République Algérienne Démocratique et Populaire
Université Abou Bekr Belkaid -Tlemcen

Faculté des Sciences

Département d'Informatique

Mémoire de Fin d'Études

Pour l'obtention du diplôme de Master en Informatique
Option : **Réseaux et Systèmes Distribués (R.S.D)**

Thème

Conception et réalisation d'une plateforme sécurisée de gestion des données médicales des patients

---

Réalisé par :

- **HASNAOUI Nour El Houda**
- **MEGREZ Rayhane**

Soutenu le **28 Juin 2025** Devant le jury composé de :

Mme BENMAHDI Meryem Bochra	Présidente
Mr LEHSAINI Mohamed	Encadrant
Mr FEHAM Mohammed	Co-encadrant
Mr DEGDEG Hicham	Co-encadrant
Mr SEBBAH Abderrazak	Examinateur
Mr FEKAR Riyadh	Expert I2E

Année universitaire : 2024/2025

Remerciements

Avant tout, nos remerciements les plus profonds et les plus sincères vont à Allah, le Tout-Puissant, pour la force qu'Il nous a insufflée, la patience qu'Il nous a enseignée et la lumière qu'Il a placée sur notre chemin. Sans Sa volonté, aucun de ces pas n'aurait été possible.

Nos remerciements vont à notre encadrant Mr. LEHSAINI Mohamed et Co-encadrant Mr. DEGDEG Hicham pour leur accompagnement, leur soutien sans faille, leur disponibilité, ainsi que la qualité de leurs conseils et remarques, qui ont été d'une grande valeur pour mener à bien ce travail.

Nous remercions également les membres du jury pour le temps qu'ils nous ont consacré, la bienveillance de leur écoute et la pertinence de leurs observations, qui ont enrichi ce travail.

Enfin, un immense merci à nos amis et à tous ceux qui, de près ou de loin, ont contribué à la réussite de ce projet. Par un geste, un mot, une présence ou un simple regard d'encouragement, votre soutien a été précieux et réel. Ce mémoire est le fruit d'un effort collectif, mais aussi d'un chemin intérieur, tissé de volonté, de doutes, de résilience… et d'un engagement profond qui a animé tout le parcours.

Dédicaces

C'est avec une profonde gratitude et une sincérité totale que nous dédions

ce travail de fin d'études :

À nos parents, pour leurs sacrifices et leur amour sans limite.

Que Dieu leur accorde santé et longue vie.

À nos frères et sœurs, piliers silencieux de notre force, toujours présents à nos côtés.

À toute notre famille, pour leur soutien constant, même à distance.

Enfin, à ma binôme et moi-même, pour cette aventure partagée, la persévérance, la détermination et l'effort communs qui nous ont permis d'arriver jusqu'ici.

Nour El Houda HASNAOUI & Rayhane MEGREZ

Résumé

L'objectif de ce projet est de concevoir une plateforme sécurisée de gestion des dossiers médicaux, permettant une coopération sécurisée entre différents établissements de santé. Le système est conçu pour assurer la confidentialité, la traçabilité et la sécurité des données sensibles des patients en utilisant des techniques de chiffrement avancées, notamment MA-ABE (Multi-Authority Attribute-Based Encryption), qui permet un contrôle d'accès précis basé sur les attributs ainsi que la blockchain pour une sécurité renforcée. Le système adopte une approche distribuée en plusieurs couches : MongoDB Compass pour gérer les données des utilisateurs, la blockchain pour enregistrer de manière sécurisée les accès et les clés chiffrées à l'aide de MA-ABE et AES, un cloud multimédia pour héberger les dossiers médicaux, un serveur Node.js fait le lien entre les bases de données et l'interface utilisateur qui est développée avec Vue.js pour une interaction intuitive et réactive.

Keywords : Blockchain, MA-ABE, AES, Contrôle d'accès, HealthSafe

Abstract

The aim of this project is to design a secure platform for managing medical records, enabling secure cooperation between different healthcare establishments. The system is designed to ensure the confidentiality, traceability and security of sensitive patient data using advanced encryption techniques, including MA-ABE (Multi-Authority Attribute-Based Encryption), which enables granular access control based on attributes, and blockchain for enhanced security. The system adopts a distributed, multi-layered approach : MongoDB Compass to manage user data, the blockchain to securely record access and encrypted keys using MA-ABE and AES, a multimedia cloud to host medical records, a Node.js server provides the link between the databases and the user interface, which is developed using Vue.js for intuitive, responsive interaction.

Keywords : Blockchain, MA-ABE, AES, Access Control, HealthSafe

ملخص

الهدف من هذا المشروع هو إنشاء لوحة آمنة لإدارة الملفات الطبية، مما يسمح بالتعاون الآمن بين المؤسسات الصحية المختلفة. تم تصميم النظام لضمان السرية وإمكانية التتبع وأمن البيانات الحسية للمرضى باستخدام تقنيات التشفير المتقدمة، بما في ذلك MA-ABE (التشفير القائم على السمات المتعددة)، والذي يسمح بالتحكم في الوصول الحبيبي على أساس السمات و Blockchain لتعزيز الأمان. يعتمد النظام نهجًا للتوزيع والأسطح المتعددة: MongoDB Compass لتوزيع بيانات المستخدمين، و Blockchain للتسجيل الآمن تمامًا للوصول والكلمات المشفرة بمساعدة MA-ABE و AES، ووسائط متعددة جديدة لحفظ الملفات طبي، خادم Node.js يضمن الامتياز بين قواعد البيانات وواجهة المستخدم، التي تم تطويرها بمساعدة Vue.js من أجل تفاعل بديهي وسريع الاستجابة.

الكلمات المفتاحية: Blockchain, MA-ABE, AES, Access Control, HealthSafe

TABLE DES MATIÈRES

TABLE DES FIGURES

ACRONYMES

ABAC Attribute-Based Access Control. 12

ABE Attribute-based Encryption. 14

ACL Access Control List. 10

AES Advanced Encryption Standard. 23, 28

CEI Commission électrotechnique internationale. 25

CID Confidentialité, Intégrité et Disponibilité. 4

CNIL Commission Nationale de l'Informatique et des Libertés. 5

CSS Cascading Style Sheets. 26

DAC Discretionary Access Control. 10

ENISA European Union Agency for Network and Information. 5

HDS Hébergeurs de Données de Santé. 7

HIPAA Health Insurance Portability and Accountability Act. 5, 7

HTML HyperText Markup Language. 26

IAM Gestion des identités et des accès. 5, 8

IDS systèmes de détection d'intrusion. 5

JS JavaScript. 26

MA-ABE Multi-authority Attribute-based Encryption. ii, 14, 29

MAC Mandatory Access Control. 10

OMS Organisation mondiale de la Santé. 9

RBAC Role-Based Access Control. 12, 14

RGPD Règlement Général sur la Protection des Données. 7, 9

SGSI système de gestion de la sécurité de l'information. 6

INTRODUCTION GÉNÉRALE

Introduction générale

La sécurité des données médicales est devenue une priorité essentielle à l'ère du numérique. Avec la digitalisation rapide des systèmes de santé, les cliniques et les hôpitaux utilisent de plus en plus des plateformes numériques pour gérer les informations relatives aux patients. Ces données sont souvent très sensibles et il est donc essentiel de les protéger. Cependant, de nombreux établissements de santé ne disposent pas encore de solutions appropriées et sécurisées, exposant ainsi leurs systèmes à de nombreuses menaces telles que les cyberattaques et les fuites de données.

Dans ce contexte, une question centrale se pose : comment concevoir une plateforme numérique capable de garantir la sécurité, la confidentialité et la conformité des données médicales, tout en restant efficace et accessible aux utilisateurs du secteur de la santé ?

Pour répondre à cette problématique, notre projet propose de concevoir et de réaliser une plateforme sécurisée de gestion des données médicales appelée *HealthSafe*. L'idée est de combiner plusieurs technologies modernes, telles que le cloud, la blockchain et des mécanismes de sécurité avancés, pour offrir un système fiable, transparent et conforme aux normes de confidentialité.

Ce mémoire est organisé en quatre chapitres, chacun abordant une étape essentielle de la construction de la plateforme :

- Le premier chapitre est consacré aux principes de la sécurité des systèmes d'information. Il présente les concepts clés tels que la confidentialité, l'intégrité et la disponibilité, les mécanismes de sécurité (chiffrement, IAM, sauvegarde, etc.), les normes applicables aux données médicales, ainsi que les risques et menaces spécifiques au domaine de santé.

- Le deuxième chapitre décrit en détail l'architecture de la plateforme. Il décrit les différents composants (patient, personnel médical, cloud, blockchain, etc.), leurs rôles et la manière dont ils interagissent les uns avec les autres. Ce chapitre comprend également un schéma explicatif de l'architecture.

- Le troisième chapitre présente les technologies et les outils utilisés pour développer la plateforme. Il couvre les front et back ends, les bases de données, la sécurité et surtout

l'utilisation de la blockchain dans le domaine médical, avec ses caractéristiques, son fonctionnement et ses applications pratiques.

- Le quatrième chapitre est consacré à la mise en œuvre pratique de la plateforme. Il montre les principales fonctionnalités développées à travers des captures d'écran, expliquant le fonctionnement du système du point de vue de l'utilisateur.

A travers ce travail, notre objectif est de démontrer qu'il est possible de construire une plateforme médicale sécurisée, permettant une collaboration efficace entre plusieurs établissements de santé, en utilisant des technologies modernes et appropriées. Cette solution pourrait aider les établissements de santé à mieux protéger les données de leurs patients, tout en améliorant la qualité de leurs services.

CHAPITRE 1

PRINCIPES DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATIONS DANS LE DOMAINE MÉDICAL

1.1 Introduction

Dans un contexte où les établissements de santé s'appuient de plus en plus sur des systèmes informatiques pour gérer les dossiers médicaux, la question de la sécurité des données devient cruciale. Les informations médicales, en raison de leur nature sensible, représentent une cible privilégiée pour les cyberattaques. Ainsi, la protection des systèmes d'information dans le secteur médical ne relève plus d'un simple choix technique, mais constitue une exigence stratégique, éthique et réglementaire. Á cet effet, garantir la confidentialité, l'intégrité et la disponibilité des données médicales dans un environnement coopératif est désormais indispensable pour assurer un service médical fiable et conforme aux normes internationales.

Dans ce chapitre, nous présentons les concepts fondamentaux de la sécurité informatique en particulier pour la sécurisation des données médicales.

1.2 Concepts fondamentaux de la sécurité informatique

Dans cette section, nous présentons quelques notions sur la sécurité informatique, les mécanismes de sécurité, et les normes et réglementations pour la sécurité des données médicales.

1.2.1 Définition de la sécurité informatique

La sécurité des systèmes d'information regroupe l'ensemble des mesures techniques, organisationnelles et juridiques visant à protéger les ressources numériques ; données, logiciels, réseaux, et équipements contre toute menace susceptible de compromettre leur fonctionnement ou leur

intégrité. Elle repose sur trois principes fondamentaux, souvent désignés par le modèle "Confidentialité, Intégrité et Disponibilité (CID)" :

- **Confidentialité** : La confidentialité vise à empêcher tout accès non autorisé à l'information. Dans le cadre médical, cela signifie que seules les personnes habilitées (comme le personnel soignant) peuvent consulter les dossiers médicaux des patients. Une violation de la confidentialité peut entraîner une perte de confiance, des sanctions légales, voire des conséquences médicales graves si les informations sont utilisées de manière inappropriée.

  La confidentialité repose sur des mécanismes comme le chiffrement, l'authentification des utilisateurs et la gestion fine des droits d'accès. Toute fuite de données peut compromettre le secret médical et nuire gravement à la réputation de l'établissement.

- **Intégrité** : Ce principe garantit que les données n'ont pas été modifiées, volontairement ou accidentellement, sans autorisation. Dans un dossier médical, une simple erreur dans le dosage d'un médicament ou dans le diagnostic peut avoir des répercussions directes sur la santé du patient.

  L'intégrité permet de préserver l'exactitude et la fiabilité de l'information. Elle est assurée par des mécanismes comme les signatures numériques, les contrôles de versions et les journaux de modifications. La moindre altération peut fausser les décisions médicales, mettre en danger les patients et engager la responsabilité des professionnels de santé.

- **Disponibilité** : La disponibilité assure que les données et les services informatiques sont accessibles aux utilisateurs autorisés au moment opportun. En médecine d'urgence, une indisponibilité du système peut retarder un traitement critique, mettant la vie des patients en danger. Il est donc essentiel de garantir une haute disponibilité des systèmes de santé, souvent 24h/24. Cela passe par des infrastructures redondantes, des systèmes de sauvegarde automatisés et des plans de reprise après sinistre. Toute interruption, même brève, peut paralyser une chaîne de soins et compromettre la prise en charge rapide des patients.

Ces principes prennent une importance capitale vu que les données relatives à la santé sont extrêmement sensibles et que leur compromission peut avoir de graves conséquences, non seulement pour la vie privée des patients, mais aussi pour les soins médicaux qui leur sont prodigués.

1.2.2 Mécanismes de sécurité

La sécurité des systèmes d'information ne repose pas sur une barrière unique, mais plutôt sur un ensemble de mécanismes complémentaires, un peu comme les différentes couches d'une armure. Dans le domaine médical, où la moindre faille peut compromettre des vies humaines ou violer la vie privée des patients, ces mécanismes prennent une importance particulière [1].

1.2.2.1 Chiffrement

Le chiffrement représente l'une des premières lignes de défense en cybersécurité. Il consiste à transformer les données en un format illisible, appelé texte chiffré, grâce à des algorithmes

cryptographiques. Seules les personnes disposant de la clé de déchiffrement peuvent accéder aux données originales [2].

Dans le domaine médical, cela est particulièrement crucial, car les informations personnelles de santé doivent être protégées à tout prix pour garantir la confidentialité des patients. Même en cas de vol ou de piratage du système, les informations restent inaccessibles aux personnes non autorisées [3]. Par exemple, un dossier médical numérique contenant des données sensibles peut être chiffré de manière à empêcher toute lecture par un tiers non autorisé, même si celui-ci parvient à l'obtenir [4].

1.2.2.2 Gestion des identités et des accès (IAM)

La Gestion des identités et des accès (IAM) est une tâche fondamentale de la sécurité des systèmes d'information. Elle vise à garantir que chaque utilisateur (médecin, infirmière ou administrateur) n'a accès qu'aux données nécessaires à l'exercice de ses fonctions. Il s'agit d'attribuer à chaque professionnel une identité numérique, qui définit précisément ses droits d'accès. Par exemple, un médecin n'aura accès qu'aux dossiers médicaux de ses propres patients, tandis qu'un autre praticien ne pourra pas consulter ces mêmes dossiers, sauf autorisation explicite.

