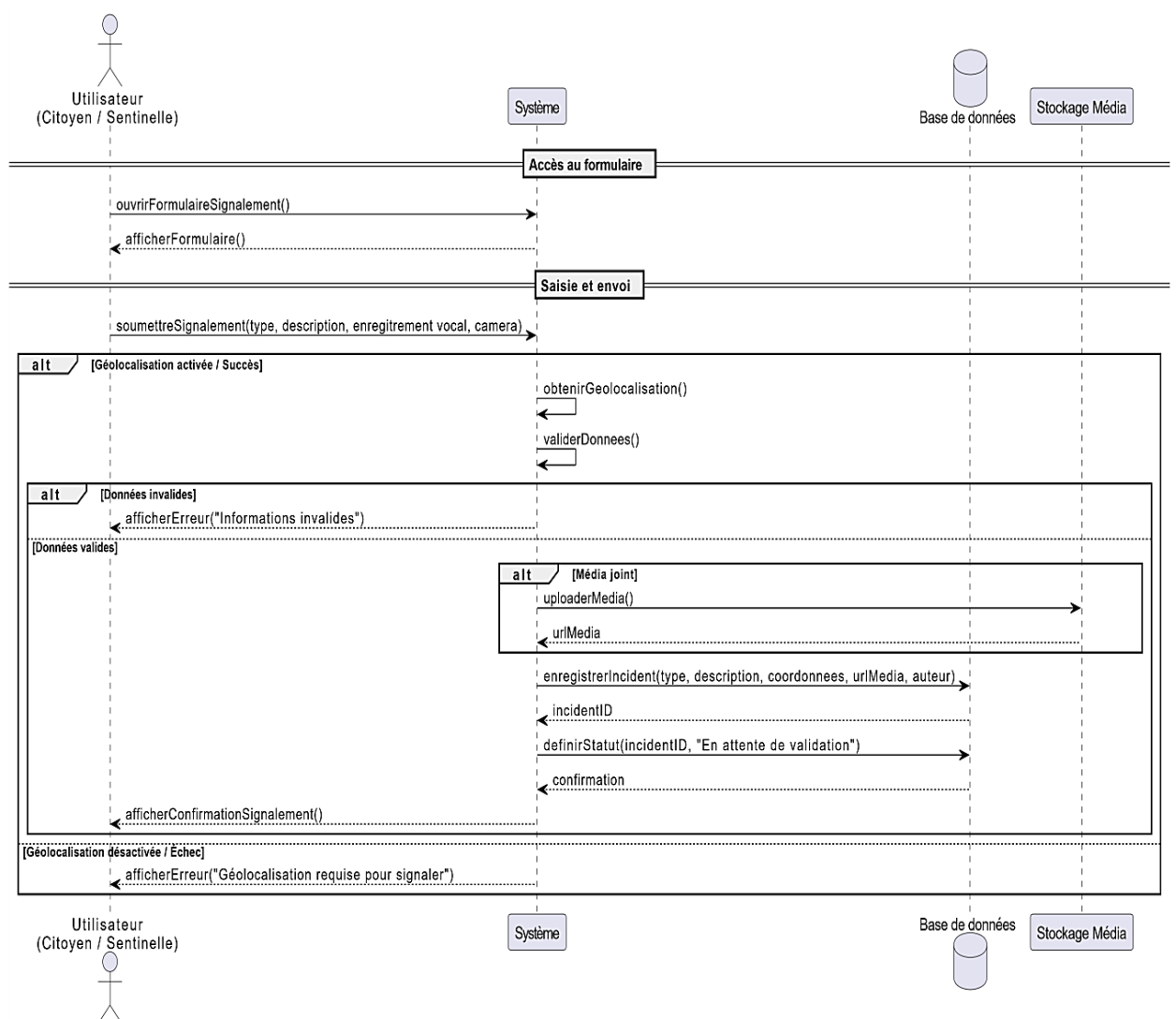


Figure 2-5: Diagramme de séquence du CU signaler incident

2.4.4 Consulter signalement

Le diagramme de séquence décrit comment un citoyen et une sentinelle est informé de la présence d'un incident signalé à proximité de sa position. Après réception d'une notification, il clique dessus, l'application s'ouvre automatiquement sur la carte interactive et permet au citoyen de confirmer ou d'infirmer l'incident à travers un système de vote simple (Like/Dislike) et à la sentinelle de valider ou rejeter le signalement.

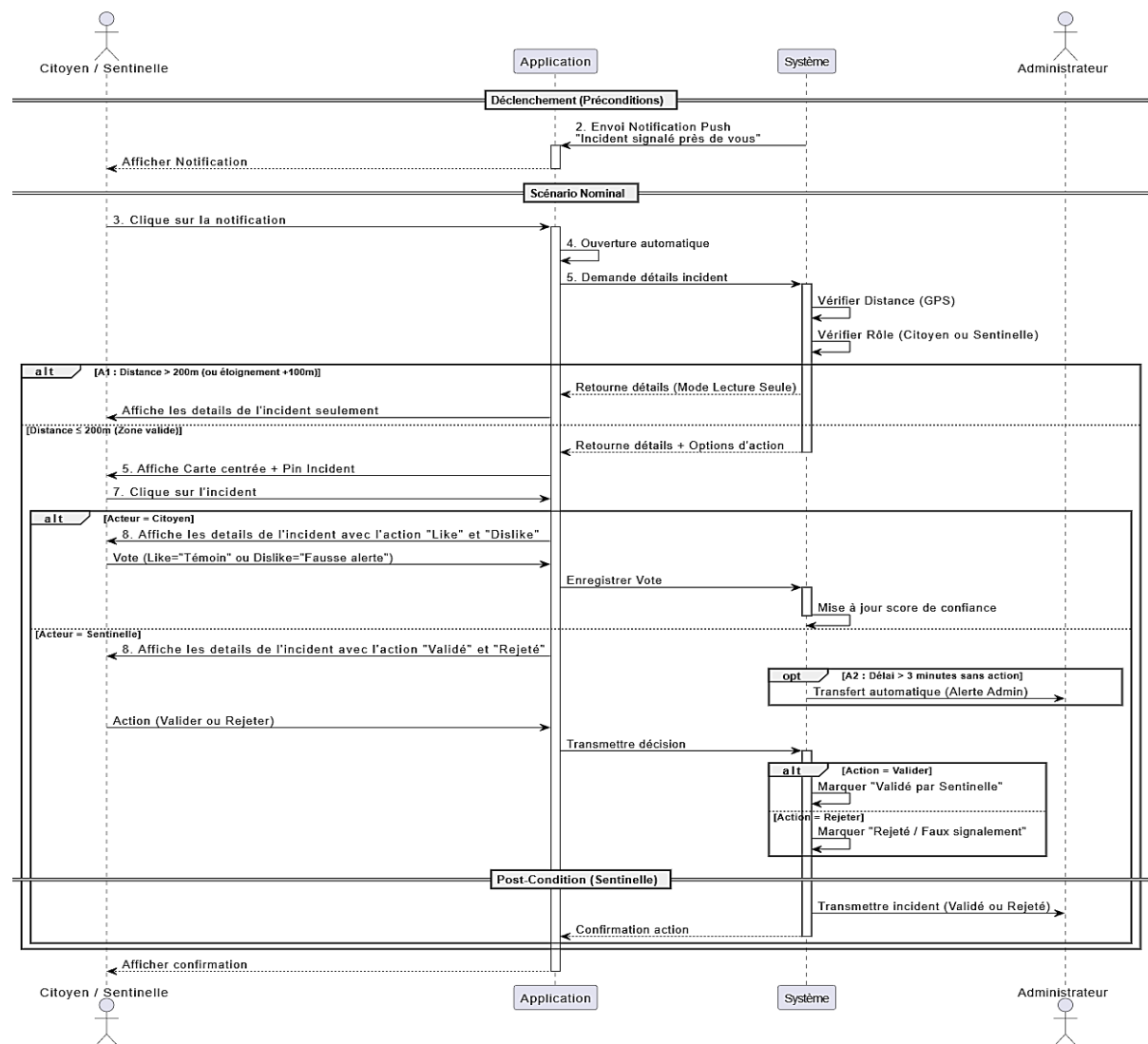


Figure 2-6: Diagramme de séquence du CU Consulter signalement

2.4.5 Visualiser les Statistiques

Ce diagramme de séquence ci-dessous illustre le flux d'interactions permettant à l'administrateur de consulter le tableau de bord. Il détaille le chargement initial des indicateurs de performance (KPI) et de la carte thermique, ainsi que le rafraîchissement dynamique de l'interface lorsque des filtres (période, zone, type) sont appliqués.

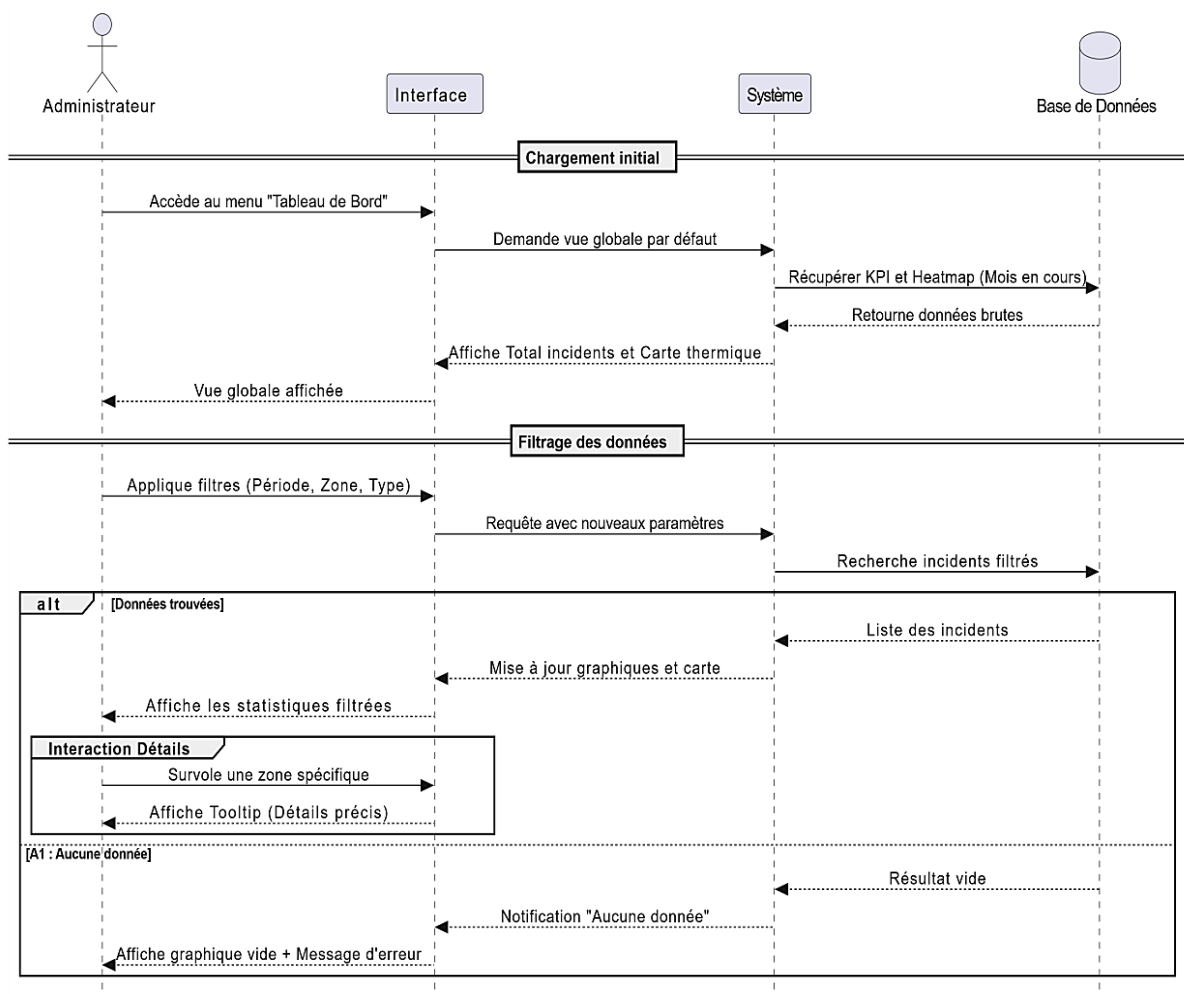


Figure 2-7: Diagramme de séquence du CU Visualiser les Statistiques

2.4.6 Générer des Rapports

Ce diagramme représente le processus de création des documents exportables.