Cette segmentation limite fortement les risques de consultation abusive ou accidentelle de données sensibles comme s'est présenté dans la Commission Nationale de l'Informatique et des Libertés (CNIL) [5]. De ce fait, l'instauration des contrôles d'accès précis, l'IAM permet également de tracer toutes les actions effectuées sur les données, renforçant ainsi la transparence et la responsabilité. Dans un secteur aussi sensible que celui de la santé, cette exigence devient essentielle pour préserver la confidentialité des patients et se conformer aux obligations légales, telles que celles définies par la "Health Insurance Portability and Accountability Act (HIPAA)" Security Rule, qui encadre strictement l'accès aux données de santé protégées [6].

1.2.2.3 Systèmes de détection d'intrusion

Les systèmes de détection d'intrusion (IDS) sont essentiels dans la cybersécurité des établissements de santé. Ils analysent en temps réel le trafic réseau et les activités des systèmes pour identifier toute tentative d'accès non autorisé ou comportement suspect. Une connexion inhabituelle à des heures tardives ou un transfert massif de données, par exemple, peuvent déclencher une alerte immédiate.

Selon l'"European Union Agency for Network and Information (ENISA)" [7], l'intégration des IDS est recommandée pour prévenir les comportements malveillants dans les infrastructures critiques, y compris les systèmes hospitaliers. Ces outils sont en parfaite adéquation avec la norme ISO/IEC 27001 [1] relative à la surveillance continue des systèmes d'information pour assurer la sécurité des données sensibles.

1.2.2.4 Sauvegarde des données

La sauvegarde régulière des données est essentielle pour assurer la continuité des soins médicaux. En cas de cyberattaque, de panne matérielle ou d'erreur humaine, la disponibilité de copies de sauvegarde permet de restaurer et de récupérer rapidement des informations cruciales et d'éviter toute interruption des soins aux patients. L'ENISA [7] recommande la mise en œuvre de stratégies de sauvegarde robustes pour réduire le risque de perte de données et renforcer la sécurité des systèmes de santé face aux menaces.

Pour sa part, la norme ISO/IEC 27001 [1] souligne l'importance de protéger les données contre la perte ou la destruction en définissant des politiques appropriées de gestion des sauvegardes.

Ces mécanismes, lorsqu'ils sont combinés, créent un environnement sécurisé, résilient et conforme aux exigences réglementaires. Ils ne sont pas seulement des outils techniques, mais des garants de la confiance entre le patient et l'établissement de santé (CNIL, ISO27001) [1, 5].

1.2.3 Normes et réglementations pour la sécurité des données médicales

Pour protéger les données dans le secteur de la santé, un certain nombre de normes et de lois ont été mises en place, tant au niveau national qu'international.

1.2.3.1 Importance des normes dans la sécurité des données médicales

Les normes et les réglementations instaurées pour les données médicales ont été mises en place pour permettre les objectifs suivants :

- Limiter l'accès aux données médicales aux seules personnes habilitées et autorisées.
- Prévenir le vol, la perte ou l'altération des données sensibles.
- Garantir la conformité légale des hôpitaux, cliniques et prestataires, afin d'éviter des sanctions administratives ou judiciaires.

1.2.3.2 Principales normes et lois applicables

Dans ce qui suit, nous présentons les principales normes qui ont été instaurées par les organisations internationales pour préserver la sécurité des données médicales.

ISO/IEC 27001 [1]

Il s'agit d'une norme internationale qui définit les exigences relatives à la mise en œuvre d'un système de gestion de la sécurité de l'information (SGSI). Elle encourage les organisations à identifier, évaluer et traiter les risques associés à leurs informations sensibles, y compris les données médicales.

Cette norme constitue un cadre de référence pour notre projet, notamment pour l'organisation de la sécurité (politiques, procédures, audits, etc.).

Règlement Général sur la Protection des Données (RGPD)

Il s'agit d'une loi européenne qui protège les données personnelles de tous les citoyens de l'Union européenne. Elle s'applique également aux hôpitaux et aux cliniques. Par exemple, elle exige que le consentement des patients soit obtenu avant que leurs données ne soient collectées ou partagées.

HIPAA

C'est une loi américaine qui impose des normes strictes pour garantir la confidentialité, l'intégrité et la disponibilité des données de santé. Elle s'applique aux hôpitaux, aux médecins, aux compagnies d'assurance et aux autres entités de soins de santé, qui doivent protéger les données de santé des patients contre les accès non autorisés ou la fuite de données.

Hébergeurs de Données de Santé (HDS)

En France, les données de santé doivent être hébergées chez des prestataires certifiés (HDS), selon un référentiel strict contrôlé par l'agence du numérique en santé [8].

Cette certification garantit la mise en œuvre des mesures pratiques telles que le chiffrement des données, les sauvegardes, la traçabilité des accès et la gestion des incidents.

1.3 Risques et menaces dans le domaine médical

Le secteur de la santé est devenu une cible privilégiée des cybermenaces, en raison de la valeur stratégique et sensible des données qu'il manipule. Que ce soit par malveillance ou par erreur, toute faille de sécurité peut avoir de graves conséquences : atteinte à la vie privée des patients, interruption des soins et lourdes sanctions juridiques pour les établissements concernés.

1.3.1 Cyberattaques et ransomwares

Les établissements de santé tels que les hôpitaux et les cliniques sont souvent la cible d'attaques par ransomware où les pirates informatiques chiffrent les données de l'établissement et demandent une rançon en échange de leur déverrouillage. Ce type d'attaque peut complètement paralyser les systèmes de santé, retarder des interventions critiques et même mettre des vies en danger. Selon une étude menée par Kaspersky [9], près de 50 % des établissements de santé ont subi au moins une attaque de ce type au cours des dernières années.

1.3.2 Erreurs humaines

L'erreur humaine est une faille de sécurité majeure. Elle peut prendre la forme de :

- Un mot de passe faible ou partagé.
- Un clic sur un lien malveillant.

- Mauvaise configuration des systèmes.

D'après IBM [10], les erreurs humaines sont responsables de 23 % des violations de données dans le secteur de la santé.

Ces erreurs montrent qu'aucune technologie ne peut garantir seule la sécurité. Ainsi, la sensibilisation et la formation des professionnels de santé sont tout aussi cruciales.

1.3.3 Accès non autorisés

L'accès non autorisé aux systèmes de données médicales, qu'il soit interne (par des employés) ou externe, représente une menace importante. Un mauvais contrôle de l'accès aux données ou des failles dans les systèmes d'authentification peuvent permettre à des personnes non autorisées de consulter ou de modifier les informations médicales sensibles des patients. La IAM est essentielle pour prévenir ce type de menace.

1.3.4 Fuite ou vol de données

Le vol ou la fuite de données sensibles, en particulier d'informations médicales, est une menace persistante dans le secteur médical. Les cybercriminels peuvent exploiter ces données en les vendant sur le marché noir, mettant ainsi en péril la confidentialité des patients et exposant les établissements à des sanctions juridiques.

Le Ponemon Institute [11] estime que le coût moyen d'une violation de données dans le secteur de santé peut atteindre 7,13 millions de dollars par incident.

1.3.5 Malwares et logiciels malveillants

Les malwares sont des logiciels malveillants conçus pour modifier, voler ou détruire des données. Dans un hôpital, un simple virus informatique peut :

- Compromettre l'accès aux dossiers des patients.
- Ralentir les systèmes critiques.
- voire interrompre les services médicaux.

Selon Extencia [12], certains logiciels malveillants ciblent directement les professionnels de santé, ce qui augmente le risque de compromission.

1.4 Importance de la sécurité dans les cliniques et hôpitaux

La sécurité des données dans les établissements de santé n'est pas seulement une exigence technique mais c'est un impératif vital. Chaque jour, les hôpitaux et les cliniques traitent des

données extrêmement sensibles : antécédents médicaux, diagnostics, traitements, informations personnelles, etc. Un défaut de protection de ces données peut avoir de graves conséquences, telles que :

- La perte de confiance entre les patients et l'établissement.
- La responsabilité juridique, en cas de non-respect de réglementations telles que le "RGPD".
- Risque pour la santé des patients, en cas d'indisponibilité, d'altération ou de suppression de leurs données.

Par exemple, une attaque informatique qui bloque l'accès aux dossiers médicaux peut retarder un traitement urgent, voire le rendre impossible. C'est pourquoi il est essentiel que les hôpitaux mettent en place des systèmes de protection solides : chiffrement, authentification sécurisée, sauvegardes régulières et surveillance en temps réel.

Selon les avis d'experts :

- L'ENISA [7] souligne que les hôpitaux sont des cibles privilégiées car leurs systèmes sont souvent insuffisamment protégés.
- L'Organisation mondiale de la Santé (OMS) affirme que *"la cybersécurité fait désormais partie intégrante de la sécurité des soins"* [13]. Cela signifie que protéger les systèmes informatiques, c'est aussi protéger la vie humaine.

Dans le domaine médical, protéger les systèmes d'information, c'est aussi protéger la vie humaine.

1.5 Contrôle d'accès

Les applications médicales gèrent des données sensibles et critiques, soumises à des réglementations strictes (HIPAA, GDPR, HDS). Un contrôle d'accès robuste est indispensable pour :

- Protéger la vie privée des patients.
- Limiter les accès aux seuls professionnels autorisés.
- Assurer la traçabilité des actions (audit).

Dans cette section, nous présentons le contrôle d'accès dans les applications médicales et les principaux modèles de contrôle d'accès décrits dans la littérature.

1.5.1 Définition

Le contrôle d'accès est un mécanisme de sécurité utilisé pour restreindre l'accès à un système ou à ses ressources, physiques ou numériques, aux seules entités autorisées. En informatique, ce

processus permet d'accorder aux utilisateurs des droits d'accès spécifiques à certains systèmes, informations ou ressources [14].

Pour obtenir un accès, les utilisateurs doivent fournir des informations d'identification (telles qu'un mot de passe ou une carte d'accès). Dans les systèmes physiques, ces identifiants peuvent varier, mais ceux qui ne peuvent pas être transférés (comme les données biométriques) offrent généralement une sécurité supérieure.

Le contrôle d'accès repose sur trois fonctions clés :

- l'authentification, qui vérifie l'identité de l'utilisateur ;
- l'autorisation, qui définit les droits d'accès accordés ;
- l'audit, qui enregistre les tentatives d'accès et les actions pour en assurer la traçabilité.

Dans un système informatique, le sujet (souvent un utilisateur) tente d'accéder à un objet (généralement une ressource, telle qu'un fichier ou un logiciel). Une liste de contrôle d'accès "Access Control List (ACL)" est souvent utilisée pour déterminer quels utilisateurs ont quels droits sur chaque ressource. Ces droits peuvent concerner l'accès à certaines informations, le temps de consultation ou la possibilité de modifier des données.

L'administrateur du système peut ainsi définir et gérer les privilèges d'accès pour assurer la confidentialité et la sécurité des données [14].

1.5.2 Catégories de contrôle d'accès

Dans cette sous-section, nous présentons les principales catégories de contrôle d'accès.

1.5.2.1 Contrôle d'accès discrétionnaire (DAC)

Définition

Le contrôle d'accès discrétionnaire "Discretionary Access Control (DAC)" [15] est un modèle de sécurité dans lequel le propriétaire d'une ressource (comme un fichier ou un dossier) détermine qui peut y accéder et quels droits lui sont accordés. Ce type de contrôle d'accès repose sur l'identité des utilisateurs ou de leurs groupes et permet au propriétaire de transférer ou de modifier les autorisations d'accès. La Figure 1.1 illustre le fonctionnement du protocole de contrôle d'accès DAC.

Exemple

Sous un système Windows, un utilisateur peut créer un dossier, y placer un fichier, puis choisir quels autres utilisateurs ont l'autorisation de le lire, de l'écrire ou de le supprimer.

1.5.2.2 Contrôle d'accès obligatoire (MAC))

Définition

Le contrôle d'accès obligatoire "Mandatory Access Control (MAC)" [16] est un modèle de

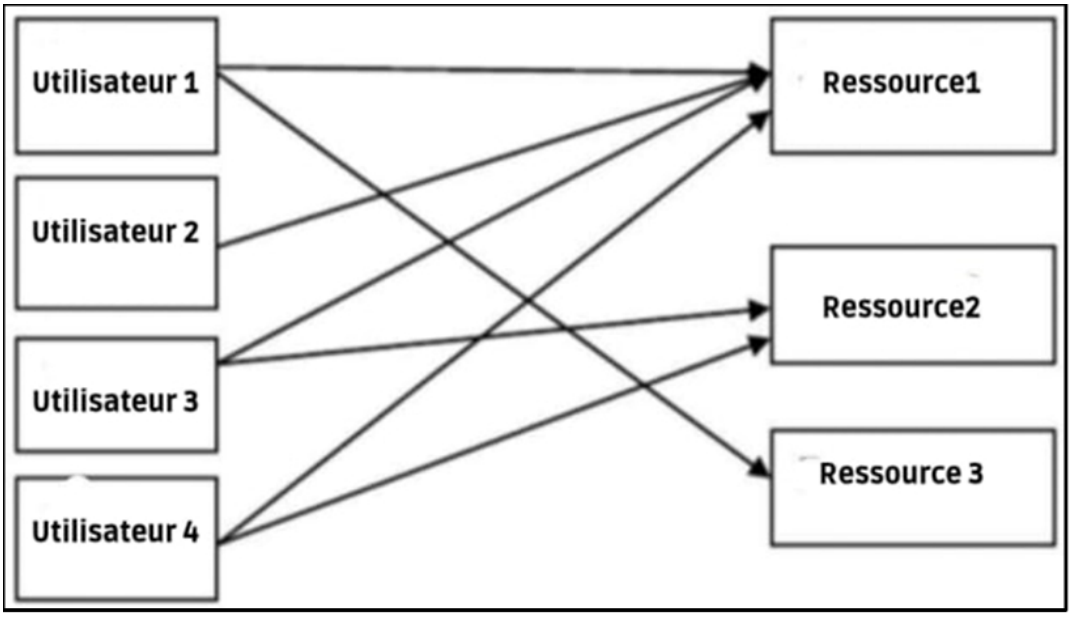


Fig. 1.1 : Modèle de contrôle d'accès DAC [15]

sécurité dans lequel l'accès aux ressources est déterminé par une politique centralisée, basée sur les niveaux de classification des sujets (entités actives demandant l'accès aux objets) et des objets (entités passives stockant des informations) du système (par exemple, confidentiel, secret). Dans ce modèle de contrôle d'accès, les utilisateurs ne peuvent pas modifier ces règles. La Figure 1.2 symbolise le fonctionnement du modèle de contrôle d'accès MAC.

Exemple

Dans un système militaire, un utilisateur sans *"accès secret"* ne pourra pas lire un document classé *"secret"*, même s'il en connaît l'existence.

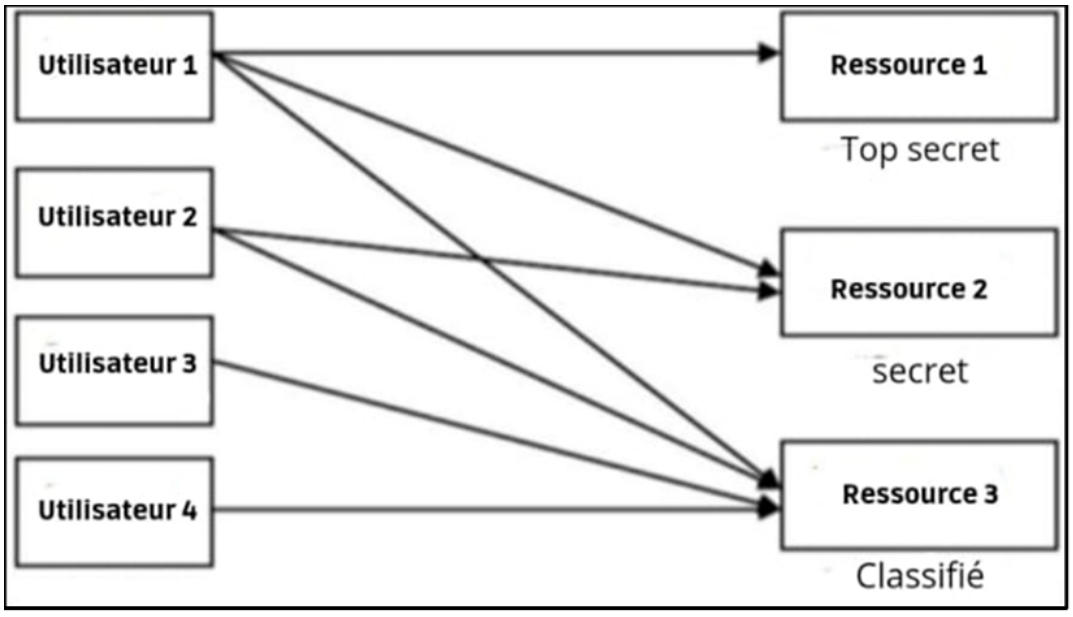


Fig. 1.2 : Modèle de contrôle d'accès MAC [16]

1.5.2.3 Contrôle d'accès basé sur les rôles (RBAC)

Définition

Le contrôle d'accès basé sur les rôles "Role-Based Access Control (RBAC)" [17] est un modèle de sécurité dans lequel les autorisations sont attribuées à des rôles plutôt qu'à des utilisateurs individuels. Un utilisateur se voit attribuer un ou plusieurs rôles, et chaque rôle détermine les actions qu'il peut effectuer.

Le modèle RBAC permet une gestion centralisée et simplifiée des droits d'accès, notamment dans les grandes organisations. La Figure 1.3 montre le fonctionnement du modèle de contrôle d'accès RBAC.

Exemple

Dans un hôpital :

- Le rôle "Médecin" permet d'accéder aux dossiers des patients et de prescrire des médicaments.
- Le rôle "Secrétaire" permet uniquement de consulter les informations administratives des patients.
- Si un utilisateur obtient le rôle de "Médecin", il héritera automatiquement des droits associés à ce rôle, sans qu'on ait à les lui attribuer individuellement.

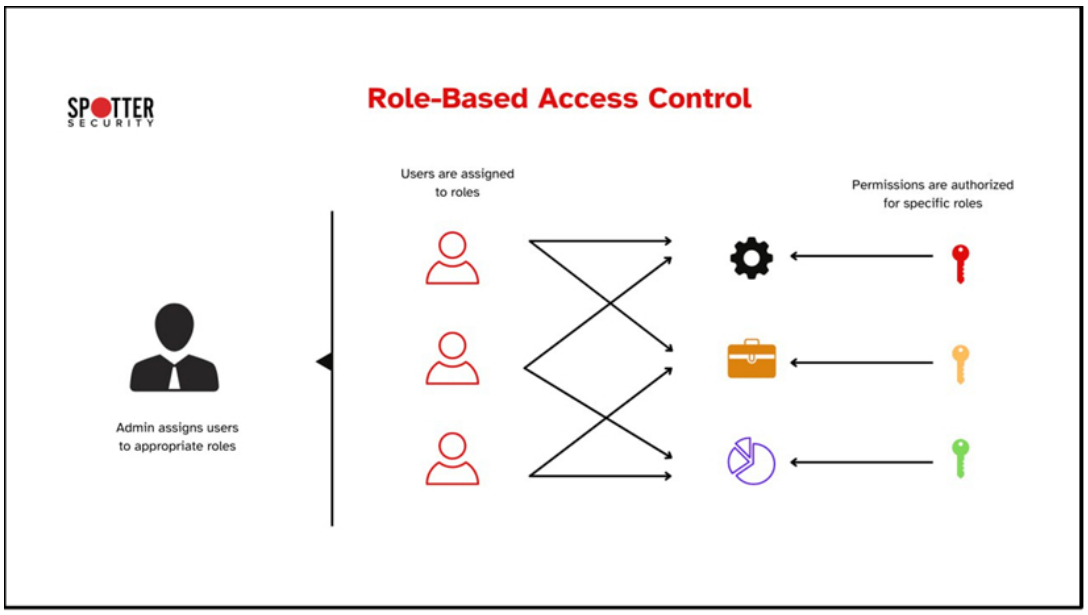


FIG. 1.3 : Modèle de contrôle d'accès RBAC [17]

1.5.2.4 Contrôle d'accès basé sur les attributs

Définition

Le modèle de contrôle d'accès basé sur les attributs Attribute-Based Access Control (ABAC)

[18] est un système dans lequel les décisions d'accès sont prises en fonction d'un ensemble d'attributs liés à :

- L'utilisateur (par exemple, son rôle, sa spécialité) ;
- La ressource (par exemple, son type, son niveau de sensibilité) ;
- L'environnement (par exemple, l'heure, le lieu, etc.) ;
- L'action demandée.

Contrairement au modèle de contrôle d'accès RBAC, le modèle ABAC ne se limite pas aux rôles ; il utilise une politique dynamique et précise, adaptée à chaque contexte. La Figure 1.4 illustre le fonctionnement du protocole de contrôle d'accès ABAC.

Exemple

Dans une clinique, un médecin peut accéder au dossier médical d'un patient uniquement s'il :

- Travaille dans la même clinique.
- Possède la spécialité correspondante (par exemple, cardiologie).
- Et que c'est entre 8 h et 18 h.
- Décision d'accès : Autorisé uniquement si tous ces attributs sont vrais.

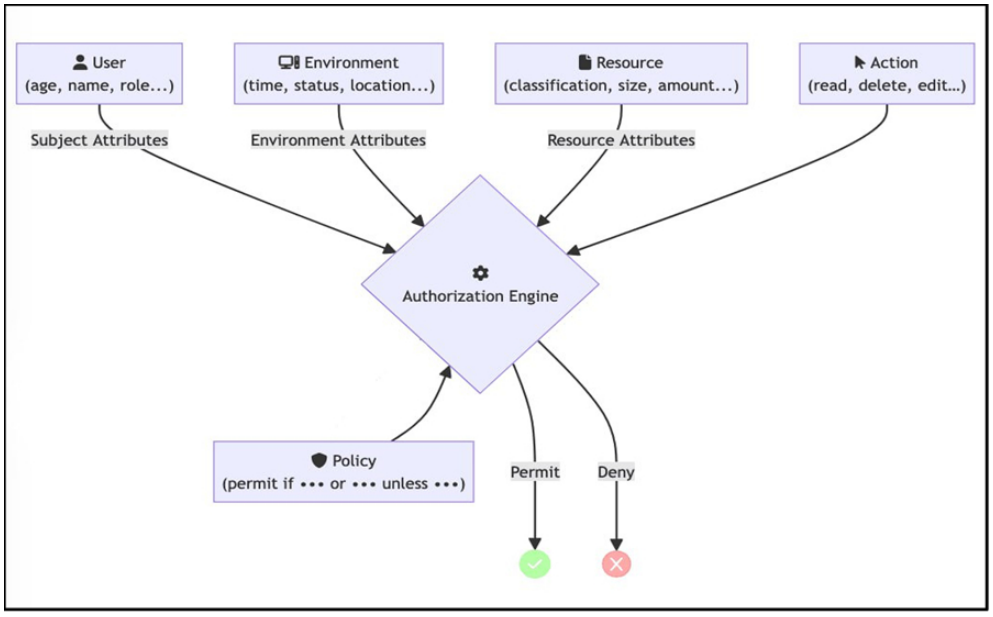


FIG. 1.4 : Modèle de contrôle d'accès ABAC [18]

1.5.2.5 Contrôle d'accès basé sur les attributs multi-autoritaires (MA-ABE)

Le Multi-authority Attribute-based Encryption (MA-ABE) [19] est une forme avancée du chiffrement basé sur les attributs "Attribute-based Encryption (ABE)". Contrairement à l'ABE classique, où une seule autorité gère tous les attributs, le MA-ABE permet à plusieurs autorités indépendantes de gérer chacune un sous-ensemble d'attributs.

Cette approche répond mieux aux exigences des environnements complexes et distribués comme les établissements de santé (cliniques, hôpitaux), où les attributs peuvent dépendre de plusieurs entités (ex. : rôle, spécialité, établissement).

Dans notre projet, nous avons utilisé MA-ABE pour chiffrer les données médicales des patients, en imposant des politiques d'accès précises où seul le personnel médical appartenant à un établissement de santé donné, avec un rôle défini et une spécialité particulière, peut déchiffrer les dossiers médicaux des patients.

Cette approche garantit un contrôle d'accès fin et sécurisé, même en cas de compromission d'une partie du système. Nous avons choisi MA-ABE pour :

- Renforcer la sécurité au-delà du simple "RBAC".
- Éviter la centralisation du pouvoir d'attribution des accès.
- Permettre une gestion souple et décentralisée des attributs, en fonction de chaque contexte métier.

Cette approche améliore la confidentialité, limite les risques d'accès non autorisé, et s'aligne avec les exigences de protection des données médicales sensibles.

1.6 Conclusion

La sécurité des systèmes d'information dans le domaine médical ne se limite pas aux mesures techniques mais elle est essentielle à la qualité des soins, à la confiance patient-médecin et au partage des responsabilités entre professionnels de santé, administrateurs système et décideurs. Par ailleurs, en combinant des mécanismes de sécurité (chiffrement, contrôle d'accès, surveillance) à des normes strictes et à une culture de cybersécurité partagée, les établissements de santé peuvent protéger efficacement les données des patients contre les menaces numériques croissantes.

Dans ce chapitre, nous avons fait un tour d'horizon sur les concepts de base de la sécurité des systèmes d'informations tout en mettant l'accent sur les systèmes d'informations qui concernent les données médicales. Puis nous avons mis en valeur le service de contrôle d'accès dans ce type de systèmes par illustration de différents modèles de contrôle d'accès.

CHAPITRE 2

ARCHITECTURE DE LA PLATEFORME DE GESTION DES DONNÉES MÉDICALES

2.1 Introduction

Dans ce chapitre, nous présentons en détail l'architecture de la plateforme de gestion des données médicales. Cette architecture est développée autour d'un ensemble de composants, et son objectif principal est d'assurer un fonctionnement indépendant et de permettre une coopération sécurisée entre différents établissements de santé, tout en respectant les exigences de confidentialité, de sécurité et de traçabilité des données. Chaque composant joue un rôle clairement défini, avec une attention particulière portée à l'intégration de mécanismes de sécurité tels que la blockchain et le chiffrement basé sur MA-ABE.

2.2 Description générale de l'architecture

La gestion confidentielle et optimale des données médicales repose sur un ensemble d'entités principales interconnectées. Chacune contribue à la cohérence du système en jouant un rôle spécifique dans le traitement, la protection et la circulation des informations sensibles.

Les entités fondamentales auteur desquelles est structurée l'architecture permettant la sécurisation des données médicales sont comme suit :

1. **L'administrateur (Admin)**
   Il s'agit de la principale entité de supervision. Son rôle est d'enregistrer les établissements médicaux dans le système, en n'approuvant que les enregistrements émanant d'entités légitimes.

2. **Établissement médical**
   Cette entité représente les établissements de santé tels que les hôpitaux, les cliniques, les laboratoires d'analyse, etc. Chaque établissement est responsable de la gestion de son

personnel médical (médecins, infirmières, etc.) en fonction des attributs qu'il administre. Il est responsable de la distribution des clés cryptographiques, de la publication des clés publiques et de la génération des clés privées pour ses utilisateurs autorisés, conformément aux politiques d'accès définies.

3. **Le patient**
   Il est responsable de la protection de ses données médicales. Avant de les stocker, il génère une clé personnelle qu'il utilise pour chiffrer ses informations de santé. Une fois chiffrées, ces données sont déposées dans un cloud multimédia accessible au personnel médical autorisé. La clé de chiffrement utilisée pour protéger les données est ensuite chiffrée à l'aide du mécanisme MA-ABE, conformément à une politique d'accès définie par le patient et cette clé chiffrée est enregistrée sur la blockchain, garantissant qu'elle ne peut être accessible que par les personnes autorisées.

4. **Le personnel médical**
   Il accède aux données médicales via le cloud. Cependant, l'accès au contenu reste strictement encadré : seules les personnes répondant à des conditions précises (comme le rôle professionnel ou les autorisations reçues) peuvent déchiffrer et exploiter ces informations, assurant ainsi un haut niveau de confidentialité.

5. **Le Cloud**
   Il sert à stocker les données en un seul endroit sûr, garantissant leur disponibilité continue et la protection contre la perte. Il facilite aussi leur partage contrôlé entre utilisateurs autorisés, tout en offrant une gestion flexible des accès et une capacité d'adaptation à l'évolution des besoins.

   Le cloud se compose de deux modules complémentaires : une base de données NoSQL pour gérer les métadonnées des utilisateurs (patients et personnel médical), et un espace de stockage multimédia dédié aux dossiers médicaux, protégés par un chiffrement robuste.

6. **La blockchain**
   La blockchain stocke les clés de chiffrement/déchiffrement ainsi que des métadonnées associées aux dossiers médicaux.

7. **Les autorités d'attribution des droits**
   Il s'agit des établissements médicaux sont responsables de la création et de la gestion des attributs utilisés pour définir les droits d'accès, garantissant ainsi l'authenticité et la pertinence des informations utilisées pour contrôler l'accès aux données.

Cette architecture assure un équilibre entre la sécurité, l'accessibilité des données et le respect strict de la confidentialité des utilisateurs.

2.3 Schéma de l'architecture et description des composants

2.3.1 Diagramme de cas d'utilisation

Le diagramme de cas d'utilisation illustre les principales interactions entre les utilisateurs et la plateforme de gestion des dossiers médicaux. Il montre les fonctionnalités disponibles pour chaque acteur en fonction de son rôle dans le système.

La Figure 2.1 présente le diagramme de cas d'utilisation et montre qu'il s'agit d'un système structuré et décentralisé dans lequel chaque utilisateur a un rôle bien défini. L'accès aux données est sécurisé et contrôlé par des règles basées sur les attributs.