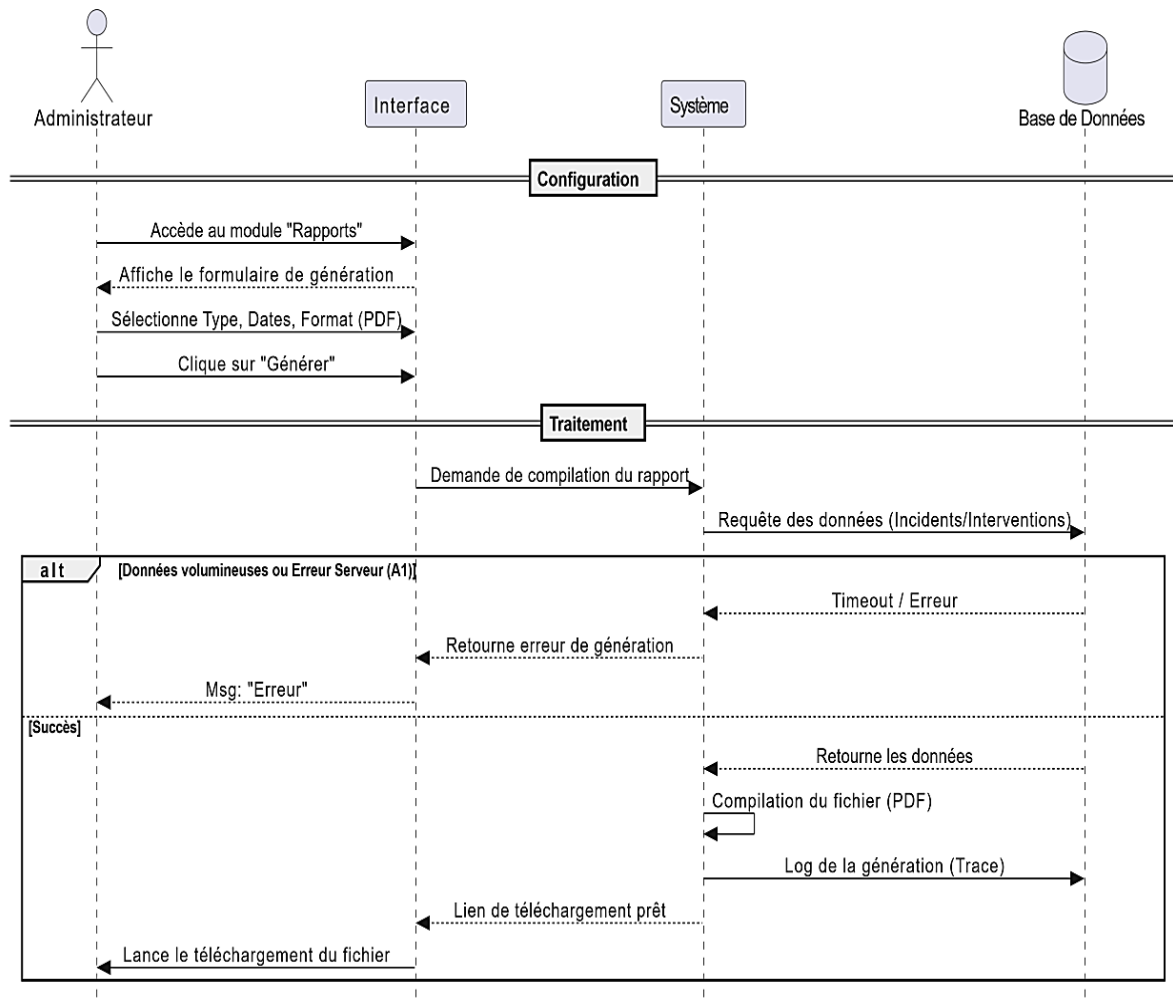


Figure 2-8: Diagramme de séquence du CU Générer des Rapports

2.4.7 Gérer les utilisateurs

Le diagramme de séquence décrit comment l'administrateur accède à l'interface dédiée afin de consulter, modifier ou supprimer les comptes des utilisateurs. Le système enregistre ensuite les modifications effectuées dans la base de données afin de maintenir la cohérence des informations.

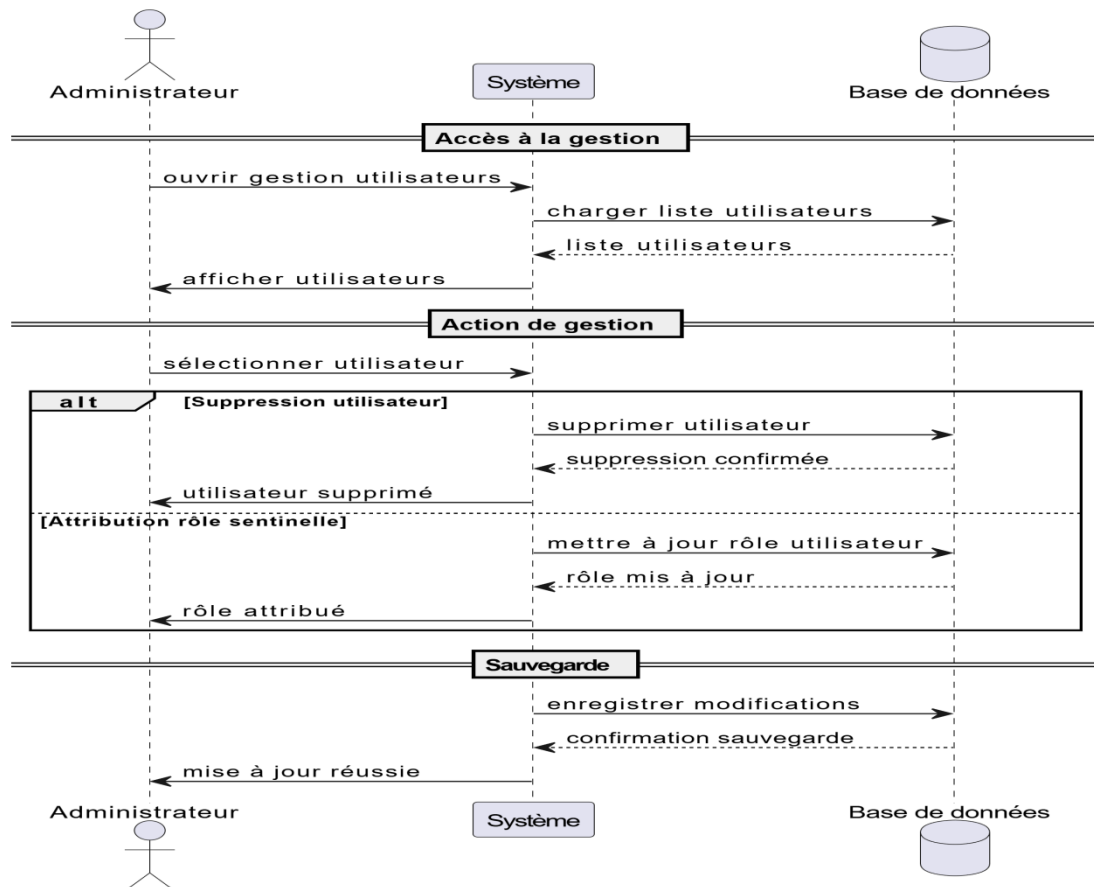


Figure 2-9: Diagramme de séquence du CU Gérer les utilisateurs

2.4.8 Consulter Signalement pour un administrateur

Ce diagramme de séquence détaille les interactions entre l'administrateur et le Système lors de la réception d'un incident, illustrant le passage du signalement de l'état de validation à sa prise en charge opérationnelle ou son rejet éventuel.

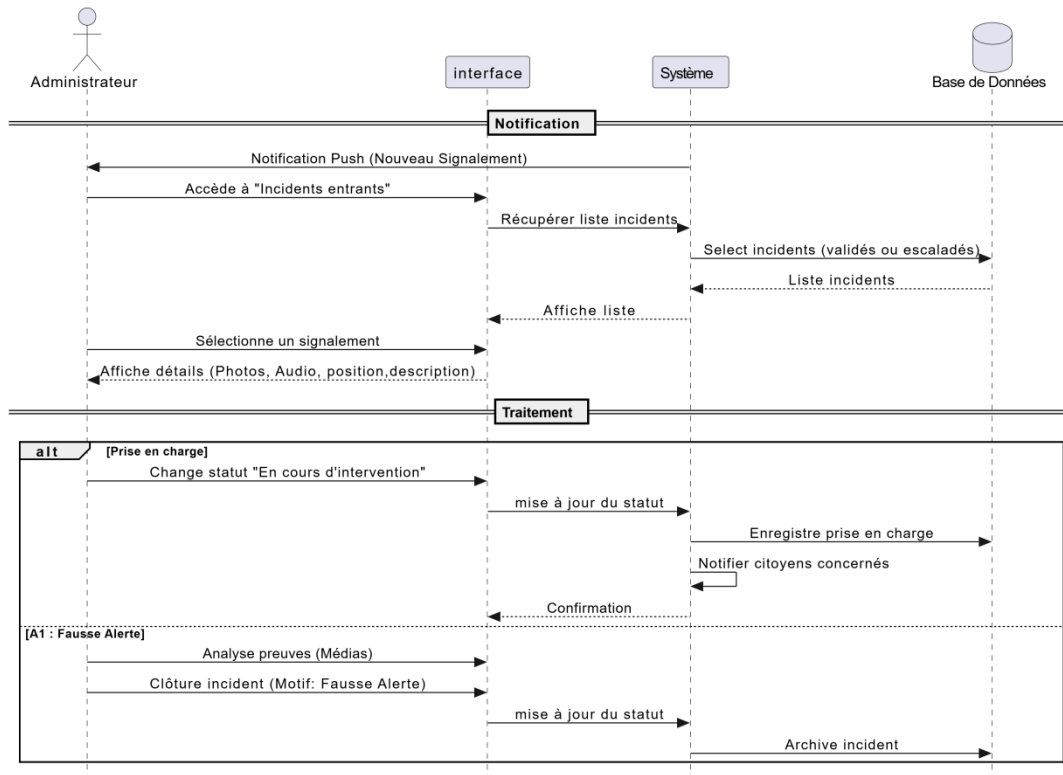


Figure 2-10: Diagramme de séquence du CU Consulter Signalement pour un administrateur

2.4.9 Déclenchement d'Alerte Silencieuse

Le diagramme suivant détaille la séquence d'urgence activée par une interaction physique discrète (boutons volume) qui active les capteurs (micro et GPS) et initie le streaming de données en temps réel vers le serveur sans éveiller les soupçons de l'agresseur.

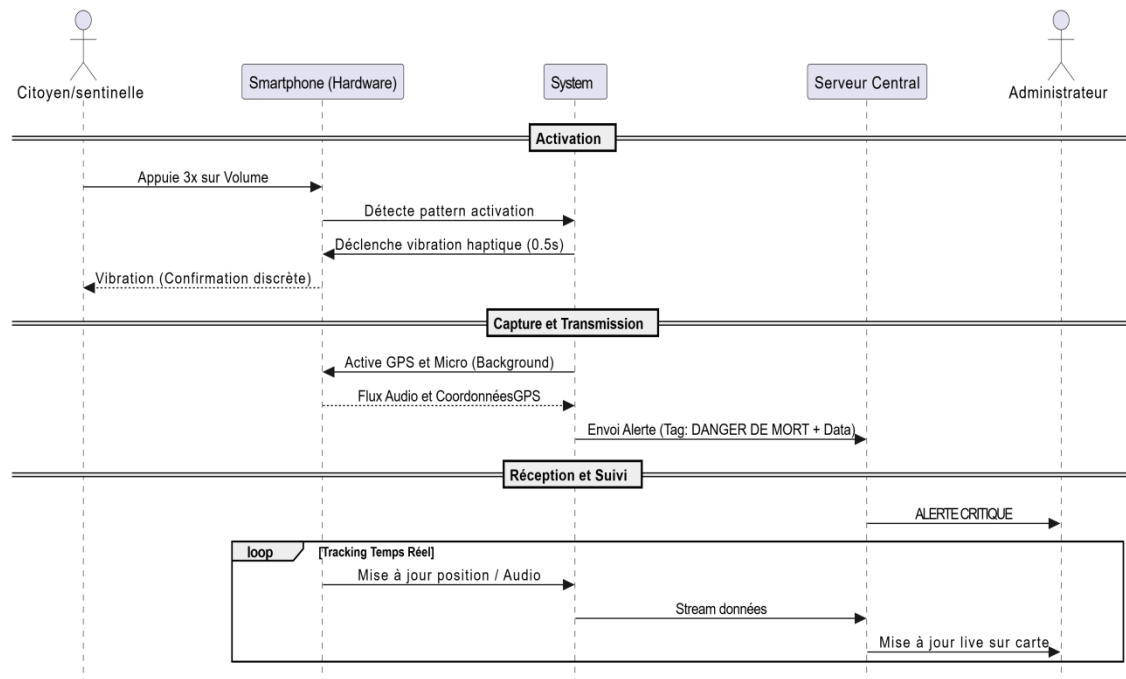


Figure 2-11: Diagramme de séquence du CU Déclenchement d'Alerte Silencieuse

Le diagramme de classes représente la structure statique du système en définissant les différentes classes, leurs attributs, méthodes et les relations entre elles [37].

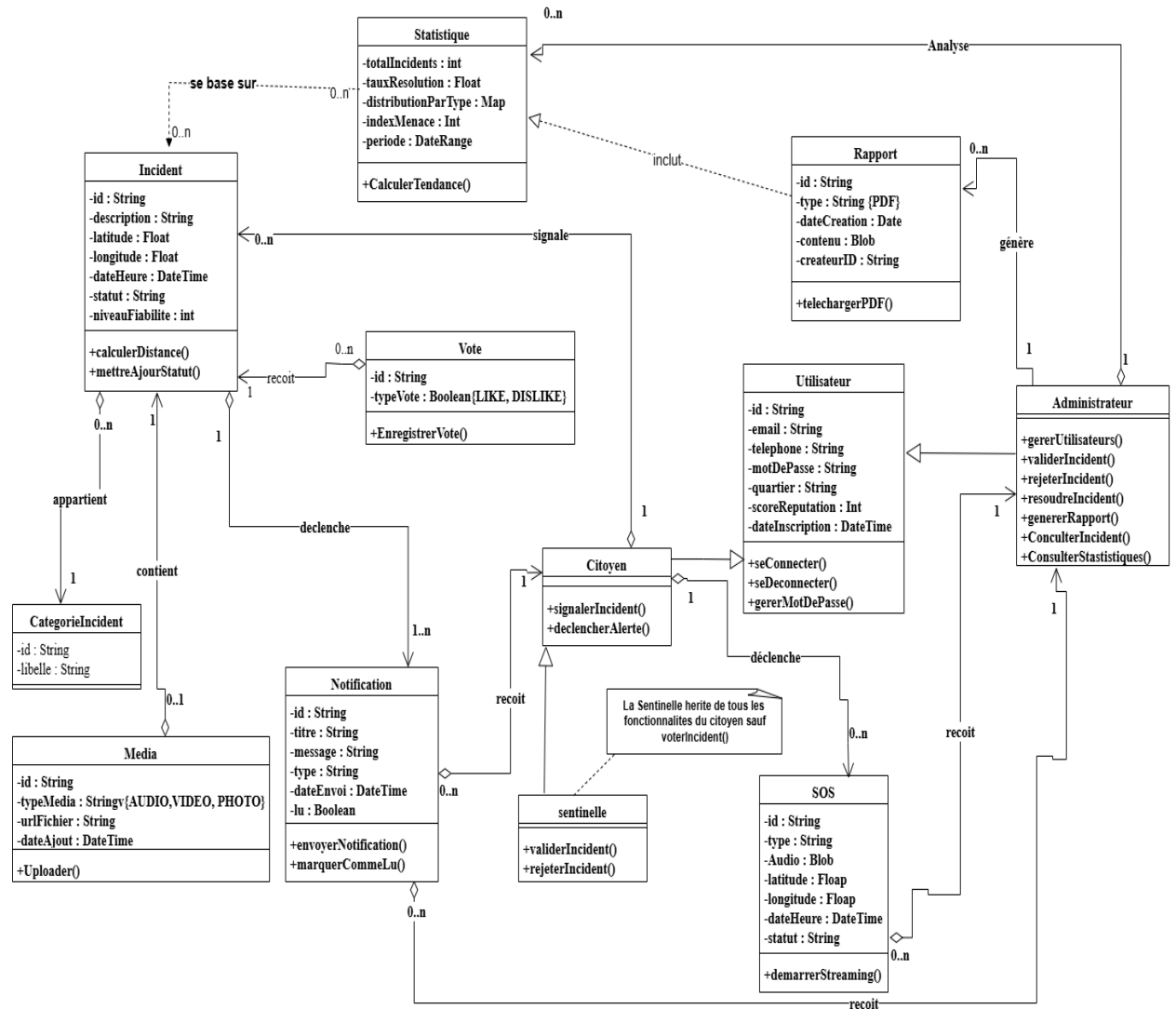


Figure 2-12: Diagramme de classe du système

2.6 Conclusion partielle

Ce chapitre a permis d'identifier les acteurs clés (citoyens, sentinelles, Administrateurs) et de définir leurs besoins. Grâce aux diagrammes de cas d'utilisation, de séquence et de classe, nous avons structuré l'analyse et garanti que la solution répond précisément aux attentes réelles. Cette modélisation constitue une base technique solide pour passer à la phase suivante qui est l'implémentation du système. Cette nouvelle étape consistera à transformer nos modèles théoriques en une solution concrète, en choisissant les technologies adaptées et en développant les fonctionnalités clés pour donner vie à notre application.

Chapitre 3 Implémentation du système

3.1 Introduction

Ce chapitre est consacré à la mise en œuvre technique d'une plateforme participative de signalement des incidents sécuritaires à Goma. Dans la continuité de l'analyse et de la conception présentées au chapitre précédent, nous détaillons ici le processus de matérialisation de la solution. Nous exposerons d'abord l'environnement technologique et les outils sélectionnés, avant d'aborder la configuration de l'infrastructure, le développement des composants front-end et back-end, ainsi que l'intégration des fonctionnalités géospatiales. Enfin, nous présenterons les interfaces, ainsi que les protocoles de tests mis en place pour valider la robustesse de l'application.

3.2 Outils et technologies de développement

Pour garantir performance et maintenabilité, le développement s'appuie sur une pile technologique moderne et open-source :

- ❖ **Front-end** : L'environnement local a été initialisé sous Node.js avec npm, et structuré via l'outil de build Vite. L'interface est développée avec React.js couplé à TypeScript [38]. Ce choix assure un typage statique rigoureux, réduisant les erreurs d'exécution et facilitant la maintenance du code.
- ❖ **Back-end et Base de données** : Nous avons opté pour une architecture Serverless via Supabase (une solution Backend-as-a-Service basée sur PostgreSQL). Au lieu de maintenir un serveur manuel, cette plateforme génère automatiquement notre API sécurisée, gère l'authentification des utilisateurs et assure la synchronisation des données en temps réel [39] [40]. La sécurité des échanges est garantie par l'utilisation de variables d'environnement (fichiers .env), isolant les clés d'API publiques (VITE_SUPABASE_URL) du code source, tandis que la configuration de la base de

données est pilotée via le tableau de bord Supabase. La gestion des utilisateurs via Supabase Auth, a permis de distinguer les rôles (Citoyen, Sentinelle, Administrateur). La sécurité des données est assurée par des politiques de Row Level Security (RLS), restreignant les droits d'écriture et de modification (ex: validation d'un incident) aux seuls rôles autorisés.

- ❖ **Cartographie et Géolocalisation** : Pour la visualisation cartographique, nous avons utilisé Leaflet [41], une bibliothèque JavaScript open-source permettant de créer des cartes interactives, couplée à OpenStreetMap pour le fond de carte. Afin de délimiter visuellement les quartiers, nous avons intégré des données vectorielles au format GeoJSON, Les tracés originaux fournis par OpenStreetMap s'avérant trop volumineux et impactant les performances de rendu, alors nous avons procédé à une adaptation et une simplification manuelle de ces fichiers. En arrière-plan, la gestion des données spatiales est assurée par l'extension PostGIS de PostgreSQL [42], référence en matière de systèmes d'information géographique (SIG). Son activation a permis l'intégration du type de données GEOGRAPHY(POINT), essentiel pour le stockage et l'indexation spatiale des coordonnées GPS.
- ❖ **Déploiement** : La gestion du code source est assurée par Git et hébergée sur GitHub, favorisant un travail collaboratif structuré par branches. Le déploiement est automatisé via Vercel : chaque fusion (merge) sur la branche principale déclenche un pipeline de construction (build) et de mise en production [43]. Vercel gère également l'injection sécurisée des variables d'environnement en production, garantissant un déploiement fluide et sécurisé.

3.3 Architecture du Système et Échanges de Données

L'application est structurée selon une architecture basée sur les composants (Component-Based Architecture), orchestrée par le point d'entrée App.tsx. Pour garantir une séparation stricte des responsabilités, le système utilise le modèle “Service-Component”. Les composants d'interface (comme IncidentForm.tsx ou MapView.tsx) ne communiquent jamais directement avec la base

de données. Ils délèguent toutes les opérations logiques au fichier `services/supabase.ts`, qui agit comme une couche d'abstraction. Cela permet de centraliser la gestion des erreurs, le typage TypeScript des données et la logique métier avant tout appel réseau.

3.3.1 Flux de Données Montant (Client vers Serveur)

Lorsqu'un utilisateur soumet un incident, le système opère une transaction en deux étapes via le protocole HTTPS sécurisé. D'abord, les fichiers multimédias (photos ou audio capturés via l'API native du navigateur) sont convertis en objets binaires (Blobs) et envoyés vers le module de stockage de Supabase. Une fois l'URL publique du fichier obtenue, le service injecte les métadonnées (type d'incident, coordonnées GPS précises, description) dans la table relationnelle incidents via une requête REST (POST).

3.3.2 Flux de Données Descendant et Synchronisation Temps Réel

Contrairement à une architecture classique qui nécessiterait un rafraîchissement manuel, le système utilise un canal de communication bidirectionnel persistant. Le composant racine `App.tsx` initialise un écouteur d'événements sur le canal `postgres_changes`. Dès qu'une modification survient dans la base de données, le serveur pousse instantanément la nouvelle donnée (payload JSON) vers tous les clients connectés. L'état global de l'application (React State) est alors mis à jour, provoquant le re-rendu immédiat de la carte et du fil d'actualité sans intervention de l'utilisateur.

3.4 Présentation des interfaces de l'application

Après avoir détaillé l'architecture technique et les choix d'implémentation, il convient à présent d'exposer la dynamique fonctionnelle de la plateforme GomaSecure. Cette section illustre le parcours utilisateur et les interactions possibles au sein du système. Nous décrirons les scénarios d'utilisation clés, allant de l'authentification à la visualisation géospatiale des menaces, en passant par le processus critique de soumission et de validation des alertes. Cette présentation met en lumière l'ergonomie de la solution et sa capacité à répondre aux exigences de vigilance communautaire définies précédemment.

3.4.1 Interface d'authentification

L'entrée dans l'écosystème GomaSecure est conditionnée par une authentification rigoureuse, garantissant la traçabilité des actions et la fiabilité de la communauté. L'utilisateur entre son adresse email et son mot de passe pour accéder au système, comme l'illustre la Figure 3-1.

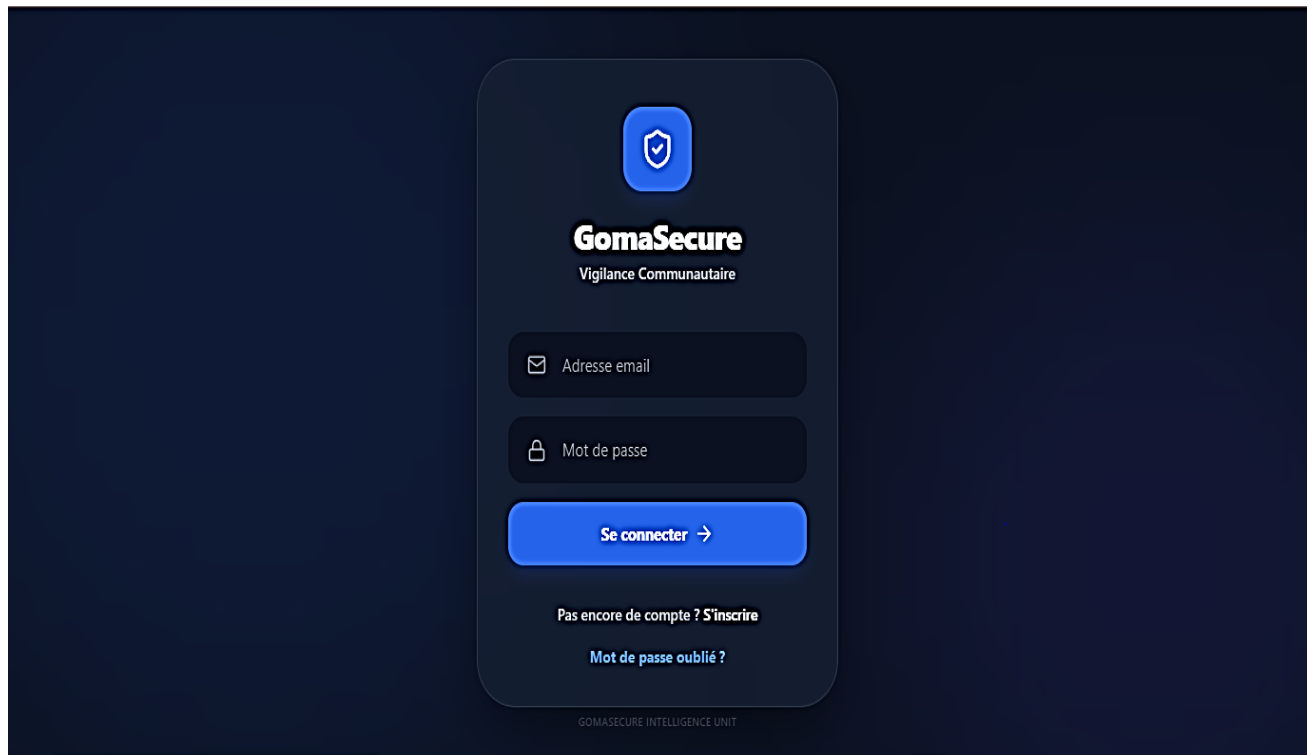


Figure 3-1: Interface d'authentification à la plateforme

3.4.2 Interface d'inscription des citoyens

Cette interface, montrée à la Figure 3-2, permet à un nouveau citoyen de s'inscrire sur la plateforme en remplissant un formulaire de création de compte. Les informations saisies sont ensuite validées et enregistrées dans la base de données afin d'activer l'accès personnalisé.

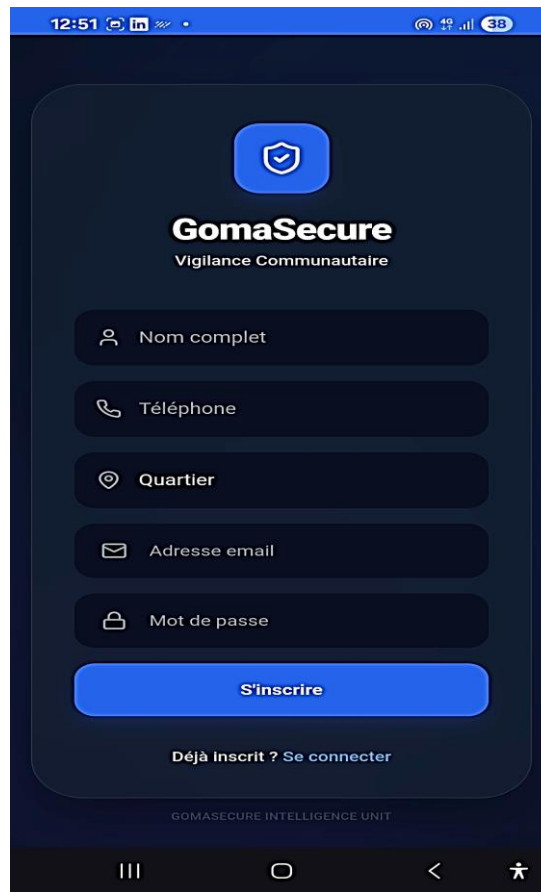


Figure 3-2: Interface d'inscription des citoyens

3.4.3 Interface de signalement d'incident

Le module de signalement constitue le cœur opérationnel de notre application. L'objectif ergonomique principal est de minimiser la charge cognitive et le temps de saisie pour un utilisateur potentiellement en état de stress. De plus, afin de garantir l'inclusivité envers les populations peu familiarisées avec le numérique ou éprouvant des difficultés à l'écrit, l'interface privilégie l'enregistrement vocal.