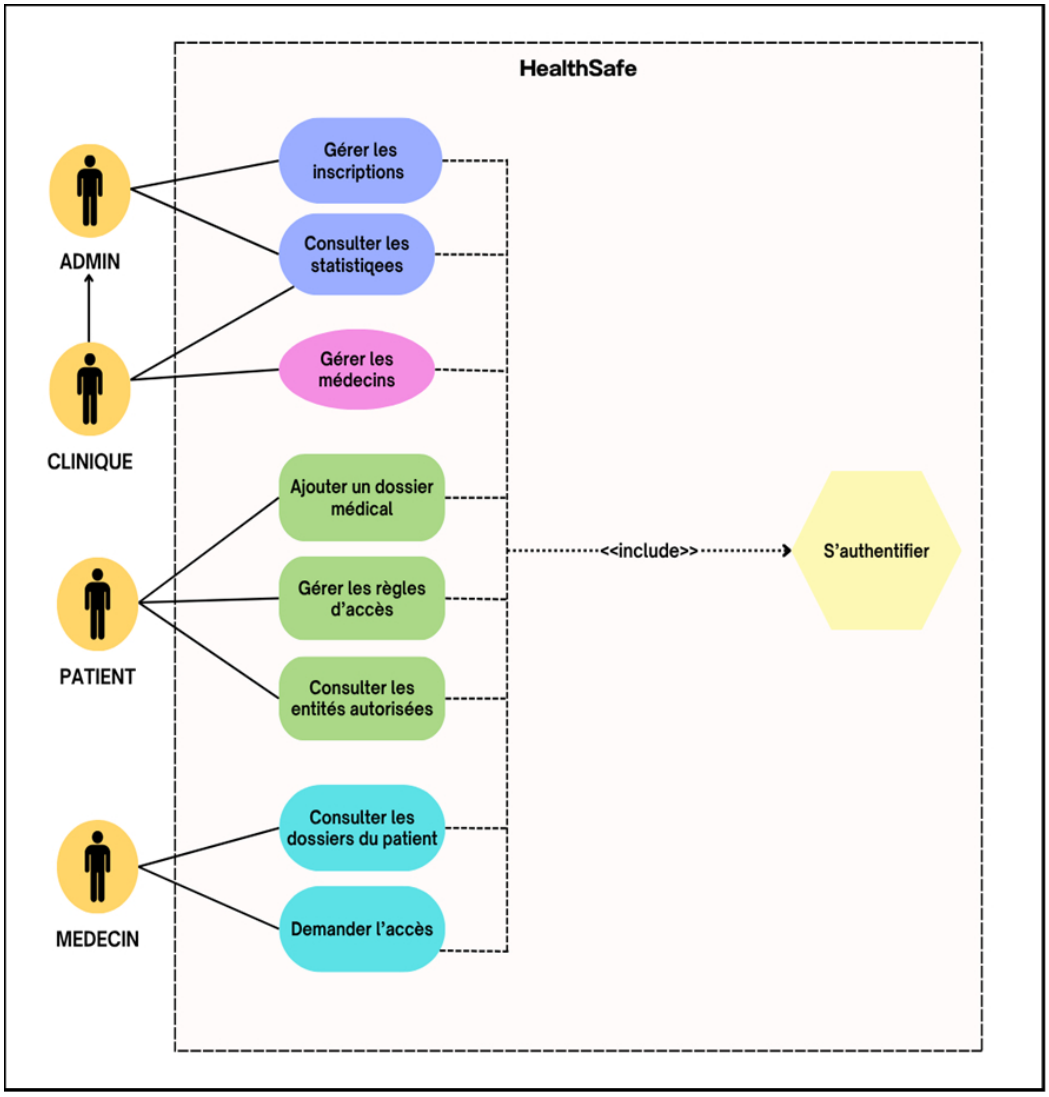


Fig. 2.1 : Diagramme de cas d'utilisation

Les cas d'utilisation

1. **S'authentifier**
   - **Admin** : Se connecter pour accéder aux fonctionnalités
   - **Établissement médical, Personnel médical** : Connexion après validation.
   - **Patient** : Se connecter au système.
2. **Gérer les inscriptions**
   L'admin valide les demandes d'inscription des cliniques et des patients si les informations et les données sont correctes, sinon il les rejeter.
3. **Consulter les statistiques**
   - **L'admin** : Visualise le nombre total d'utilisateurs, le nombre d'utilisateurs actifs, ainsi que le nombre de documents des patients.
   - **Établissement médical** : voir le nombre de patients ayant accordé l'accès à leurs médecins, le nombre de médecins autorisés, ainsi que leurs noms.
4. **Gérer les utilisateurs**
   - L'admin enregistre les établissements médicaux dans le système en approuvant uniquement les inscriptions des entités légitimes
   - L'admin affiche la liste des utilisateurs, consulte les dossiers des patients, et supprime un utilisateur.
   - Établissement de santé gère le personnel médical (médecins, infirmiers, etc.) en fonction des attributs qu'il administre.
5. **Ajouter un dossier médical**
   Un dossier médical est ajouté par le patient et il est stocké dans le cloud.
6. **Gérer les règles d'accès**
   - Créer une règle s'il n'en existe pas, en se basant sur les noms des cliniques affichées et les spécialités des médecins qui y travaillent.
   - Modifier la règle pour ajouter ou retirer des médecins autorisés.
   - Supprimer la règle définissant les accès autorisés.
7. **Consulter les entités autorisées**
   Voir les établissements de santé, le personnel médical ayant accès à ses données, ainsi que leurs noms.

8. **Demander l'accès**

   Récupérer les clés de déchiffrement dans la blockchain et les dossiers médicaux chiffrés dans le cloud par le personnel soignant autorisé. L'accès aux dossiers des patients n'est autorisé que si les attributs détenus par l'utilisateur sont conformes à la politique d'accès définie.

2.3.2 Schéma global de l'architecture

La Figure 2.2 présente l'architecture globale de la plateforme de gestion sécurisée des dossiers médicaux et illustre toutes interactions entre les différentes entités dans le système.

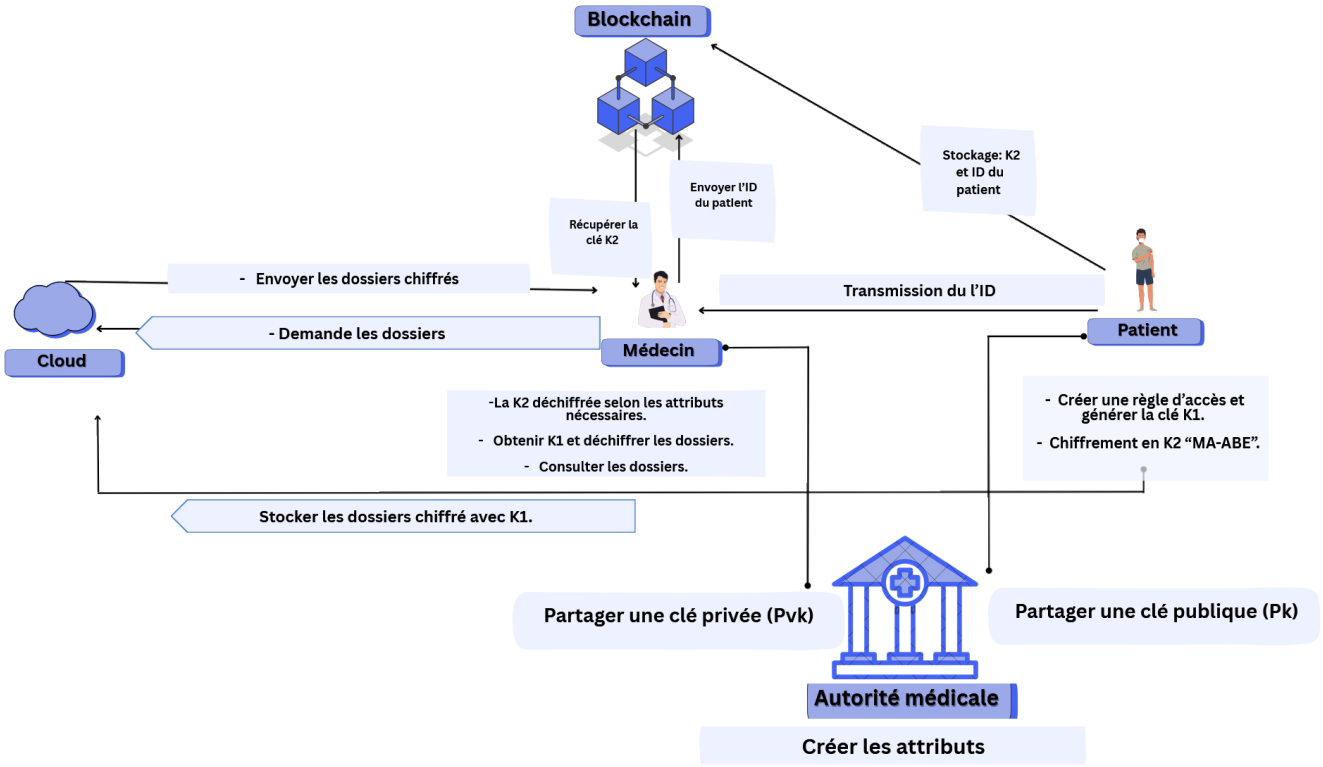


FIG. 2.2 : Architecture de la plateforme de gestion sécurisée des dossiers médicaux

2.3.3 Description des composants (Rôle et interaction)

Dans cette sous-section, nous présentons les différentes entités actives dans la plateforme de sécurité des données médicales, en précisant leurs rôles et leurs interactions.

1. **Patient**

   - **Rôle**
     - Le patient est à l'origine des données médicales. Il peut créer, consulter et supprimer ses dossiers, définir les attributs d'accès, et publier les clés chiffrées liées à son identifiant dans la blockchain.

- **Interactions**
  - Ajoute ses dossiers médicaux au cloud.
  - Partage les données et la clé avec le cloud.
  - Le patient crée une règle d'accès, et à chaque modification de cette règle, une nouvelle clé est générée puis chiffrée.
  - Il publie les clés chiffrées avec son identifiant dans la blockchain, assurant un contrôle d'accès sécurisé et traçable.
  - Transmet son identifiant, via une carte magnétique ou un code QR, au personnel médical concerné afin de permettre l'identification du propriétaire des données.
  - Gère les droits d'accès en collaboration avec les autorités compétentes.

2. **Autorités**

- **Rôle**
  - Les autorités sont responsables de la création et de la gestion des attributs utilisés pour définir les droits d'accès aux données médicales ainsi que de la gestion de leur personnel médical (médecins, infirmiers, etc.).
- **Interactions**
  - Génèrent des attributs nécessaires à la définition des politiques d'accès ;
  - Publient les clés publiques associées à chaque attribut ;
  - affectent des attributs aux utilisateurs selon leurs rôles et fonctions ;
  - Distribuent des clés privées aux utilisateurs, en fonction des attributs qu'ils possèdent
  - Veillent à leur validité et leur mise à jour lorsque c'est nécessaire.

3. **Blockchain**

- **Rôle**
  - La blockchain stocke de manière sécurisée et immuable les clés chiffrées ainsi que l'identifiant du patient, garantissant leur conservation et la traçabilité des opérations.
- **Interactions**
  - Les clés chiffrées, régulièrement mises à jour, sont enregistrées dans le dernier bloc, et c'est cette clé présente dans ce bloc qui est effectivement partagée avec les parties concernées.
  - Partage de la clé chiffrée destinée au stockage centralisé avec le cloud via le dernier bloc.
  - Partage de la clé chiffrée destinée au personnel médical avec les médecins via le dernier bloc, facilitant ainsi leur accès contrôlé.

- Valider ou refuser les demandes d'accès selon les règles établies.
- Le système garantit la transparence et la conformité des échanges entre tous les acteurs.

4. **Cloud**

   - **Rôle**
     - Assure le stockage sécurisé des dossiers médicaux des patients.
   - **Interactions**
     - Reçoit et conserve les dossiers transmis par le patient.
     - Reçoit l'identifiant du patient de la part du médecin lors d'une demande d'accès.
     - Transmet cet identifiant à la blockchain pour récupérer la clé chiffrée correspondante.
     - Déchiffre cette clé à l'aide d'une clé de partage et l'utilise pour chiffrer les dossiers du patient avant de les transmettre au médecin.
     - Travaille en coordination avec les mécanismes de sécurité afin de garantir la confidentialité et l'intégrité des données échangées.

5. **Le personnel médical**

   - **Rôle**
     - Le personnel médical consulte, analyse ou télécharge les données médicales du patient dans le cadre de son activité professionnelle.
   - **Interactions**
     - Soumet une demande d'accès via la plateforme pour consulter les données d'un patient, en précisant l'identifiant qui lui a été partagé.
     - Transmet cet identifiant au cloud afin de récupérer les dossiers médicaux chiffrés.
     - En parallèle, il envoie une requête à la blockchain pour récupérer la clé chiffrée enregistrée dans le dernier bloc correspondant à ce patient.
     - Le personnel médical tente ensuite de déchiffrer cette clé en fonction de ses attributs. Si le déchiffrement réussit, il obtient la clé de déchiffrement des dossiers.
     - Il utilise cette clé pour déchiffrer les dossiers récupérés du cloud. Une fois les données déchiffrées, il peut les consulter et les télécharger si nécessaire.

2.3.4 Diagramme de séquence

Ce diagramme de séquence comme montre la Figure 2.3 représente le scénario global de l'accès sécurisé aux dossiers médicaux dans la plateforme. Il montre comment les différents acteurs interagissent avec le système, en suivant les étapes de vérification, de chiffrement et de contrôle d'accès.