La Figure 3-3 présente le formulaire de soumission qui s'articule autour de trois actions rapides : la sélection catégorielle de l'incident (Vol, Incendie, Agression, etc.), la capture de preuves multimédias (audio, photo ou vidéo) et la saisie optionnelle d'une description. Lors de la soumission, l'application sollicite l'API de géolocalisation du navigateur pour capturer les coordonnées exactes (latitude/longitude) de l'utilisateur. Ces données sont formatées en objets

spatiaux PostGIS et insérées en base de données via l'API Supabase. La figure se décompose en deux états : a) présente le formulaire vierge à l'ouverture, tandis que b) montre le formulaire complété, prêt pour la transmission du signalement.

Parallèlement, les fichiers multimédias (audios, photos, videos) sont envoyés vers un conteneur Supabase Storage sécurisé, dont l'URL est liée à l'enregistrement de l'incident. Ce processus garantit l'intégrité et la contextualisation géographique de chaque alerte.

The figure displays two screenshots of the GomaSecure mobile application interface for incident reporting. Both screenshots show the same layout with a top status bar, a header with the app name 'GomaSecure', and a bottom navigation bar with icons for 'Carte', 'Liste', a central '+' button, 'SOS', and 'Profil'.

Screenshot a) - Empty Form: The 'TYPE D'INCIDENT' section contains seven buttons: 'Vol', 'Agression', 'Incendie', 'Accident', 'Enlèvement', 'Alerte SOS', and 'Autre'. The 'PROOFS' section has three options: 'AUDIO' (a large red button), 'Caméra', and 'Galerie'. The 'DÉTAILS' section has a text input field with the placeholder 'Décrivez la situation (lieu précis, nombre de personnes...)'. At the bottom is a large grey button labeled 'Envoyer Signalement'.

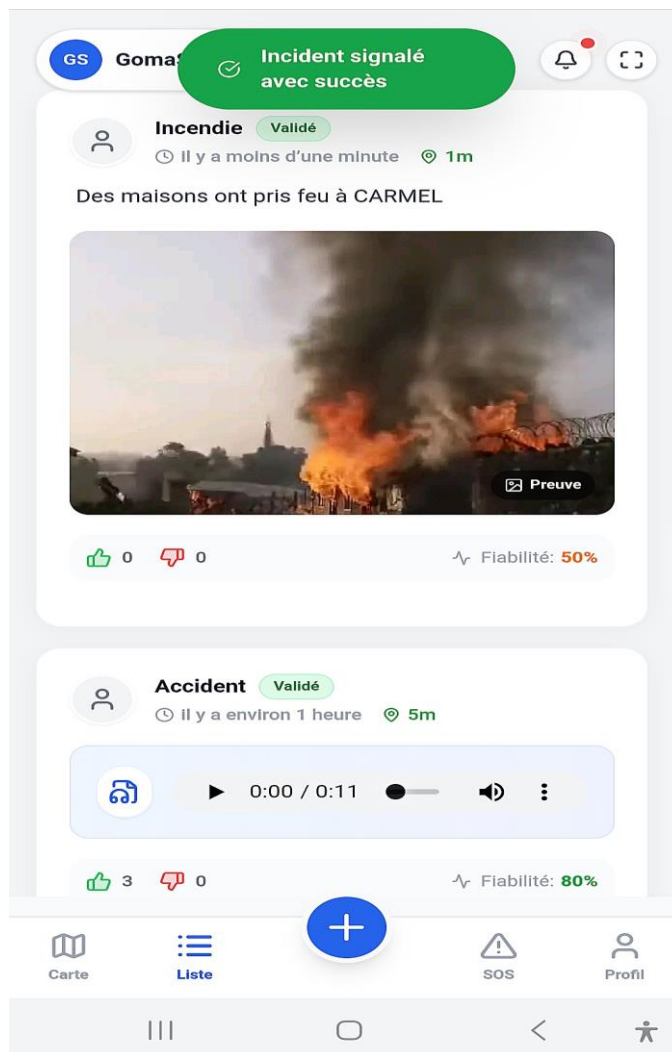
Screenshot b) - Filled Form: The 'TYPE D'INCIDENT' section has 'Incendie' selected. The 'PROOFS' section has a photo of a fire uploaded. The 'DÉTAILS' text field contains the text 'Des maisons ont pris feu a CARMEL'. The 'Envoyer Signalement' button is now dark blue.

a)

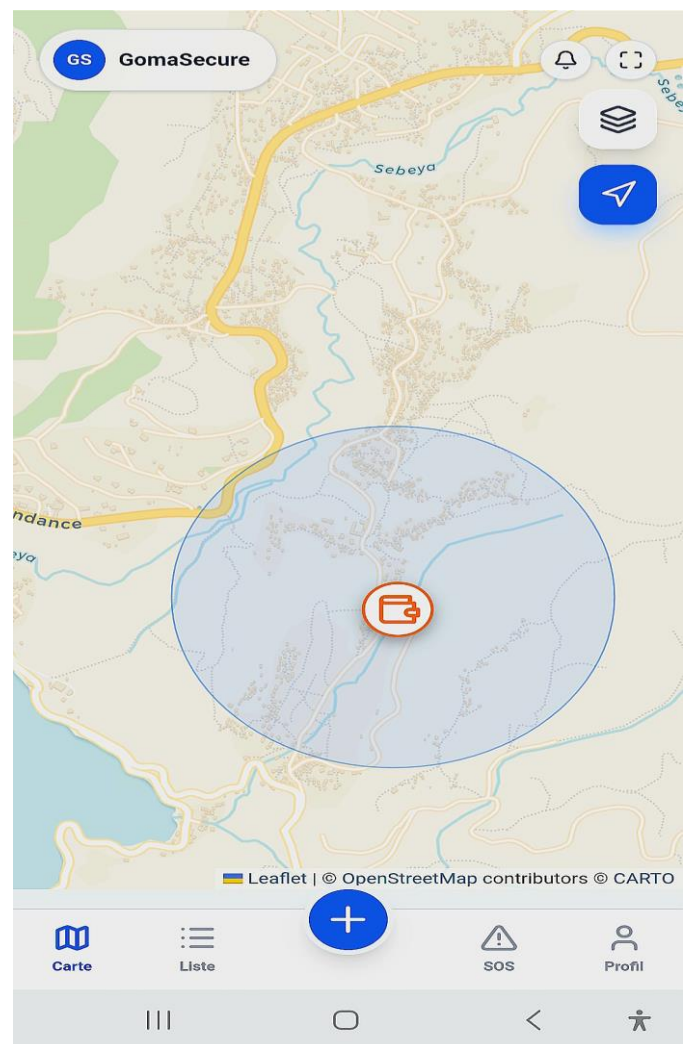
b)

Figure 3-3: Interface du formulaire de signalement d'incident

Sur la *Figure 3-4*, a) On remarque que l'incident est validé instantanément lors de son signalement. Cela s'explique par le fait que tout signalement émis par une sentinelle est considéré comme authentique par défaut. Par contre sur b) On peut voir que l'incident présente une couleur orange après son émission, cela s'explique par le fait que le signalement en question était émis par un citoyen standard, ce qui indique qu'il est en attente de validation. Son statut est donc "En attente".



a)



b)

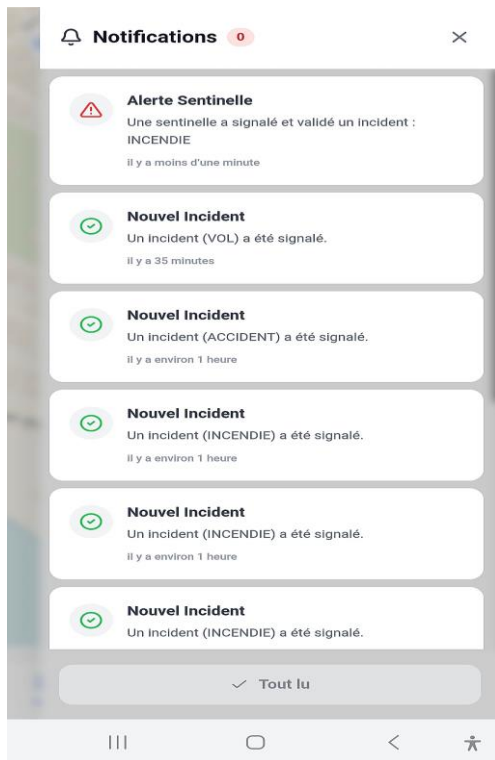
Figure 3-4: Interface d'incident signaler

3.4.4 Interface de consultation des signalements

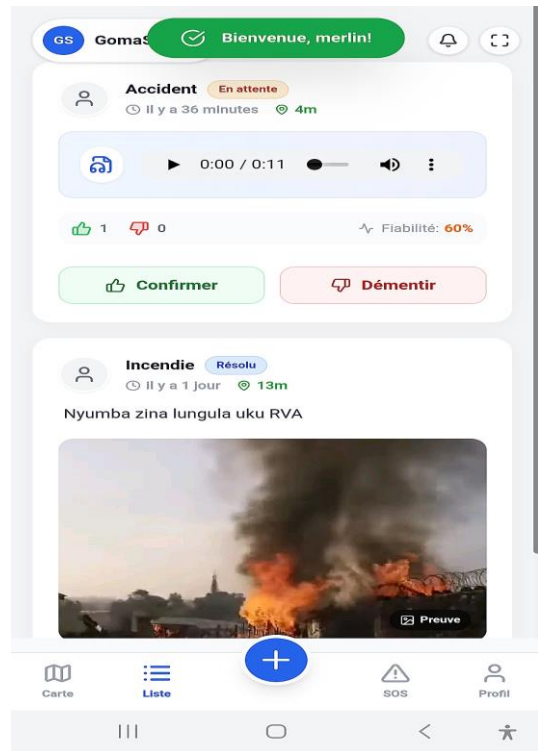
Une fois l'incident signalé, il devient visible pour la communauté locale via une interface de consultation interactive. La Figure 3-5 montrent comment l'information est restituée aux citoyens et aux sentinelles, une carte dynamique permet de situer l'événement, accompagnée d'une fiche détaillée contenant les preuves visuelles ou sonores. C'est ici qu'intervient le mécanisme de validation participative. L'interface propose des boutons d'interaction (“Confirmer” ou “Démentir”) permettant aux citoyens proches de corroborer les faits, comme sur la Figure 3-5 b).

Pour les utilisateurs disposant du rôle de “Sentinelle “, des options de modération avancées (Valider/Rejeter) apparaissent, permettant de filtrer les fausses alertes Figure 3-5 c). Sur la Figure 3-5 d), à l'inverse, on constate que l'interaction avec l'incident est impossible. Cette restriction repose sur une contrainte de proximité géographique : le système suppose qu'au-delà d'une certaine distance, un utilisateur n'est pas en mesure de juger de la véracité d'un incident (par exemple, un accident). Cette sécurité empêche les validations arbitraires effectuées par des personnes non présentes sur les lieux.

Sur la Figure 3-5 a), on observe ici l'interface des notifications. La notification d'un incident signalé par une sentinelle se distingue des autres par son caractère prioritaire, car elle est jugée fiable par défaut. Bien que cet incident ne nécessite aucune interaction supplémentaire de la part des utilisateurs à proximité (son statut étant déjà “ Validé ” dès sa soumission), il demeure visible pour l'ensemble de la communauté. Cette visibilité immédiate répond à un impératif de sécurité publique, informer en temps réel les personnes situées dans la zone de danger afin de les protéger et de renforcer leur vigilance face à une menace confirmée. Ce rôle modérateur est contrôlé par l'authentification et les rôles définis dans la base. Des politiques RLS (Row Level Security) ont été établies pour que seuls les utilisateurs avec le rôle approprié puissent modifier le champ de validation.



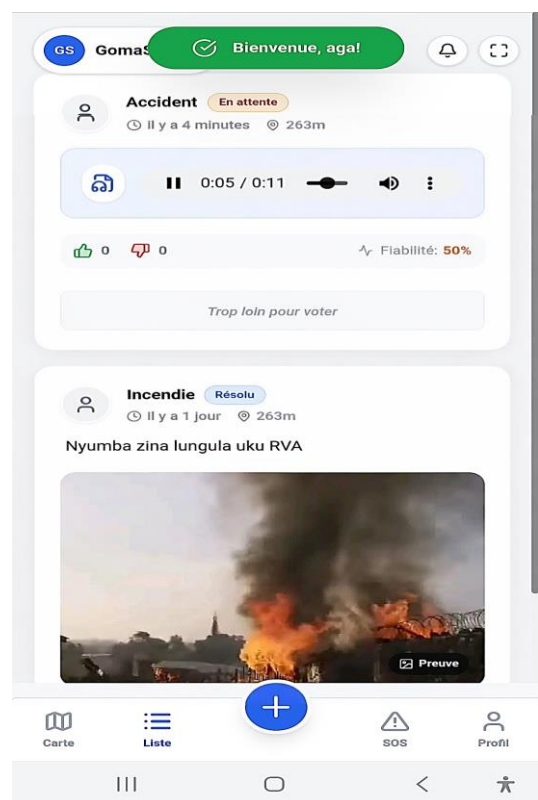
a)



b)



c)



d)

Figure 3-5: Interface de consultation des signalements

3.4.5 Interface de consultation des signalements pour administrateur

Cette interface est le centre névralgique. Elle présente une vue cartographique globale de tous les incidents en cours. Contrairement à la vue citoyenne, l'administrateur dispose ici d'outils de filtrage avancés (par statut, par urgence, par quartier, etc.) et de la capacité de modifier le statut d'un incident (de "En attente" ou "validé" à "Résolu" ou "Rejeté") après intervention.

L'écran est structuré en trois zones principales pour faciliter la prise de décision rapide :

- Le Menu Latéral (à gauche) : Il permet une navigation rapide entre les modules d'administration. L'icône « Personnages » permet d'accéder à la gestion des utilisateurs, tandis que l'icône « Entonnoir » ouvre les filtres pour trier les incidents sur la carte. Et en cliquant sur l'icône de diffusion, une fenêtre s'ouvre vous permettant de rédiger et d'envoyer une alerte ciblée aux utilisateurs du quartiers selectionners ou tous les utilisateurs de la ville.
- La Cartographie Centrale : Elle constitue l'élément principal du centre de commandement. Elle affiche la localisation géospatiale des incidents signalés ainsi que leur répartition par quartiers. Les zones sont délimitées et peuvent être visualisées sous forme de superposition ou de carte thermique afin d'identifier les secteurs les plus touchés. Chaque incident est représenté par un marqueur interactif. En cliquant sur celui-ci, une fenêtre contextuelle s'affiche (comme illustré dans la Figure 3-6 pour l'incident "Incendie"), présentant un résumé comprenant le type d'incident, l'heure de signalement, une brève description, le statut (par exemple "Validé") ainsi qu'un bouton d'action « Voir détails » permettant d'accéder aux informations complètes.
- Le Flux d'Incidents (à droite) : Cette liste latérale présente les signalements par ordre chronologique inversé.

Chaque incident affiché dans le flux ou sur la carte possède un indicateur de statut coloré, informant l'administrateur de l'état de traitement de l'alerte :

Orange (EN ATTENTE), signale un incident récemment rapporté qui n'a pas encore été corroboré. Il nécessite une vérification par une Sentinelle ou par le vote de la communauté. Vert (VALIDÉ), indique qu'un incident a été confirmé par une Sentinelle (Validé). Ces incidents sont considérés comme des informations fiables. Bleu (RÉSOLU), indique qu'un incident a été résolu par un administrateur et que l'intervention des forces de l'ordre est terminée. Rouge (REJETÉ / SOS), Ce statut a une double signification selon le contexte. Pour un incident classique, il signifie "Rejeté" (fausse alerte). Cependant, dans le cas d'une alerte SOS, le rouge clignotant signale une urgence vitale critique nécessitant une intervention immédiate.

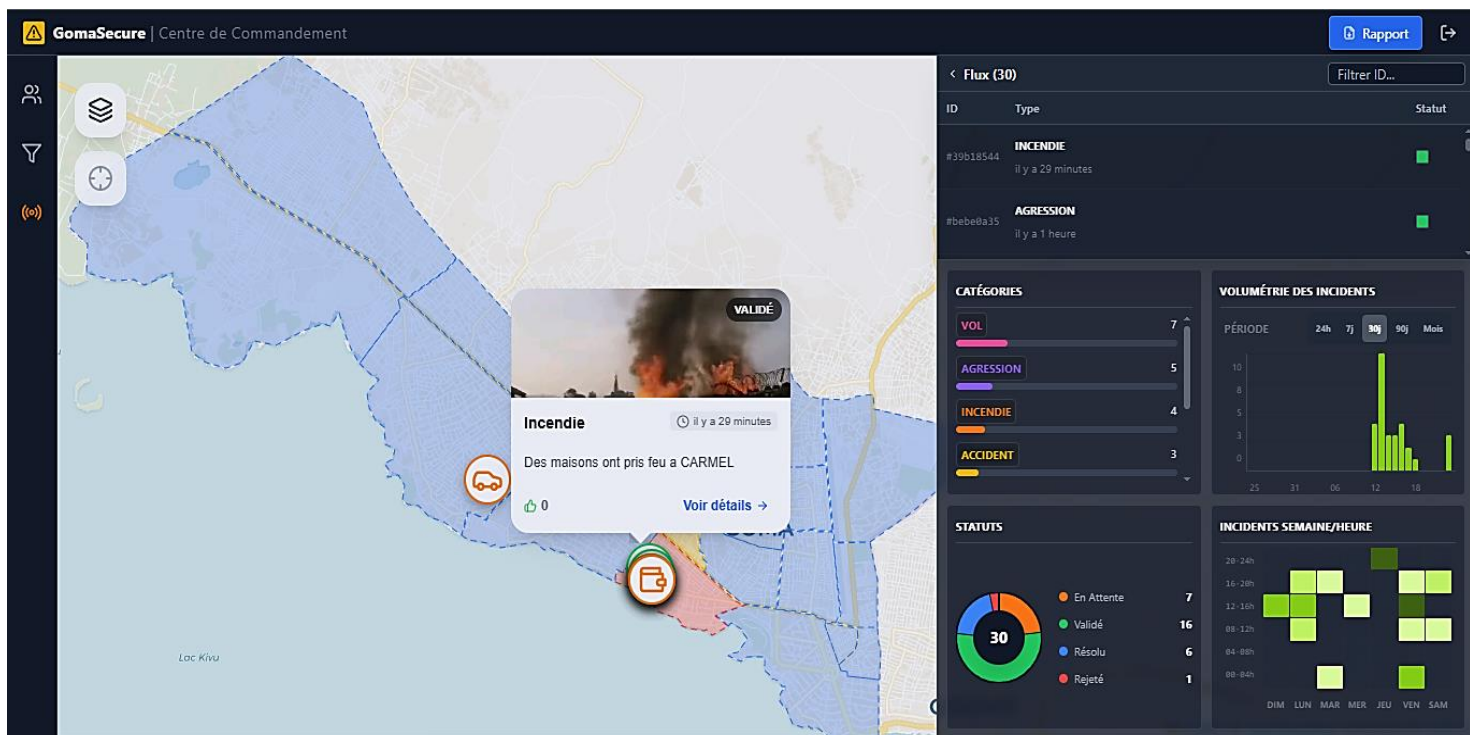


Figure 3-6: Interface de consultation des signalements pour administrateur

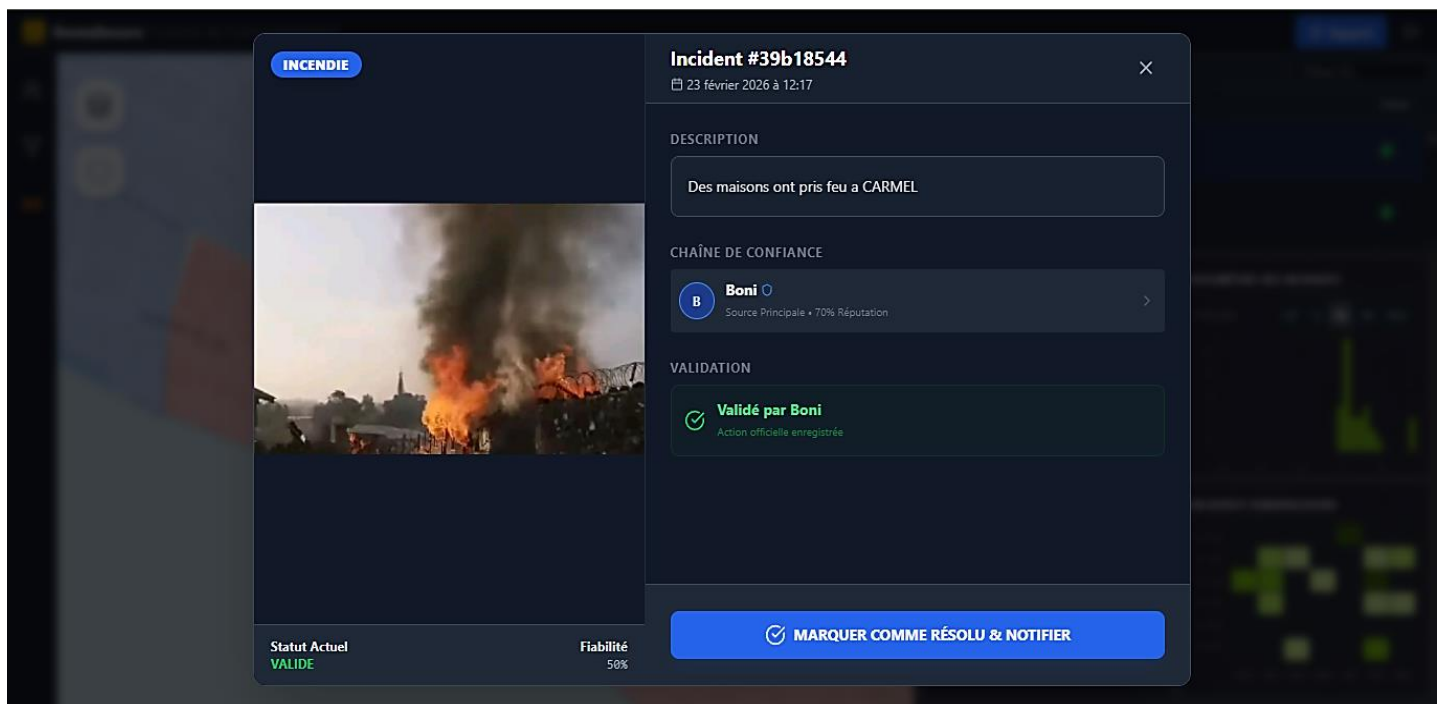


Figure 3-7: Interface de validation pour administrateur

Lorsqu'un administrateur clique sur le bouton “ Voir détails” (visible dans la bulle de la Figure 3-6) ou sélectionne un élément dans la liste (flux à droite), le système ouvre une fenêtre modale détaillée, c'est cette vue approfondie, illustrée par la Figure 3-7, qui permet le traitement du dossier. Elle affiche les éléments de preuve (audio, photo ou vidéo à gauche) pour confirmer visuellement la gravité de la situation, ainsi qu'une description textuelle précise.

Un élément clé de cette interface est la section “Chaîne de Confiance” (à droite). Elle identifie l'auteur du signalement (ici “Boni”) et affiche son score de réputation (70%), permettant à l'administrateur de juger rapidement de la crédibilité de la source avant d'agir, On remarque ici que l'incident a été signalé et validé par la même personne, cela s'explique par le fait que tout signalement émis par une sentinelle est considéré comme valide d'office

Enfin, le bas de la fenêtre propose les boutons d'action administrative permettant de modifier l'état du signalement. Si celui-ci est encore “En attente”, l'administrateur a la possibilité de le valider ou de le rejeter. Une fois le signalement validé, il peut alors changer le statut de l'incident en cliquant, sur “Marquer comme résolu & Notifier”. Cette action change instantanément l'état de l'incident en “Résolu” et déclenche l'envoi automatique d'une notification aux citoyens concernés pour les informer de la fin du danger.

3.4.6 Interface de visualisation des statistiques

L'interface présentée en Figure 3-8 offre une vue synoptique de la situation sécuritaire à Goma, plus précisément dans le quartier Katindo, celui-ci étant sélectionné. Elle transforme les données brutes en informations exploitables grâce à un tableau de bord centralisé. La section analytique permet une lecture immédiate de la typologie des menaces au moyen d'un histogramme classant les catégories par code couleur : rose pour les vols, violet pour les agressions, orange pour les incendies, jaune pour les accidents, bleu pour les enlèvements, rouge pour les alertes SOS et vert pour les autres incidents. Elle permet également de suivre l'efficacité de la réponse à travers un diagramme des statuts (Validé, En attente, Résolu, Rejeté). Enfin, la dimension temporelle est analysée à l'aide d'un graphique de volumétrie (par exemple sur les trente derniers jours) et d'une matrice de densité (heatmap), permettant d'identifier avec précision les pics de criminalité ainsi que les périodes critiques selon les tranches horaires.