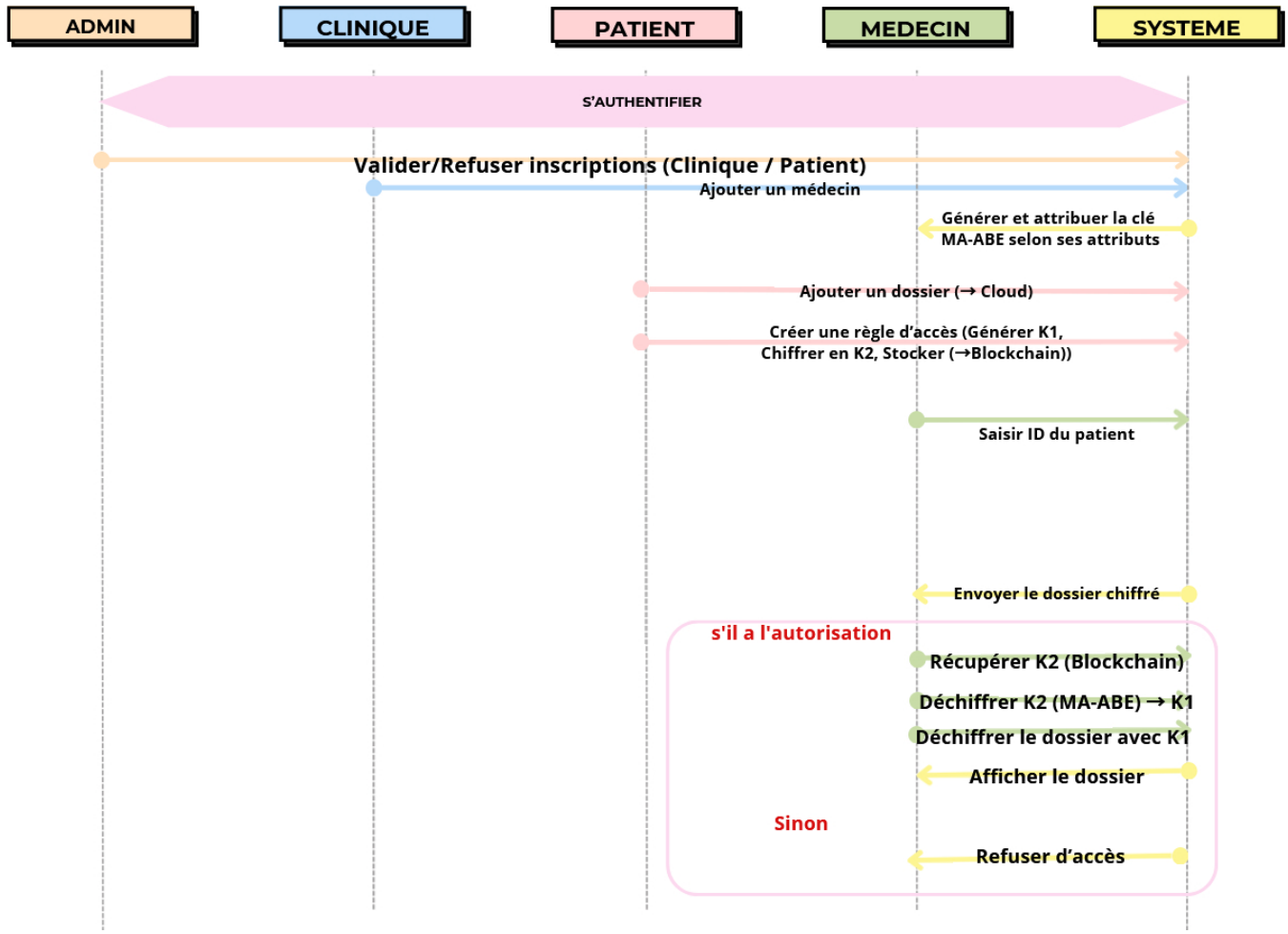


FIG. 2.3 : Diagramme de séquence

Déroulement du scénario

1. **Connexion**
   Chaque utilisateur doit être authentifié pour accéder à son espace. Cette étape est commune à tous les rôles : administrateur, hôpital, médecin et patient. L'authentification permet d'activer les fonctions propres à chaque profil en toute sécurité.

2. **Validation des inscriptions (Admin)**
   L'administrateur consulte les demandes en attente et décide de les valider ou de les rejeter, qu'il s'agisse de patients ou de cliniques. Les comptes validés peuvent se connecter, tandis que les comptes rejetés restent inaccessibles.

3. **Ajout de médecin (établissement médical)**
   L'établissement médical accède à son espace de gestion du personnel médical. Lorsqu'un nouveau personnel médical est ajouté, le système lui attribue automatiquement des caractéristiques, telles que la spécialité et le nom de l'établissement. Une clé privée MA-ABE est alors générée sur la base de ces attributs. Cette clé sera partagée avec le personnel

médical afin qu'il puisse l'utiliser ultérieurement pour déchiffrer les dossiers des patients auxquels il a accès.

4. **Ajout de dossier et définition des règles d'accès (Patient)**

   - Le patient ajoute un dossier médical, qui est stocké dans le cloud.
   - Il définit une règle d'accès en choisissant les attributs (nom de l'établissement de santé, spécialité, etc.) qui détermineront qui peut accéder au dossier. Cela se fait selon les étapes suivantes :
     - **Étape 1**
       Génération et chiffrement avec clé symétrique à l'aide du cryptosystème AES où le système génère une clé aléatoire appelée K_1. Cette clé est générée à l'aide d'un générateur cryptographiquement sécurisé (ex. crypto.randomBytes ou équivalent WebCrypto). La clé K_1 est utilisée pour chiffrer le contenu du dossier médical à l'aide de l'algorithme "Advanced Encryption Standard (AES)", garantissant ainsi la confidentialité des données stockées.
     - **Étape 2**
       Chiffrement avec MA-ABE : Le système utilise les clés publiques MA-ABE fournies par les différentes autorités (par exemple, l'autorité "Hôpital", l'autorité "Spécialité"). Chaque attribut (par exemple "Spécialité : cardiologie", "Établissement : Clinique de Tlemcen") est associé à une clé publique distincte, générée par son autorité d'attribut respective. Ces clés publiques individuelles sont ensuite combinées pour former une clé publique globale que le patient peut utiliser pour chiffrer la clé K_1 avec une politique d'accès personnalisée. Exemple de politique définie par le patient : "Spécialité : Cardiologie" ET "Établissement : Clinique Tlemcen". Le chiffrement est ensuite effectué comme suit :

       $$K_2 = MAABE\_encrypt(K_1, Policy, Public\_combined\_keys)$$

       Résultat
       Seule une personne (par exemple un médecin) possédant tous les attributs requis par la politique sera en mesure de déchiffrer la clé K_2 à l'aide de sa clé privée MA-ABE générée en fonction de ses attributs.
       Remarque
       Le patient n'a pas besoin de clés privées pour le système MA-ABE. Les clés publiques de MA-ABE sont obtenues auprès des autorités lors de l'initialisation du système.
     - **Étape 3**
       Enregistrement sur la blockchain : La version chiffrée de la clé K_1 est stockées dans la blockchain avec l'ID du patient : K_2 (version MA-ABE) pa-

tient_ID. Cela permet au médecin de récupérer ultérieurement la bonne clé pour ses privilèges afin de déchiffrer le dossier médical du patient.

5. **Consultation du dossier (Médecin)**
   Le médecin saisit l'ID du patient à consulter. Cet identifiant est utilisé pour récupérer les données nécessaires depuis :

   - Le cloud : pour obtenir le dossier médical chiffré.
   - La blockchain : pour récupérer la version chiffrée de la clé K_1 : K_2 (chiffrement 'MA-ABE')

   Seuls les médecins autorisés peuvent accéder aux dossiers, selon la politique définie par le patient.

   Cas 2 : Déchiffrement à l'aide de K_2 (clé MA-ABE)

   - La blockchain retourne aussi K_2 (clé K_1 chiffrée selon une politique MA-ABE).
   - Le médecin tente de déchiffrer K_2 avec sa clé privée MA-ABE, générée en fonction de ses attributs (rôle, spécialité, hôpital, etc.).
   - Si les attributs du médecin satisfont la politique définie par le patient, le déchiffrement réussit : $K_1 = \text{MAABE\_decrypt}(K_2, \text{Clé\_privée\_du\_médecin})$. Puis, K_1 est utilisée pour déchiffrer le dossier :

     $$Dossier = AES\_decrypt(\text{Dossier\_chiffré}, K_1)$$

   - **Accès refusé** : Si le médecin ne satisfait pas les conditions MA-ABE (attributs insuffisants) : Le déchiffrement de la clé K_1 échoue et le dossier médical reste inaccessible.

2.4 Conclusion

L'architecture de la plateforme proposée repose sur une structure modulaire et sécurisée, où chaque composant assure une fonction bien définie. Elle garantit une gestion rigoureuse des données médicales, en intégrant des mécanismes de contrôle d'accès, de traçabilité et de confidentialité renforcés. Ainsi, grâce à l'interaction cohérente entre les éléments, notamment la blockchain pour le stockage des clés chiffrées et la traçabilité, le cloud pour l'hébergement des dossiers, et la plateforme pour la gestion des accès, le système assure un traitement fiable et maîtrisé des données. Cette organisation facilite l'adaptation du système à de nouveaux besoins tout en maintenant un haut niveau de sécurité et de transparence dans les échanges.

Le chapitre suivant sera consacré à la présentation des outils logiciels et matériels nécessaires au développement de la plateforme pour la sécurisation des dossiers médicaux des patients.

CHAPITRE 3

OUTILS LOGICIELS ET TECHNOLOGIES UTILISÉES POUR LA PLATEFORME HEALTHSAFE

3.1 Introduction

Le développement de la plateforme de gestion des données médicales repose sur un choix rigoureux des outils et technologies, répondant aux exigences de performance, de sécurité et de conformité réglementaire.

Selon le CHUM [20], la mise en place de solutions numériques dans le domaine médical nécessite une sécurité renforcée des données et une intégration fluide avec les systèmes existants. La norme "Commission électrotechnique internationale (CEI)" 62304 [21] précise les directives pour garantir la fiabilité et la conformité des logiciels médicaux.

Les technologies choisies pour ce projet ont été sélectionnées sur la base de critères tels que la stabilité à long terme, la compatibilité entre les composants, et la capacité à garantir une gestion sécurisée des données.

Ce chapitre détaille les solutions techniques adoptées, en abordant les aspects liés au développement frontend et backend, à la gestion des données, à la sécurité, ainsi qu'à l'intégration de la blockchain et MA-ABE.

3.2 Outils logiciels de développement

Éditeur de code : Visual Studio Code

Visual Studio Code a été adopté comme éditeur principal en raison de sa légèreté, de sa flexibilité et de ses nombreuses fonctionnalités intégrées, telles que l'auto-complétion, le débogage, la coloration syntaxique et le terminal intégré. Il offre également une excellente intégration avec Git, ce qui facilite la gestion des versions et le travail collaboratif.

Cet éditeur est aujourd'hui largement utilisé dans le développement de logiciels (Microsoft,

VS Code Overview).

Gestion de version : Git

Git a été utilisé pour suivre les modifications apportées au code et faciliter la collaboration entre les membres de l'équipe. Il permet une gestion efficace des versions et garantit la traçabilité des modifications tout au long du projet [22].

Outils de communication et collaboration

Slack a été utilisé pour la communication en temps réel, tandis que Gmail a facilité les échanges par e-mail et la gestion des communications. Ces outils sont essentiels pour assurer une collaboration fluide et une organisation efficace au sein de l'équipe.

3.3 Technologies utilisées

Dans cette section, nous présentons les différentes technologies que nous avons utilisées pour réaliser la plateforme HealthSafe.

3.3.1 Frontend : Vue.JS

Le frontend a été développé à l'aide de Vue.js [23], choisi pour sa simplicité, sa réactivité et sa structure modulaire, qui facilite la création d'interfaces dynamiques et faciles à entretenir. Il regroupe les différentes technologies du web :

1. **HyperText Markup Language (HTML)**
   Il s'agit d'un langage utilisé pour structurer le contenu des pages web à l'aide de balises. Contrairement aux langages de programmation, HTML se concentre uniquement sur l'organisation du contenu, sans aucune logique dynamique [24].

2. **Cascading Style Sheets (CSS)**
   C'est un langage qui sert à styliser les documents HTML. Il permet de personnaliser l'apparence des pages web, en définissant des éléments tels que les polices, les couleurs, et les mises en page [25].

3. **JavaScript (JS)**
   Il s'agit d'un langage de programmation utilisé pour ajouter de l'interactivité aux pages web. Il permet d'effectuer des mises à jour dynamiques, de gérer les événements utilisateur et de manipuler le DOM.

Parmi les bibliothèques principales utilisées :

- **@fortawesome/vue-fontawesome** : pour les icônes.
- **Axios** : pour les requêtes HTTP.

- **Sweetalert2** : pour les messages interactifs et les alertes personnalisées.
- **Vue-router** : pour la navigation entre les pages.
- **Jwt-decode** : pour décoder les tokens JWT et extraire les informations utilisateur.

3.3.2 Backend : Node.js et Express.js

Le backend a été implémenté avec *Node.js*, un environnement d'exécution JavaScript orienté événement, qui permet de gérer efficacement les opérations asynchrones et les requêtes simultanées. Nous avons utilisé *Express.js* pour concevoir des API REST de manière rapide et modulaire, facilitant ainsi la communication avec le frontend *Vue.js*. Parmi les bibliothèques principales utilisées côté serveur :

- **Bcryptjs** : pour le hachage sécurisé des mots de passe.
- **Cors** : pour gérer les politiques de sécurité CORS entre les origines.
- **Dotenv** : pour la gestion des variables d'environnement sensibles.
- **Express-fileupload** : pour le traitement des fichiers envoyés via HTTP.
- **JSONWebtoken** : pour la génération et la vérification des tokens d'authentification.
- **Sanitize-html** : pour nettoyer les entrées utilisateurs et prévenir les injections XSS.
- **Cloud** : pour le stockage et la gestion des fichiers dans le cloud.

3.3.3 Base de données : une architecture en trois couches

Pour assurer une meilleure gestion des données, une meilleure sécurité et une meilleure résilience, nous avons conçu notre système de base de données en utilisant une architecture à trois couches. Cette approche permet non seulement une séparation claire des types de données, mais aussi une meilleure tolérance aux défaillances partielles. En cas de défaillance ou de blocage d'une couche (par exemple MongoDB), certaines fonctionnalités du système restent accessibles, assurant ainsi une continuité partielle du service.

3.3.3.1 MongoDB : stockage des données utilisateurs

Nous avons utilisé MongoDB comme système de gestion de base de données NoSQL, qui est particulièrement bien adapté aux applications nécessitant une structure flexible et évolutive. L'administration est assurée par l'interface locale MongoDB Compass, qui permet de :

- La visualisation des collections et documents,
- L'exécution de requêtes filtrées,

- La modification directe des données sans requêtes manuelles.

MongoDB est utilisé pour stocker les données structurées, telles que les informations des utilisateurs et des patients.

La plateforme conçue est tolérante aux pannes, de sorte que si MongoDB tombe en panne (par exemple, si les patients ne peuvent pas accéder à la plateforme en raison d'un blocage), le système reste partiellement opérationnel et les médecins peuvent toujours accéder à d'autres fonctionnalités qui ne dépendent pas directement de cette couche.

3.3.3.2 Cloud : stockage des données multimédias

Les fichiers volumineux (PDF, images, résultats d'analyses, etc.) ne sont pas stockés dans MongoDB pour des raisons de performance. Ils sont externalisés vers une solution cloud spécialisée, décrite dans la section backend. Cela permet :

- Une gestion optimisée des fichiers,
- Une réduction de la charge sur la base principale,
- Une meilleure scalabilité pour les contenus multimédias.

3.3.3.3 Blockchain : gestion des clés de chiffrement

Pour garantir la sécurité et la traçabilité des données sensibles, notamment les fichiers stockés dans le cloud, les clés de chiffrement sont enregistrées dans une blockchain. Cette couche offre :

- Une protection contre la falsification,
- Une distribution décentralisée des clés,
- Un accès contrôlé et sécurisé aux données.

3.3.4 Sécurité basée sur AES et MA-ABE

La sécurité des données a été une priorité majeure dans le développement de la plateforme *HealthSafe*, notamment en raison de la nature sensible des informations médicales traitées. Deux mécanismes complémentaires ont été mis en place pour assurer la confidentialité des données et le contrôle d'accès.

3.3.4.1 AES (Advanced Encryptions Standard)

AES est un algorithme de chiffrement symétrique utilisé pour sécuriser les données. Il est largement adopté pour son efficacité et sa robustesse. AES fonctionne avec des clés de longueur fixe (128, 192 ou 256 bits) pour chiffrer et déchiffrer des données [26].

Fonctionnement

- AES utilise une méthode de chiffremeent par blocs, où les données sont divisées en blocs et traitées à l'aide de la clé secrète.
- Le même algorithme et la même clé sont utilisés pour les opérations de cryptage et de décryptage, ce qui en fait un cryptage symétrique.
- Ce processus permet de protéger rapidement et efficacement les données sensibles [4].

Avantages

- **Efficacité** : AES est rapide et performant, même avec de grandes quantités de données.
- **Sécurité éprouvée** : Il est considéré comme l'un des standards les plus sûrs et est utilisé à l'échelle mondiale [26].
- **Large adoption** : AES est largement accepté par les organismes de réglementation et les normes de sécurité.

3.3.4.2 MA-ABE

Fonctionnement

- Dans un système MA-ABE, plusieurs autorités peuvent émettre des clés d'attributs pour un utilisateur.
- Ces clés sont utilisées pour chiffrer et déchiffrer des données en fonction des attributs de l'utilisateur.
- L'accès aux données est accordé si les attributs de l'utilisateur correspondent à ceux définis lors du chiffrement des données.
- Par exemple, un médecin avec un certain rôle et spécialité pourrait être autorisé à accéder à des informations spécifiques sur un patient [19].

Avantages

- **Contrôle d'accès fin**
  MA-ABE permet un contrôle d'accès détaillé en fonction des attributs des utilisateurs, garantissant que seules les personnes ayant les droits appropriés peuvent accéder à certaines informations [27].
- **Flexibilité**
  Il est particulièrement utile dans les environnements multi-organisationnels, où plusieurs autorités (par exemple, différents hôpitaux ou cliniques) contrôlent les accès.
- **Conformité réglementaire**
  Il permet de respecter des exigences strictes en matière de gestion des données et de confidentialité, comme celles définies par le RGPD [19].

3.3.4.3 Blockchain

a) Définition

La blockchain est une technologie qui fonctionne comme un grand registre numérique partagé, infalsifiable et indestructible, grâce à sa structure. Elle permet de stocker et transmettre des informations de façon sécurisée, transparente et sans avoir besoin d'un contrôle central [28].

La blockchain est constituée de blocs de données interconnectés. Chaque bloc contient des informations vérifiées par des participants appelés mineurs. Une fois validé, le bloc est ajouté de manière permanente à la chaîne à l'aide de la cryptographie.

Chaque utilisateur du réseau possède une copie de la blockchain, qui est mise à jour automatiquement chaque fois qu'un nouveau bloc est ajouté. Il est impossible de modifier ou de supprimer un bloc une fois qu'il a été ajouté. Grâce à un protocole informatique sécurisé, tous les utilisateurs peuvent ajouter des données au registre selon des règles précises [29].

Cette technologie repose sur des algorithmes cryptographiques solides (comme SHA-256) et des mécanismes de consensus distribué (comme le Proof of Work ou le Proof of Stake), ce qui renforce la sécurité et la résilience du système.

Elle assure également une traçabilité complète, utile dans des domaines comme la chaîne d'approvisionnement, les transactions financières, ou encore la gestion des données médicales sensibles, en garantissant que chaque action soit horodatée et non-répudiable.

En résumé, on pourra dire que la blockchain est une technologie fiable et sécurisée qui peut être utilisée dans de nombreux domaines, notamment la finance, la santé et les échanges numériques.

b) Fonctionnement

La Figure 3.1 illustre le fonctionnement d'une transaction sécurisée dans la blockchain où toutes les étapes de la transaction ont été explicitées.

c) Caractéristiques d'une blockchain

La technologie Blockchain repose sur un certain nombre de caractéristiques qui garantissent sa robustesse, sa fiabilité et son adoption croissante dans différents domaines. Dans ce qui suit, nous présentons les principales caractéristiques d'une blockchain :

1. **Décentralisation**
    - La blockchain utilise une architecture décentralisée, où la base de données est répartie entre plusieurs nœuds du réseau
    - Il n'y a pas d'autorité centrale pour valider les transactions, ce qui élimine la dépendance à l'égard d'un tiers de confiance.
    - Chaque participant (nœud) détient une copie du registre et participe à la validation par consensus.
2. **Transparence**

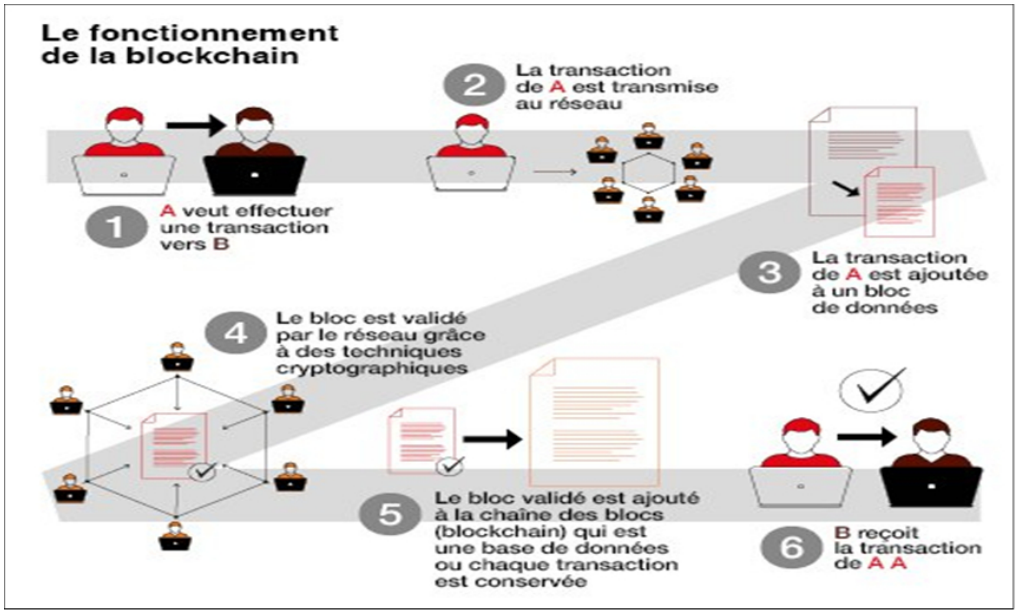


FIG. 3.1 : Fonctionnement d'une transaction sécurisée dans la blockchain [30]

- Toutes les transactions enregistrées sur la blockchain sont visibles par tous les participants au réseau.
- Le contenu réel reste chiffré et protégé par une clé privée, mais les métadonnées et l'historique sont accessibles, garantissant une traçabilité totale.
- Cette transparence renforce la confiance entre les parties concernées.

3. **Sécurité et immutabilité**

- Une fois qu'une transaction a été validée et ajoutée à un bloc, elle ne peut plus être modifiée (immutabilité).
- Pour modifier un enregistrement, il faudrait contrôler plus de 51 % des nœuds, ce qui est extrêmement coûteux et difficile.
- Le système s'appuie sur des algorithmes cryptographiques avancés (par exemple SHA-256) pour garantir l'intégrité des données.

4. **Autonomie**

- Chaque nœud du réseau blockchain peut fonctionner de manière autonome, c'est-à-dire qu'il peut valider, enregistrer et transmettre des transactions sans intervention extérieure.
- Cette autonomie renforce la résilience et la fiabilité du système.

5. **Open-source**

- La plupart des blockchains telles que Bitcoin et Ethereum sont open-source, ce qui signifie que leur code est librement accessible.

- Cela favorise l'innovation et la création d'applications décentralisées (Apps). L'ouverture du code rend également les transactions publiquement vérifiables.

6. **Anonymat**

   - Les utilisateurs interagissent avec la blockchain par le biais d'adresses cryptographiques, sans révéler leur véritable identité.
   - Bien que les transactions soient publiques et traçables, l'identité des participants reste protégée, ce qui garantit un certain niveau d'anonymat.
   - Cette caractéristique renforce la confidentialité, tout en garantissant une vérification décentralisée.

d) Développement blockchain : Outils clés et processus

1. **Outils clés**

   (a) **Ganache**
   C'est un outil local de simulation d'une blockchain Ethereum. Il permet de tester et de déployer des smart contrats sans être connecté à un réseau réel. Il est utilisé pour développer et tester des applications blockchain.

   (b) **Solidity**
   C'est un langage de programmation permettant d'écrire des smart contrats sur la blockchain Ethereum. Il peut être utilisé pour automatiser des processus tels que la gestion des transactions ou l'accès aux données sur la blockchain.

   (c) **Web3.Js**
   Il s'agit d'une bibliothèque JavaScript permettant de connecter le front-end (par exemple un site web) à la blockchain Ethereum. Il permet d'interagir avec des contrats intelligents, d'envoyer des transactions et de récupérer des données de la blockchain.

   (d) **Smart contrat**
   Programmes auto-exécutables qui s'exécutent sur la blockchain selon des conditions prédéfinies. Ils automatisent les tâches et garantissent des transactions sécurisées sans intermédiaire.

2. **Processus**

   (a) **Écrire un Smart Contract en Solidity**
   Définir les règles et les actions dans un contrat numérique (par exemple, la gestion des droits d'accès aux données).

   (b) **Tester et déployer avec Ganache**
   Déployer le smart contrat sur une blockchain locale simulée (Ganache) pour effectuer des tests avant de le déployer sur un réseau public ou privé.

(c) **Intégration avec le frontend via Web3.Js**
Utiliser *Web3.js* pour connecter l'application (*Vue.js* par exemple) à la blockchain. Cela permet de récupérer des informations sur les contrats, d'envoyer des transactions ou d'interagir avec les utilisateurs via des portefeuilles tels que Meta Mask.

3.4 Conclusion

Le choix des outils et des technologies pour ce projet assure une plateforme solide et sécurisée pour la gestion des données médicales. Les solutions utilisées pour le développement front-end et back-end, la base de données et la sécurité garantissent la fiabilité et la conformité.

L'intégration de la blockchain renforce la transparence et la sécurité des données, en permettant un contrôle d'accès décentralisé et sécurisé. Ces choix nous ont permis de créer une plateforme fiable et évolutive, adaptée aux exigences du domaine médical.

CHAPITRE 4

RÉALISATION PRATIQUE DE LA PLATEFORME HEALTHSAFE

4.1 Introduction

Ce chapitre présente le fonctionnement pratique de la plateforme de gestion des dossiers médicaux sécurisés, basée sur l'architecture décrite précédemment dans le chapitre 2.

Chaque section illustre le fonctionnement des composants décrits dans l'architecture (chapitre 2) au moyen de captures d'écran réelles de l'interface utilisateur, des principales fonctionnalités de la séquence d'interactions entre les acteurs du système.

4.2 Présentation des différentes interfaces de la plateforme HealthSafe

Dans cette section, nous présentons les différentes interfaces pour mieux exploiter la plateforme HealthSafe.

4.2.1 Interface de connexion de l'administrateur

Cette interface est la page portail de la plate-forme HealthSafe. Elle permet à l'administrateur de se connecter en saisissant son adresse électronique et son mot de passe pour s"authentifier, puis en cliquant sur le bouton "Se connecter", comme le montre la Figure 4.1.

FIG. 4.1 : Interface d'authentification de l'administrateur

4.2.2 Interface de gestion des utilisateurs par l'admin

Après l'authentification de l'administrateur, ce dernier sera connecté pour gérer différentes tâches prodiguées par la plateforme HealthSafe. Ensuite, l'administrateur sera redirigé vers l'interface principale illustrée par la Figure 4.2 pour la gestion des utilisateurs (patients et personnel soignant).

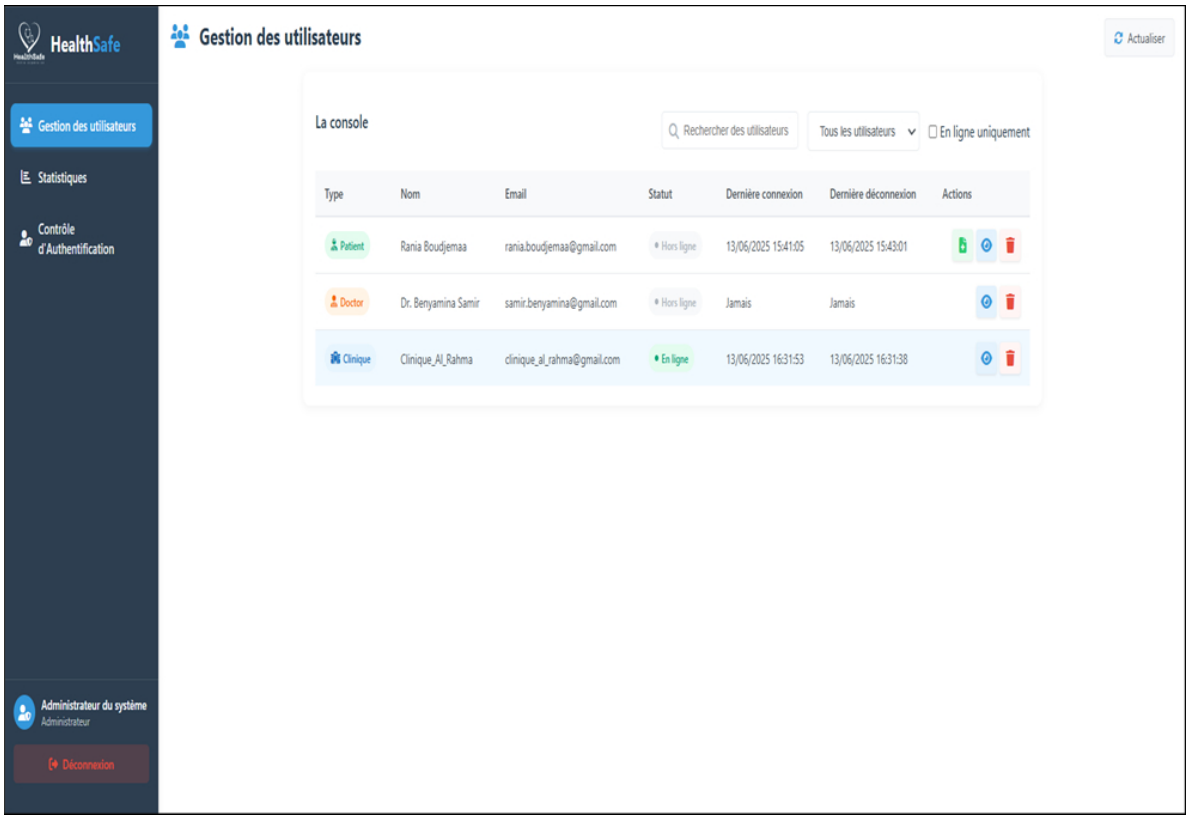


FIG. 4.2 : Interface de gestion des utilisateurs

L'interface de gestion des utilisateurs représente la première page affichée à l'administrateur après sa connexion. Elle lui permet de visualiser la liste des utilisateurs, avec leur statut (actif ou inactif), la date de leur dernière connexion et déconnexion. L'administrateur peut également supprimer un utilisateur ou consulter les dossiers des patients associés.