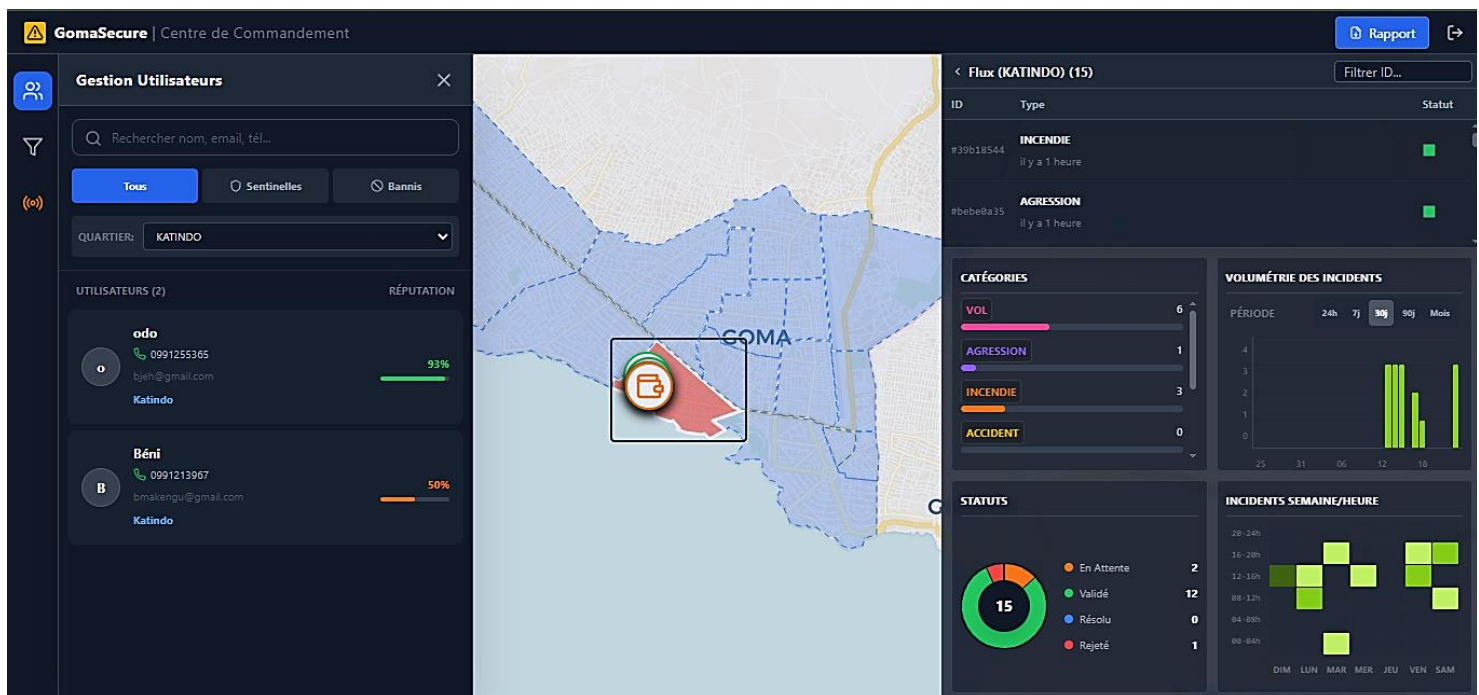


Figure 3-8: Interface de visualisation des statistiques

3.4.7 Interface de génération des rapports

L'interface “Centre de Rapports” sur la *Figure 3-9*, facilite la communication institutionnelle en permettant l'exportation des données de sécurité sous forme de documents officiels. L'utilisateur sélectionne d'abord une période d'analyse précise (par exemple, du 24 janvier au 23 février 2026) et visualise immédiatement un aperçu des statistiques clés, telles que le total des incidents (30), le nombre d'incidents graves (20) ou le taux de résolution (20%), etc. Une fois ces indicateurs validés, un simple clic sur le bouton “Télécharger PDF” génère le rapport final, garantissant ainsi une traçabilité administrative fiable et rapide. On y accède en cliquant sur le bouton “Rapport” situé en haut à droite du tableau de bord.

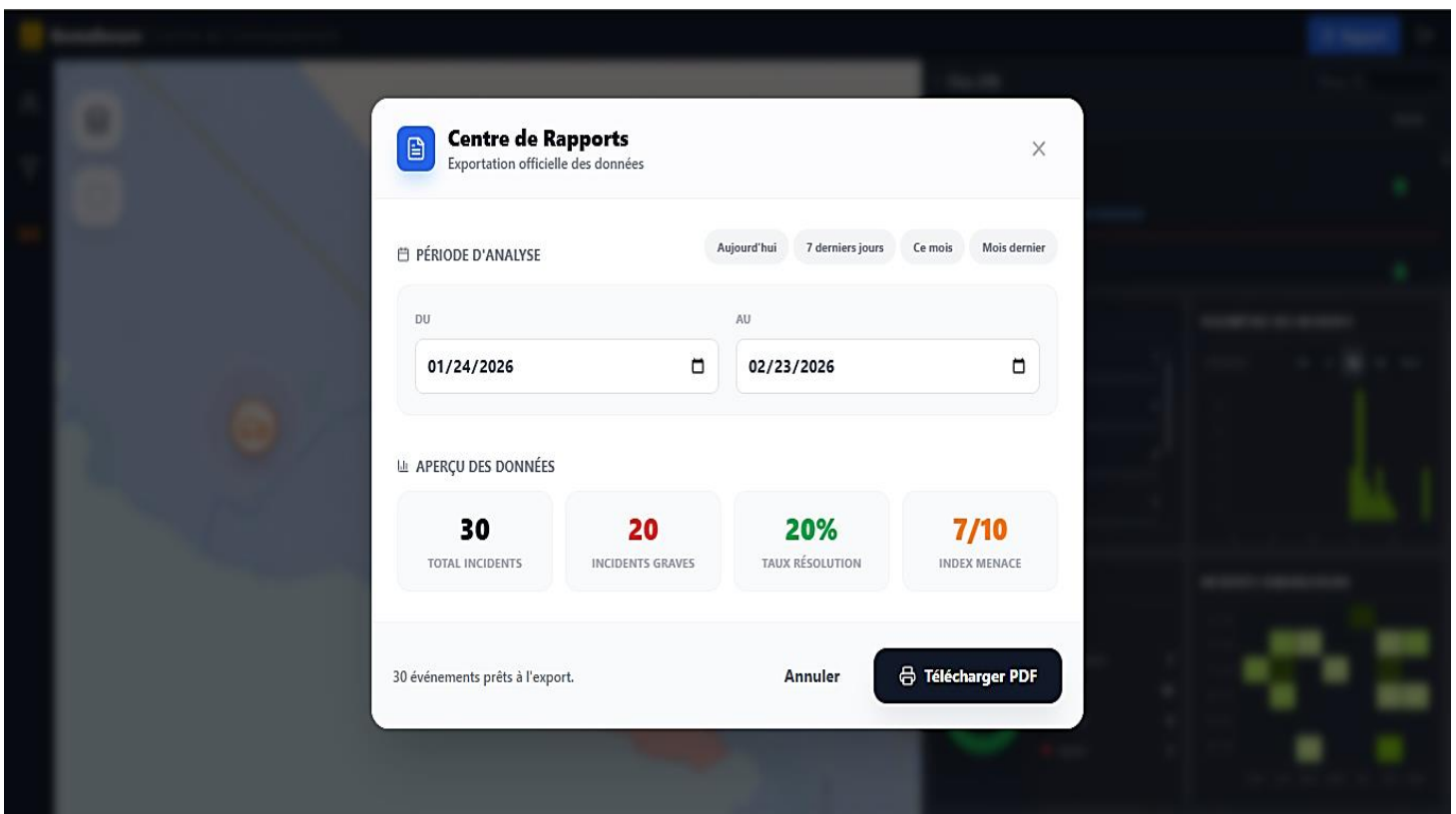


Figure 3-9: Interface de génération des rapports

3.4.8 Interface de gestion d'utilisation

L'interface de gestion des utilisateurs permet à l'administrateur de moduler les droits d'accès et les rôles au sein de la plateforme. La modification d'un profil s'effectue en sélectionnant un

utilisateur dans la liste, voir la Figure 3-10, offrant ainsi la possibilité de bannir les comptes malveillants pour préserver l'intégrité du système.

Un élément central de cette gestion est le score de fiabilité, représenté par une barre de progression; ce score augmente automatiquement chaque fois que les signalements d'un citoyen sont confirmés par la communauté ou validés par les entités dédiées. Cependant, l'attribution du rôle de Sentinelle ne dépend pas uniquement de l'atteinte d'un seuil de confiance élevé; l'administrateur doit également prendre en compte l'ancienneté de l'utilisateur sur la plateforme pour garantir une expérience suffisante.

Lorsqu'un citoyen remplit ces deux conditions, l'administrateur accède à la page de promotion pour lui attribuer ses nouveaux privilèges. Cette interface affiche ces informations clés et, via un bouton dédié, permet de lui attribuer le statut de Sentinelle lui octroyant ainsi le droit de valider ou rejeter les alertes (voir la Figure 3-11). Une fois l'action confirmée, le système enregistre les modifications dans la base de données et informe l'utilisateur de sa promotion par une notification automatique. Si l'utilisateur accepte l'invitation, son interface change immédiatement : son profil est désormais marqué par un petit badge bleu en forme de bouclier,