4.2.3 Interface d'inscription d'un établissement de santé

Cette interface permet aux établissements de santé de s'inscrire sur une plateforme sécurisée en fournissant les informations nécessaires pour :

- Vérifier leur légitimité par une authentification forte
- Configurer les accès des professionnels de santé affiliés.
- Personnaliser les paramètres de conformité (RGPD, HIPAA).

Dans cette interface, l'utilisateur "clinique" doit remplir le formulaire présenté dans l'interface comme montre la Figure 4.3, puis cliquer sur le bouton *"Inscription"* pour envoyer une demande d'inscription à l'administrateur, qui devra la valider si ce dernier accepte son inscription.

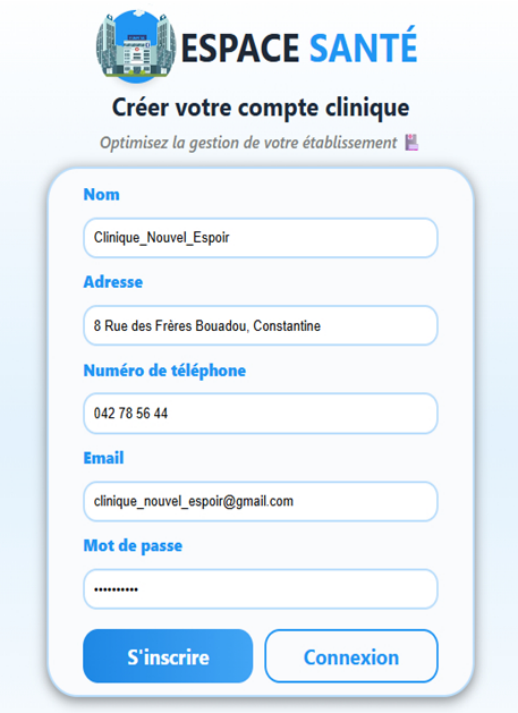


FIG. 4.3 : Interface d'inscription d'un établissement de santé (ex. clinique)

4.2.4 Interface d'inscription d'un patient

L'interface d'inscription d'un patient permet aux patients de s'inscrire de manière sécurisée et intuitive sur une plateforme médicale (ex : cabinet en ligne, hôpital), tout en :

- Vérifiant leur identité (pour éviter les fraudes).
- Respectant les normes de confidentialité (RGPD, HIPAA).
- Personnalisant leur profil médical (antécédents, etc.).

Dans cette interface le patient est invité à saisir ses données via un formulaire comme montre la Figure 4.4 puis il clique sur le bouton *"Inscription"* pour une demande d'inscription à l'administrateur et ce dernier validera cette demande dans l'affirmative.

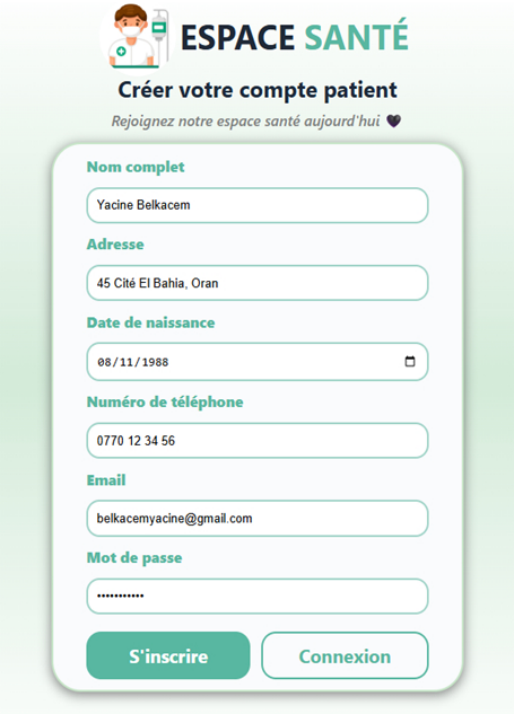


FIG. 4.4 : Interface d'inscription d'un patient

4.2.5 Interface de contrôle d'authentification et des demandes

Dans cette interface présentée par la figure 4.5, l'administrateur peut consulter les demandes d'inscription et les accepter ou les refuser. Ces deux cas sont illustrés dans les figures 4.6a et 4.6b.

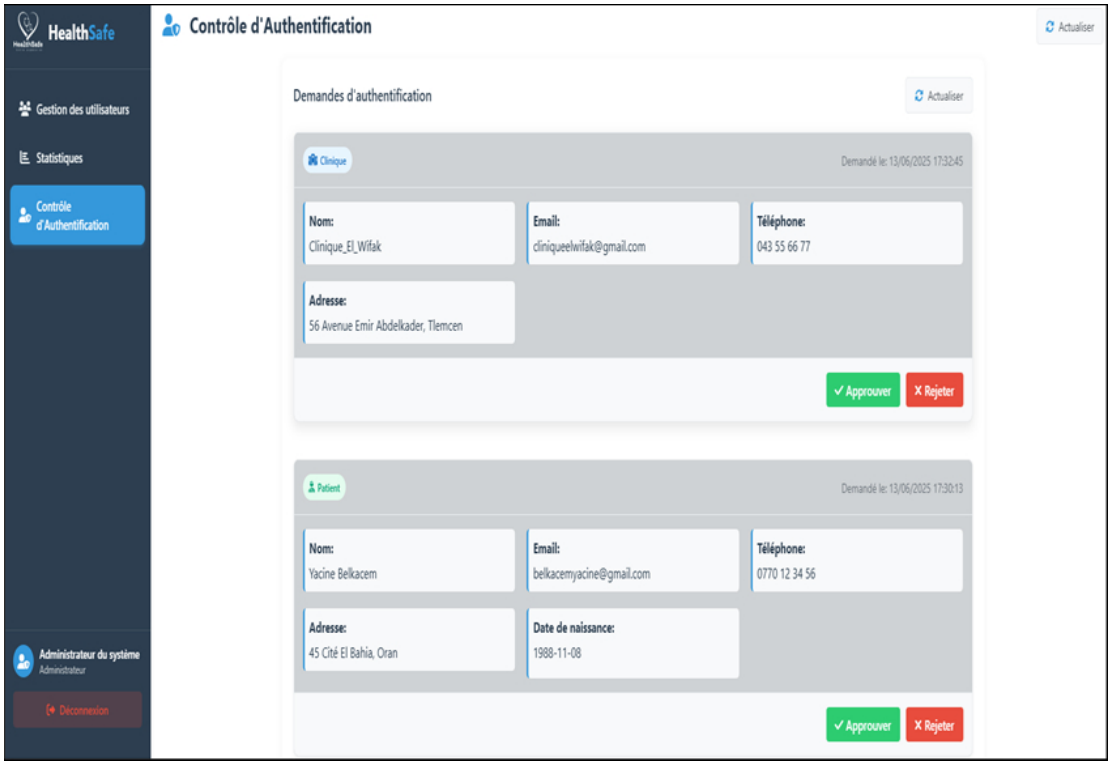
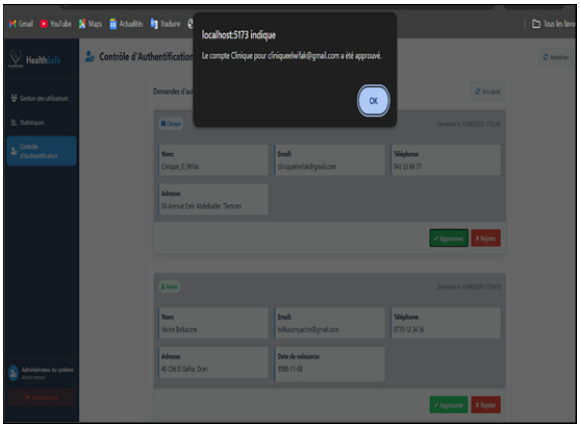
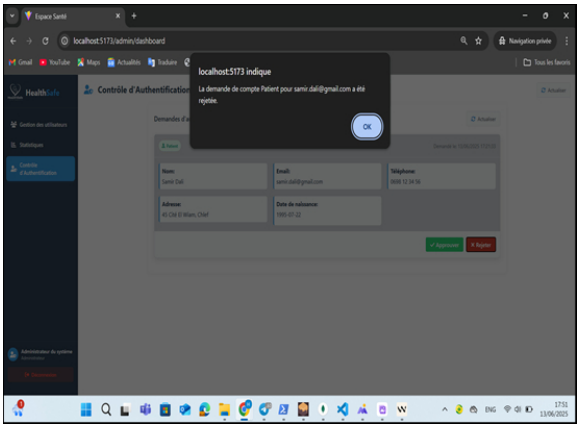


FIG. 4.5 : Interface de contrôle d'authentification des utilisateurs



(a) Alerte d'acceptation d'une demande pour un établissement de santé

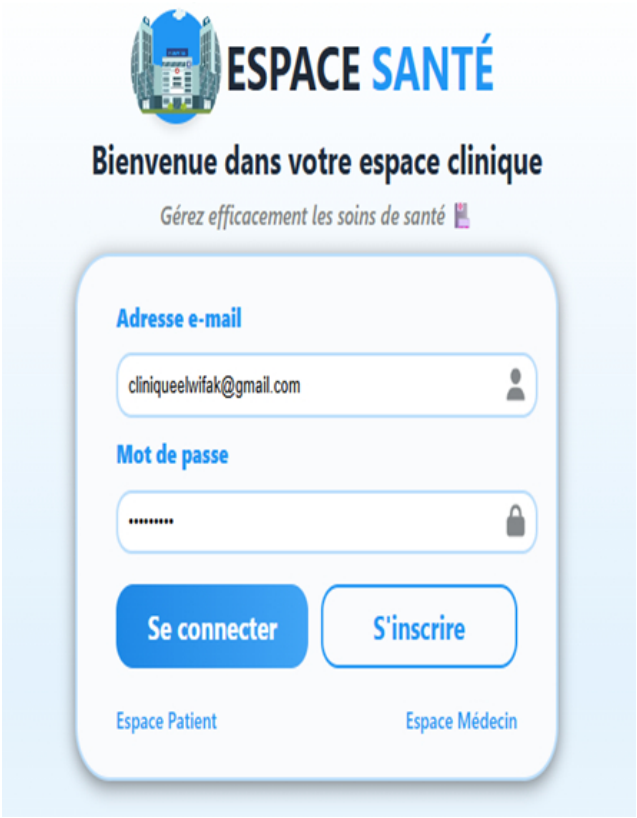


(b) Alerte de refus d'une demande pour un patient

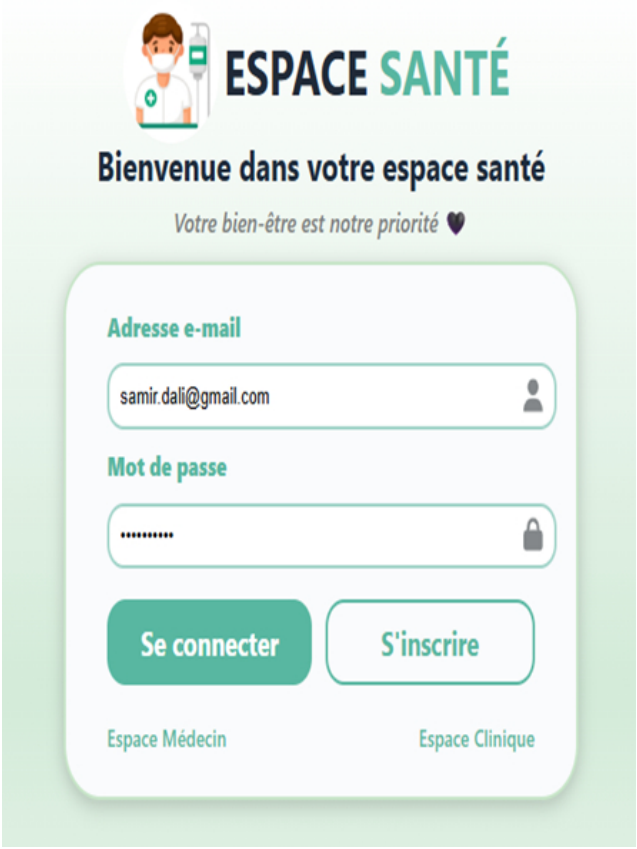
FIG. 4.6 : Interfaces de réponse à une demande d'inscription d'un utilisateur

4.2.6 Interface de connexion des utilisateurs

Les interfaces présentées par les Figures 4.7a et 4.7b permettent aux patients et au personnel médical de se connecter. Si leur demande a été rejetée par l'administrateur, une alerte s'affiche pour les en informer (voir Figure 4.8) et dans le cas contraire, ils accèdent directement à leur espace personnel (voir Figures 4.9 et 4.10).



(a) Interface de connexion d'un établissement de santé



(b) Interface de connexion d'un patient

FIG. 4.7 : Interfaces de connexion des utilisateurs

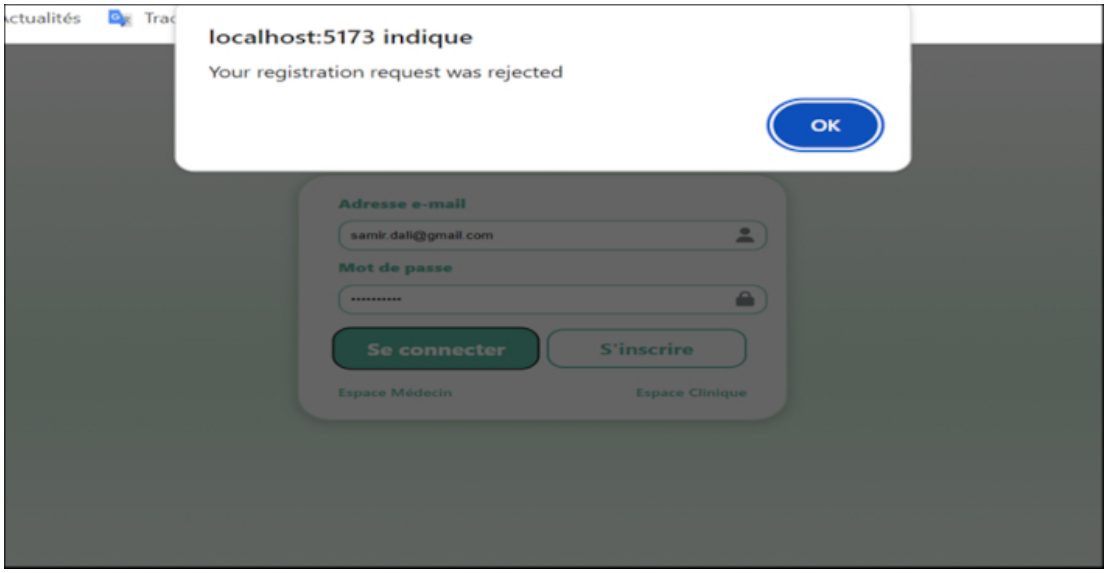


FIG. 4.8 : Alerte de contrôle d'authentification des utilisateurs

4.2.7 Interface de l'espace "établissement de santé"

Interface du personnel médical

L'interface représentée par la Figure 4.9 permet d'afficher la liste du personnel médical de l'établissement de santé. Elle permet de modifier les données concernant un personnel médical, supprimer ou ajouter un personnel médical.