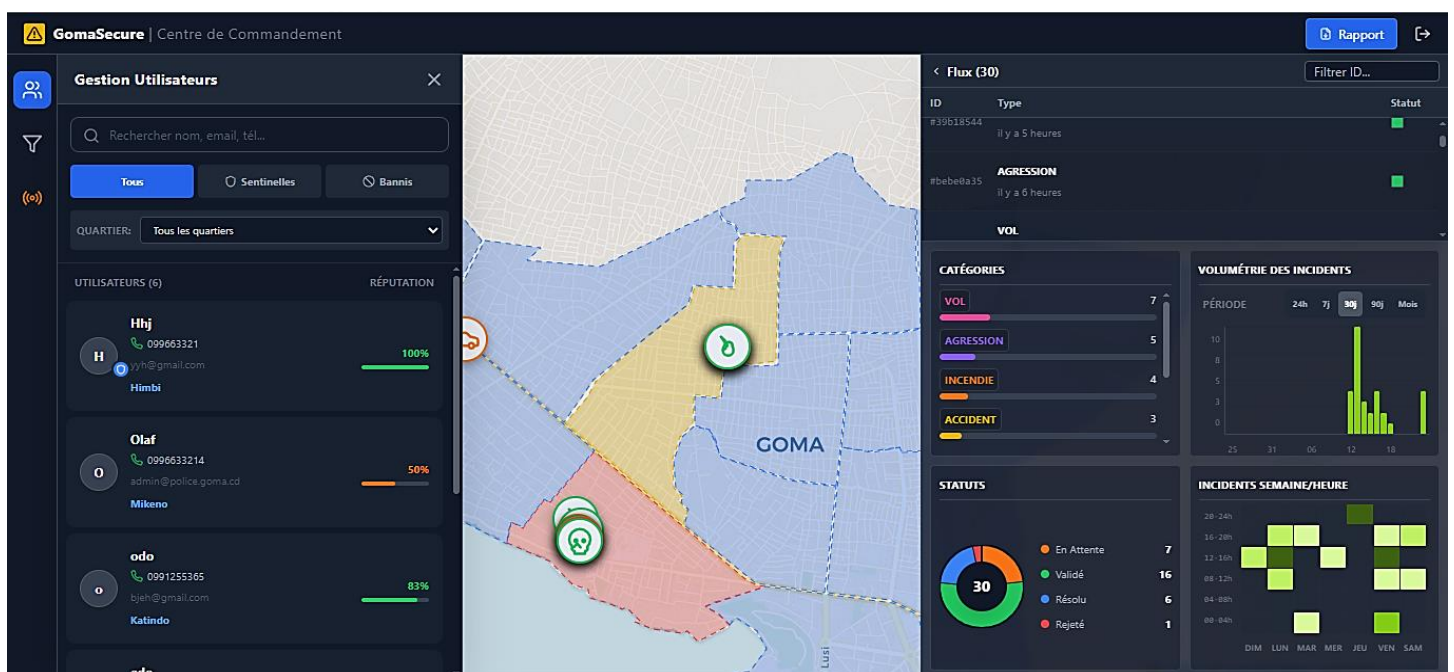


Figure 3-10: Interface de gestions des utilisateurs

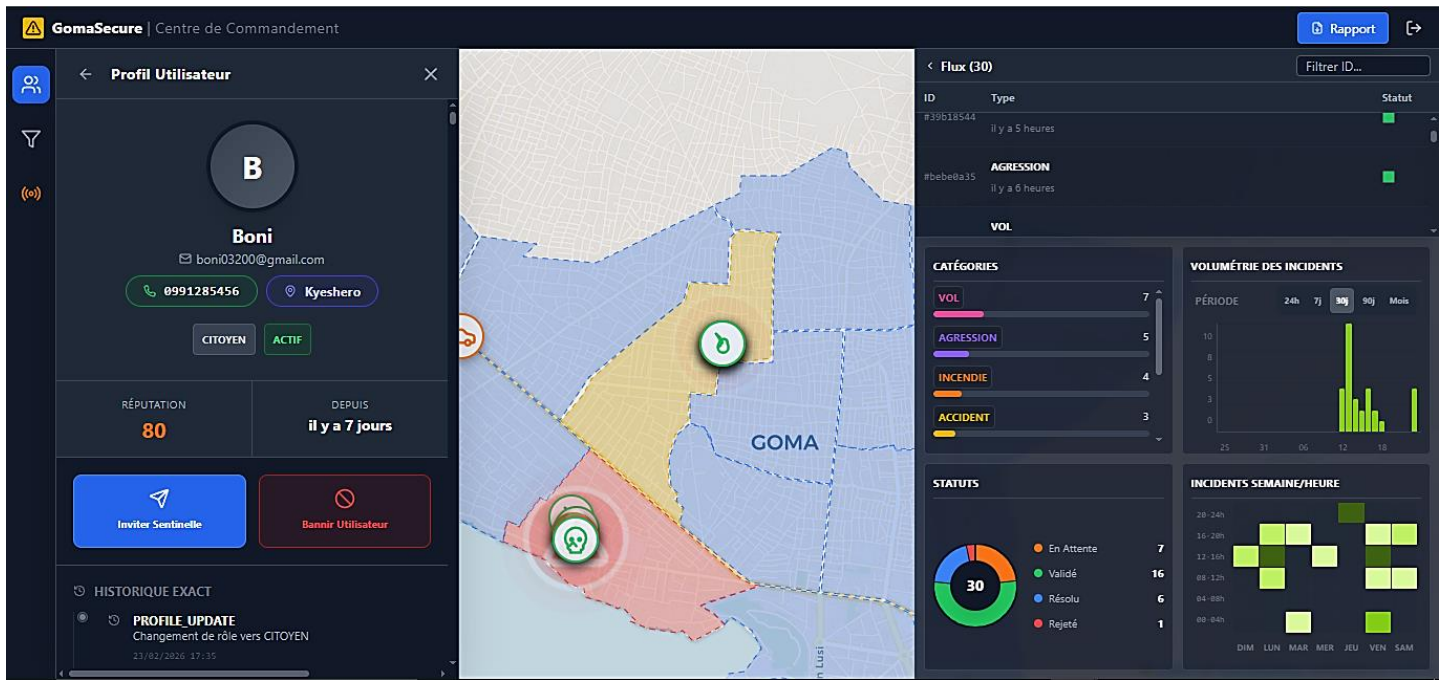


Figure 3-11: Interface profil d'utilisateur et attribution de rôle du sentinelle

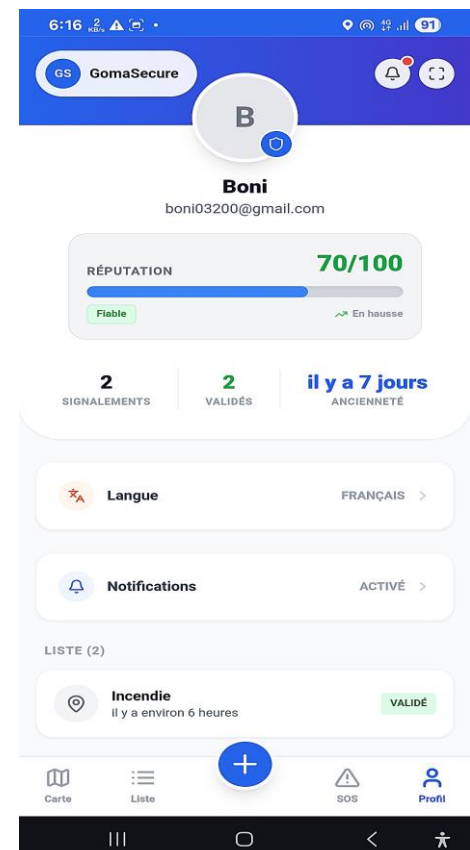
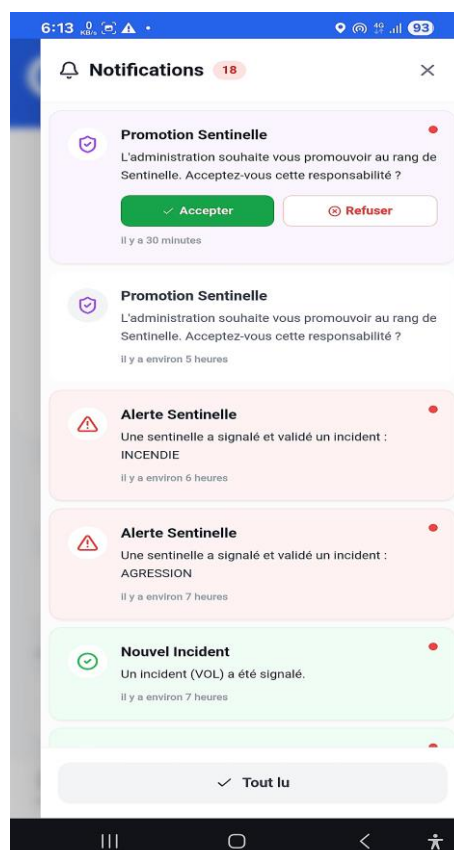
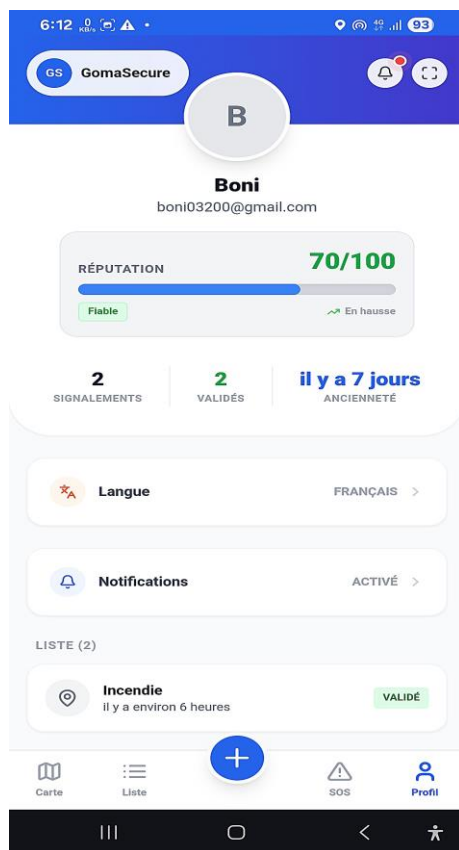


Figure 3-12: Interface de notification de promotion d'un citoyen au rang de sentinelle

3.4.9 Interface du déclenchement d'Alerte Silencieuse

Pour répondre aux situations de danger imminent où la discrétion est vitale (ex: kidnapping, braquage en cours, ect.), l'application intègre un mode SOS. La Figure 3-13 illustre cette interface minimaliste et sombre, conçue pour ne pas attirer l'attention. Lorsqu'elle est activée, l'application bascule en mode furtif : elle enregistre l'audio ambiant en continu et transmet la position en temps réel aux administrateurs, tout en simulant un écran éteint. Ce fonctionnement spécifique démontre la capacité du système à gérer des contextes critiques dépassant le simple signalement déclaratif.

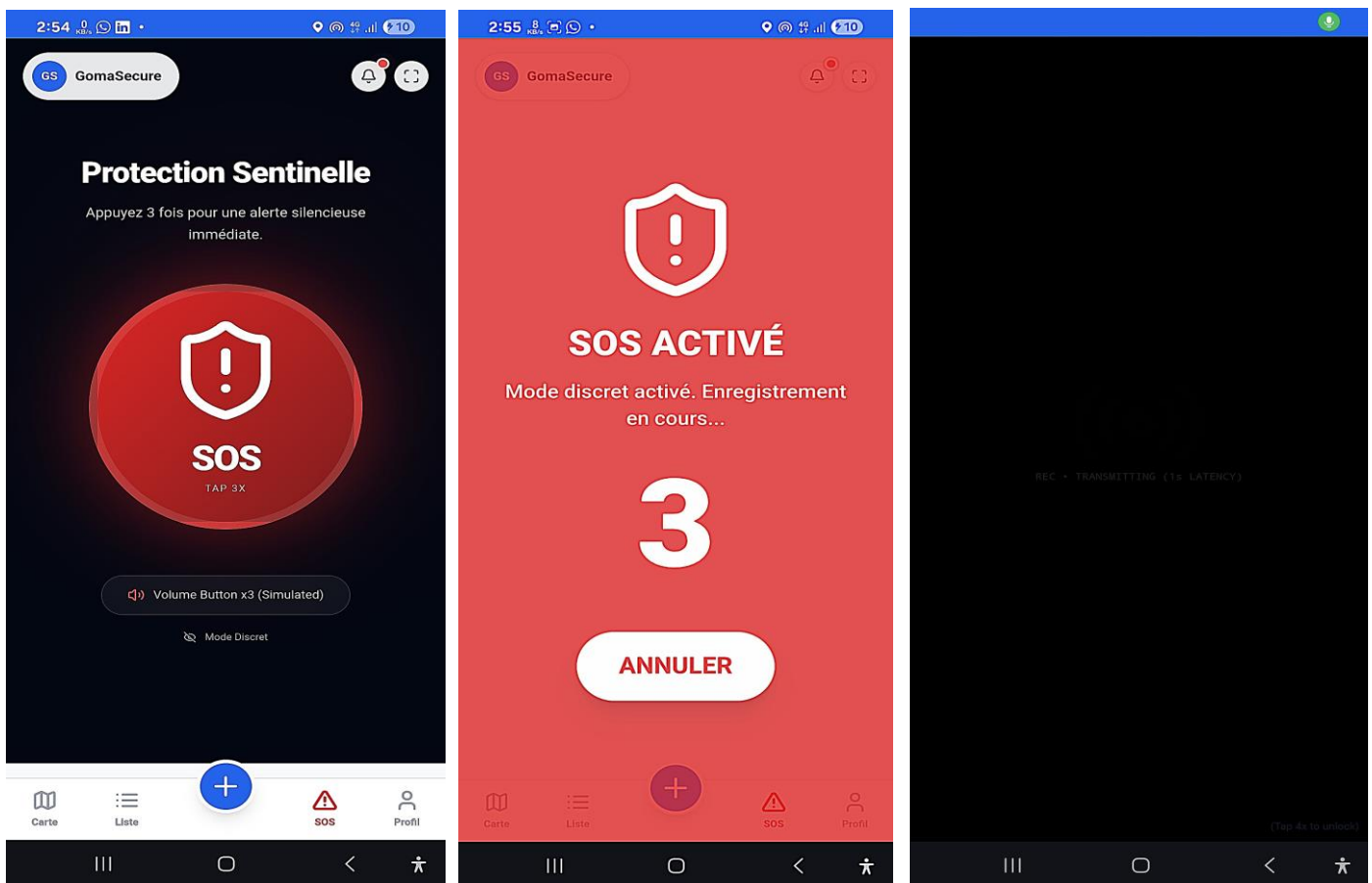


Figure 3-13: Interface du déclenchement d'Alerte Silencieuse

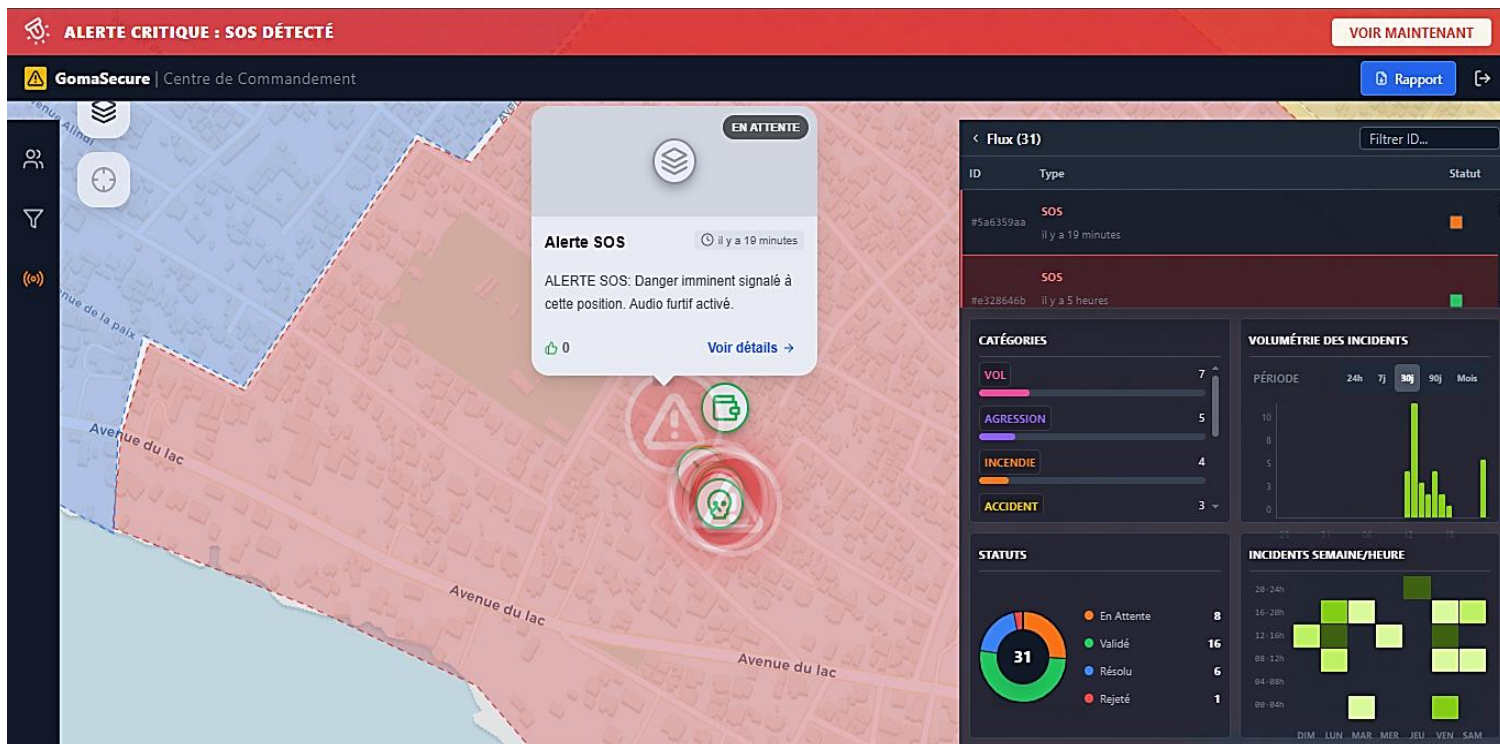


Figure 3-14: Interface de visualisation d'alerte SOS par l'administrateur

La Figure 3-14 illustre l'interface du centre de commandement destinée aux administrateurs lors de la réception d'une alerte critique (SOS). Cette vue spécifique se distingue par l'utilisation d'un indicateur de statut de couleur rouge, qui signale une urgence vitale ou un danger de mort imminent nécessitant une intervention immédiate des secours. Générée par le déclenchement du “ Mode Discret ”, cette interface fournit aux autorités des informations cruciales en temps réel, notamment la géolocalisation exacte de la victime et l'activation d'un “audio furtif”, permettant d'écouter la situation sans éveiller les soupçons de l'agresseur.

3.5 Tests et validation du système

Une stratégie de tests a accompagné le développement :

- **Tests unitaires et d'intégration** : Vérification des composants critiques (authentification, API de signalement).
- **Tests fonctionnels manuels** : Simulation de scénarios complets (création d'incident, upload de média, vote) pour valider le flux de données [39].

- **Tests d'utilisabilité** : Réalisation de tests utilisateurs ciblés pour optimiser l'expérience de navigation sur mobile et valider la fluidité de l'affichage des données géospatiales en temps réel.

Ces phases de test ont permis de corriger les anomalies et d'assurer la stabilité de l'application, même dans des conditions de connectivité dégradée.

3.6 Conclusion partielle

Ce chapitre a décrit la concrétisation technique de la plateforme GomaSecure. L'architecture choisie, combinant la flexibilité de React/Leaflet à la robustesse de Supabase/PostGIS, a permis de bâtir une solution performante pour le signalement géolocalisé et la validation communautaire. La mise en place de processus de déploiement continu et de tests systématiques garantit la fiabilité du système. Notre application est désormais opérationnelle et prête à répondre aux objectifs de surveillance participative définis dans notre projet.

Conclusion générale

Au terme de ce travail de recherche consacré à la “ Conception et implémentation d’une application web participative de signalement des incidents sécuritaires à Goma basée sur la géolocalisation”, nous sommes parvenus à matérialiser une réponse technologique concrète face à la problématique de l’insécurité urbaine. Partant du constat des limites des dispositifs d’alerte traditionnels (sifflets, clameurs publiques), notre démarche a consisté à mobiliser les concepts de Smart City et de Crowdsourcing pour offrir aux citoyens de Goma un outil de vigilance moderne.

Contributions

La principale contribution de ce mémoire est d’ordre à la fois sociotechnique et opérationnel. En réponse à notre question de recherche principale, nous avons démontré qu’il est possible d’améliorer la rapidité et la fiabilité des alertes sécuritaires grâce à une architecture web participative.

Nos résultats valident les hypothèses émises au début de cette étude qui sont :

- ❖ **Centralisation et Traçabilité** : Contrairement aux alertes sonores éphémères, l’application GomaSecure permet de documenter, d’archiver et de cartographier les incidents. La mise en place de la base de données spatiale (PostGIS) offre désormais une vue synoptique de la criminalité, répondant ainsi au besoin de statistiques fiables pour les autorités.
- ❖ **Géolocalisation et Preuves** : L’intégration de la géolocalisation automatique et de la capture multimédia (photos, audios, vidéos) dans le module de signalement comble le manque de précision des appels téléphoniques classiques. Cela permet aux forces de l’ordre de situer exactement le lieu d’intervention.
- ❖ **Fiabilisation par la Communauté** : La réponse à la problématique des “fausses alertes” a été apportée par l’implémentation du mécanisme de Validation

Communautaire. La distinction des rôles entre “Citoyens” et “Sentinelles”, couplée à un algorithme de réputation, crée un filtre social efficace qui garantit la crédibilité des informations avant leur escalade vers les autorités.

Critique du travail

Bien que les objectifs fixés aient été atteints, ce travail présente certaines limites inhérentes aux contraintes temporelles, techniques et contextuelles.

- ❖ **Dépendance à la connectivité** : L'architecture actuelle, bien que progressive (PWA), reste dépendante d'une connexion Internet mobile (3G/4G). Dans le contexte de Goma, où la couverture réseau peut être instable et le coût des données élevées, cela constitue un frein à l'accessibilité pour les couches les plus vulnérables de la population.
- ❖ **Précision GPS en zone dense** : Les tests ont révélé que la géolocalisation par navigateur peut manquer de précision dans les zones à forte densité de bâti ou en intérieur, ce qui pourrait retarder certaines interventions critiques.
- ❖ **Adoption par les autorités** : Le système, pour être pleinement efficace, requiert une intégration réelle dans les processus opérationnels de la Police Nationale Congolaise (PNC). À ce stade, le tableau de bord administrateur est fonctionnel techniquement, mais son adoption organisationnelle reste un défi politique et structurel.

Travaux futurs de recherche/Perspectives

Pour pérenniser cette solution et maximiser son impact social, plusieurs pistes d'évolution sont envisageables :

- ❖ **Intégration USSD/SMS** : Afin de franchir la fracture numérique, une extension du système permettant de signaler des incidents via des codes USSD ou SMS (pour les téléphones basiques) serait une évolution majeure pour couvrir 99% de la population.
- ❖ **Intelligence Artificielle Prédicative** : À mesure que la base de données s'enrichira, l'intégration de modules d'IA permettrait d'analyser les tendances criminelles et de

prédire les zones à risque (Predictive Policing), permettant aux autorités d'agir de manière préventive plutôt que réactive.

- ❖ **Développement Mobile Natif** : Le portage de l'application vers des technologies natives (React Native ou Flutter) permettrait une meilleure gestion des fonctionnalités hors-ligne (Offline-first) et un accès plus performant aux capteurs du téléphone (les boutons physiques, accéléromètre et gyroscope pour détection de chute, etc.).
- ❖ **Partenariat Public-Privé** : Enfin, l'officialisation d'un partenariat avec les autorités locales et les réseaux de télécommunication serait indispensable pour garantir la gratuité du trafic de données (Zero-rating) lié à l'application, la rendant ainsi véritablement accessible à tous.

En définitive, GomaSecure ne se veut pas une fin en soi, mais la première pierre d'un écosystème numérique de sécurité publique, où chaque citoyen devient un maillon actif de la protection collective.

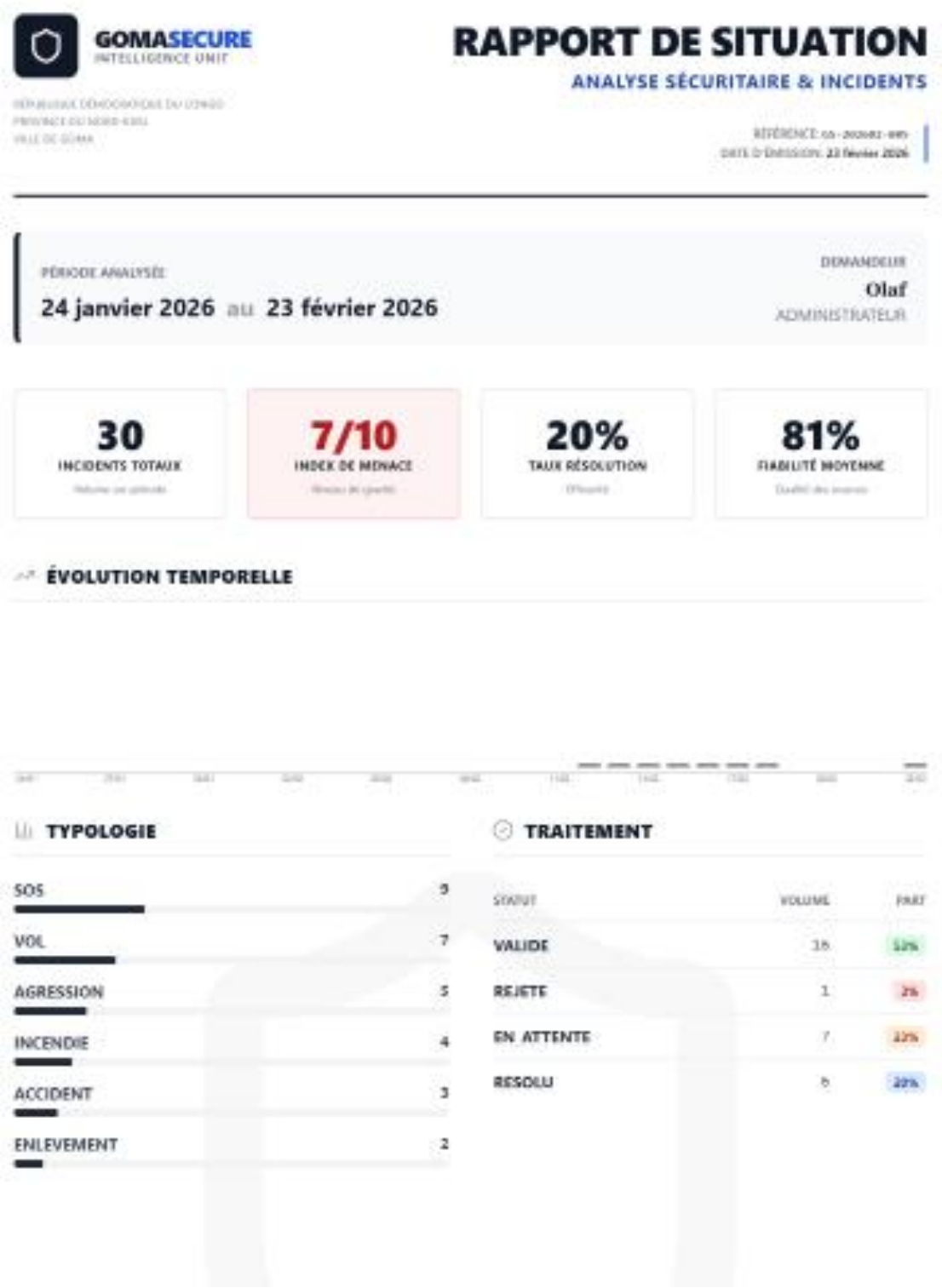
Bibliographie

- [1] DigitalCitizenship, “Building a strong foundation for the digital era.,” 2023. [Online].
- [2] Abid, S. K., Roosli, R., Nazir, U., Abid, N., & Jan, N. , “AI-enhanced crowdsourcing for disaster management: strengthening community resilience through social media. *International Journal of Emergency Medicine*,” vol. 18, pp. 11-12, 2025.
- [3] GeoPoll, “Mobile penetration and internet usage in Congo,” 15 07 2024. [Online]. Available: <https://www.geopoll.com/blog/mobile-penetration-and-internet-usage-in-congo/>. [Accessed 23 12 2025].
- [4] C. PANDI, “ Nuit de terreur à Goma : pillages, coups de feu et lynchage sur fond de psychose,” *Journal de Kinshasa*, 2025.
- [5] M. N, “Insécurité à Goma : des sifflets, sirènes et vuvuzela remis aux cadres de base à Himbi.,” *APIC-TV*, 09 avril 2022.
- [6] Promoinfos.cd, “Insécurité à Goma : une nouvelle mesure s’installe pour traquer les malfrats en commune de Goma.,” 9 décembre 2021.
- [7] Radio Okapi, “Incidents sécuritaires signalés à Goma et Nyiragongo. Radio Okapi.,” 22 avril 2025.
- [8] RVI Usalama Project, “Insecurity in Goma,” the Rift Valley Institute, London , 2019.
- [9] MDN, “What is a progressive web app?,” *Progressive web apps*.
- [10] Web.dev, “Progressive Web Apps,” *Web.dev*.
- [11] Chaves, R., Schneider, D., Correia, A., Motta, C. L. R., & Borges, M. R. S., “Crowdsourcing as a tool for urban emergency management: lessons from the literature and typology,” pp. 1-2, 2019.
- [12] M. L. Tchicaya, “Conception et développement d'une application web pour la gestion des urgences : cas de l'application SOS communautaire,” *Mémoire Online, Pointe-Noire*, 2025.

- [13] A. Silva, "Analysis of the reliability value provided by Waze, Master's thesis, Dept. of Computer and Systems Sciences," Sweden, 2018.
- [14] Hunt, A., & Specht, D. , "Crowdsourced mapping in crisis zones: collaboration, organisation and impact.," *Journal of International Humanitarian Action*, vol. 4, 2019.
- [15] Mustafa, R., Han, J., Sarkar, N. I., & Petrova, K., "Secure Cross-Layer Mobile Sensing Framework for Real-Time Disaster Reporting and Visualisation Using a Mobile Application.," *Sensors*, vol. 25, no. 21, p. 6766, 2025.
- [16] Bishr, M., & Mantelas, L., "A trust and reputation model for filtering and classification of knowledge from crowdsourcing.," *GeoJournal*, vol. 72, pp. 229-237, 2008.
- [17] C. Silverman, "Verification Handbook: An ultimate guideline on digital age sourcing for emergency coverage," European Journalism Centre, maastecht, 2014.
- [18] Ushahidi Community Resource, "Ushahidi verification guide," 2013.
- [19] jesse, "Citizen App and the controversy of crowdsourced 'Citizen Policing'," HBS Digital Initiative., 2018.
- [20] CORDIS EU, "CITY.RISKS: Participatory Urban Security System," 2020.
- [21] Perez, S., " App downloads declined again in 2025, but consumer spending soared to nearly \$156B," *TechCrunch*, 14 January 2026.
- [22] Ajene, E., "How Africa's super app landscape is evolving," *Afridigest*, 6 September 2025.
- [23] J. Galano, "Comment les Progressive Web Apps bouleversent l'usage mobile ?," 4 May 2023.
- [24] Wikipedia, "Digital citizen. (n.d.).," 2023. [Online]. Available: https://en.wikipedia.org/wiki/Digital_citizen.
- [25] B. Estes, "Geolocation – The Risk and Benefits of a Trending Technology," vol. 5, 2016.
- [26] Wikimedia, "Système d'information géographique," [Online]. Available: https://fr.wikipedia.org/wiki/Syst%C3%A8me_d%27information_g%C3%A9ographi

- maintainability-in-react-projects#:~:text=TypeScript%20for%20Enhanced%20Type%20Safety,and%20Maintainability%20in%20React%20Projects. [Accessed 04 Janvier 2026].
- [39] Supabase Docs, “REST API | Supabase Docs,” [Online]. Available: <https://supabase.com/docs/guides/api>. [Accessed 4 February 2026].
- [40] “AuTh | Supabase Docs,” Supabase Docs, [Online]. Available: <https://supabase.com/docs/guides/auth>. [Accessed 4 February 2026].
- [41] “Leaflet — an open-source JavaScript library for interactive maps. (n.d.),” [Online]. Available: <https://leafletjs.com/#:~:text=Leaflet%20is%20the%20leading%20open,features%20most%20developers%20ever%20need>.
- [42] “PostGIS: Geo queries | Supabase Docs,” Supabase Docs, 4 February 2026. [Online]. Available: <https://supabase.com/docs/guides/database/extensions/postgis>.
- [43] Vercel. (n.d.), “Vercel documentation,” [Online]. Available: <https://vercel.com/docs>.
- [44] Supabase Docs, “Client Libraries | Supabase Docs,” [Online]. Available: <https://supabase.com/docs/guides/api/rest/client-libs>. [Accessed 04 February 2026].

Annexe A



CODE SOURCE

<https://github.com/Black-Shinobi/Securegoma>