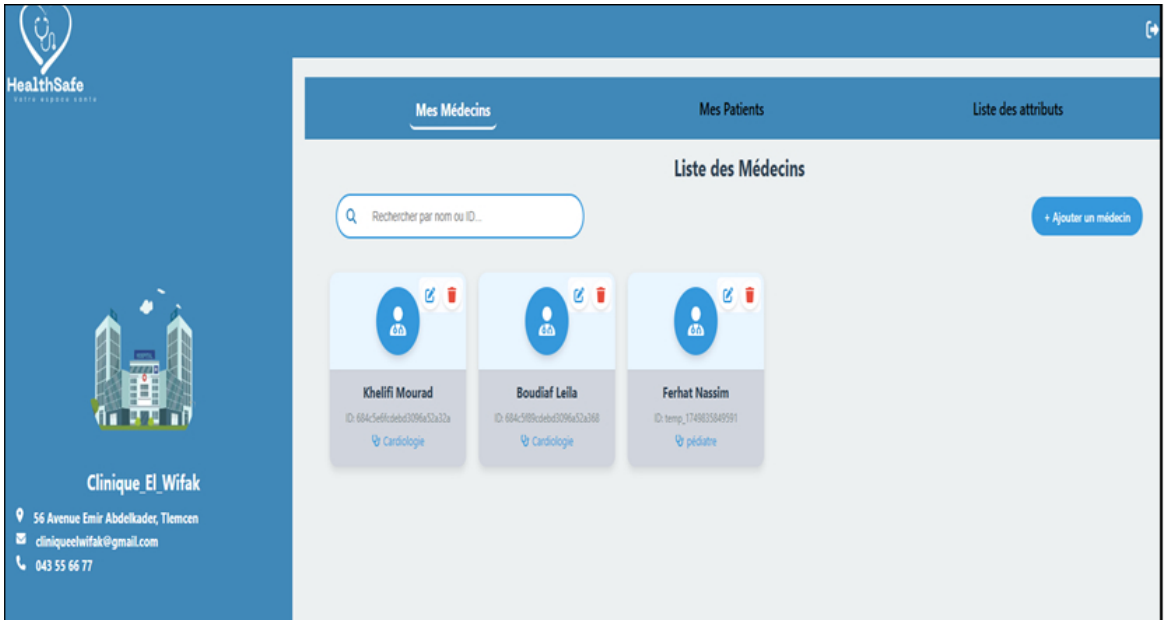


FIG. 4.9 : Interface de mes médecins

4.2.8 Interface de l'espace patient

Interface de mes dossiers

L'interface de l'espace médecin représentée par la Figure 4.10 est la première interface affichée au patient après son authentification. Elle présente la liste de ses dossiers médicaux et offre la possibilité d'en ajouter de nouveaux depuis son appareil en cliquant sur le bouton *"Ajouter un dossier"*.

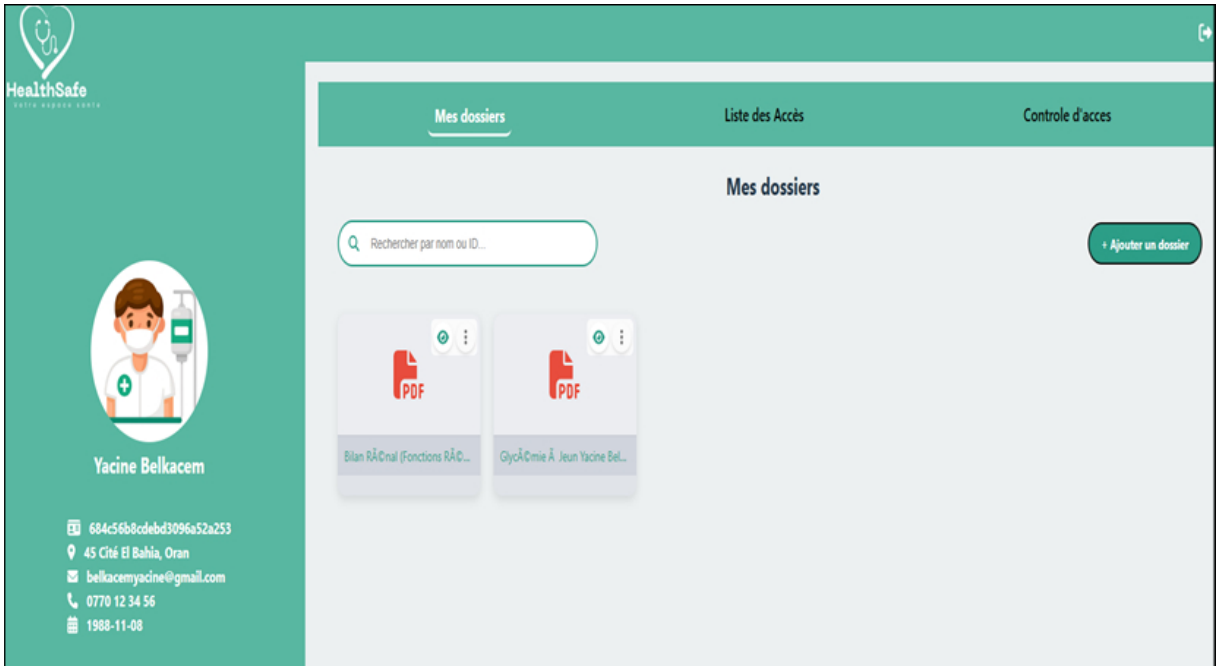


FIG. 4.10 : Interface de mes dossiers concernant un patient

4.2.9 Interface de contrôle d'accès

Lorsqu'un patient clique sur le bouton *"Créer une règle"*, l'interface présentée par la Figure 4.11 s'affiche. À ce niveau, il peut choisir la clinique en cliquant sur *"Cliniques"* et la spécialité en cliquant sur *"Spécialité"* du médecin à qui il souhaite accorder l'accès. Il doit également respecter le format requis. Une fois cliquer sur le bouton *"Générer les clés d'accès"*, il est redirigé vers l'interface présentée par la Figure 4.12.

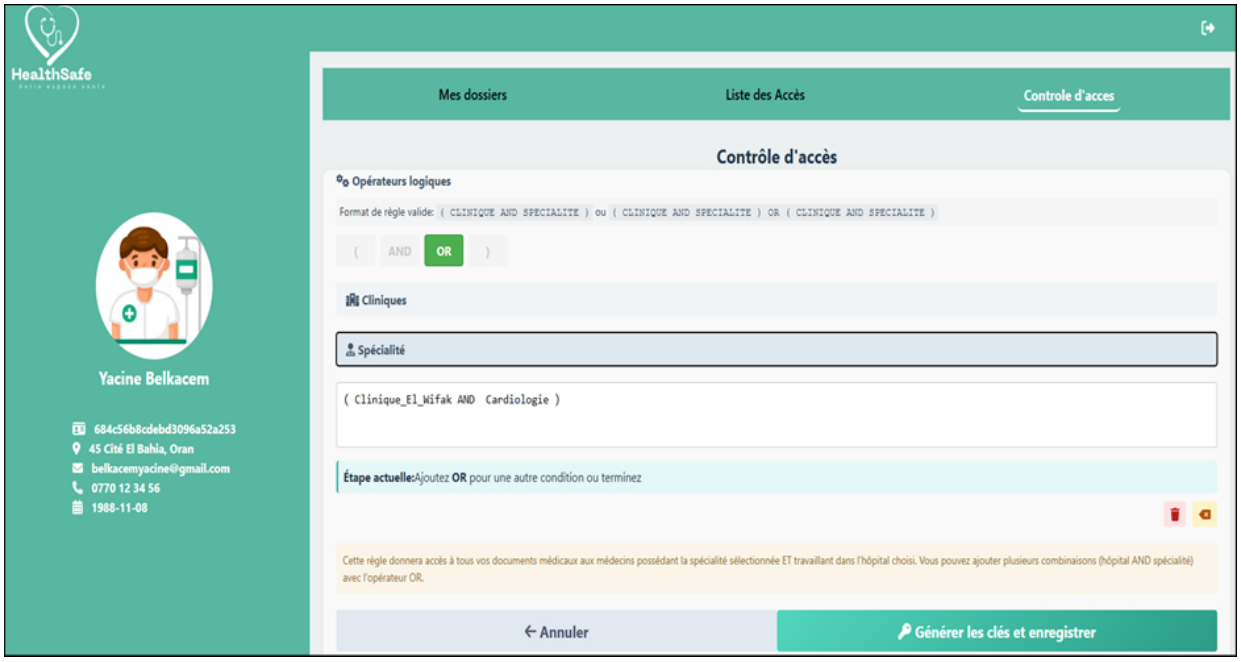


FIG. 4.11 : Interface de contrôle d'accès

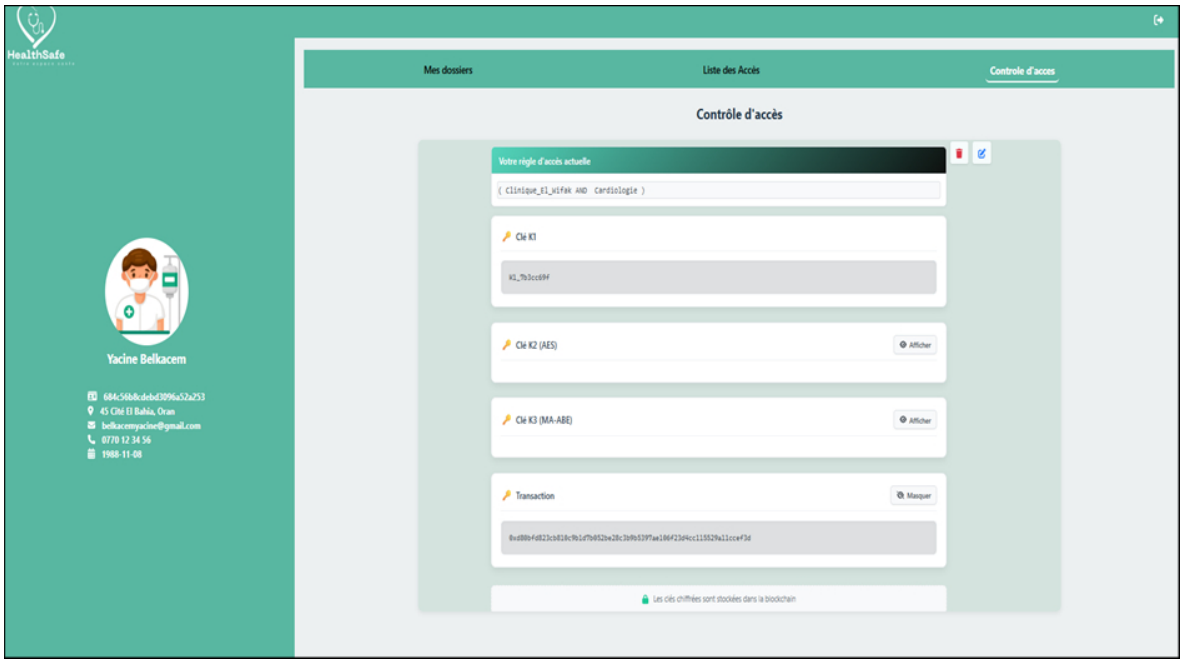
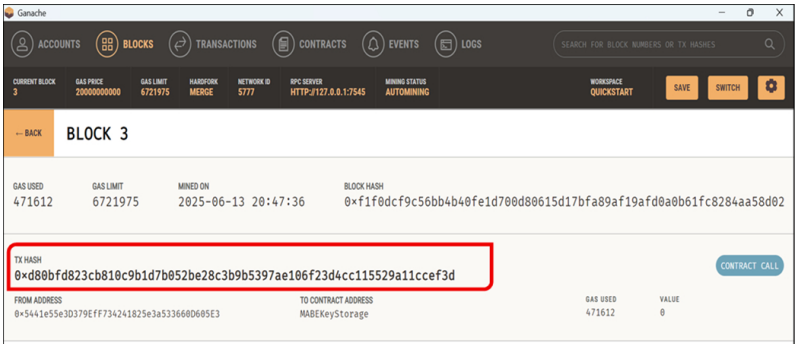
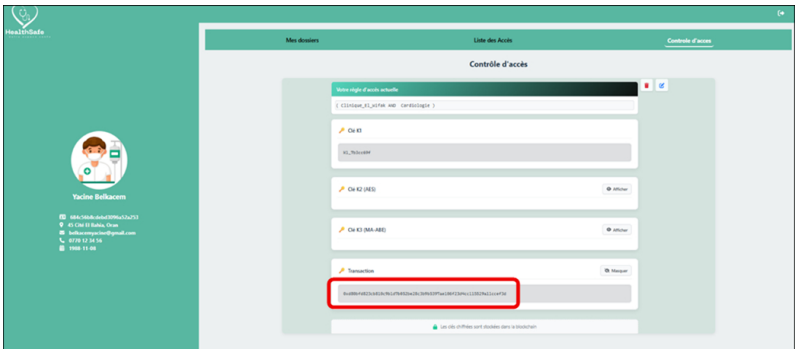


FIG. 4.12 : Interface de génération de clés et transaction

Nous avons utilisé une blockchain avec Ganache qui est un environnement de développement local pour Ethereum pour stocker les clés des patients générées par MA-ABE. L'interface de Ganache (Figure 4.13a) montre que le bloc a bien été créé, contenant la transaction dans laquelle les clés ont été stockées (Figure 4.13b).



(a) Interface représente la transaction sur Ganache



(b) Interface représente la transaction sur web

FIG. 4.13 : Interface de la transaction sur Ganache et sur le web

4.2.10 Interface des listes des accès

L'interface présentée par la Figure 4.14 permet d'afficher la liste des établissements de santé mentionnés dans la règle d'accès, ainsi que les spécialités et les noms des médecins ayant les droits d'accès.

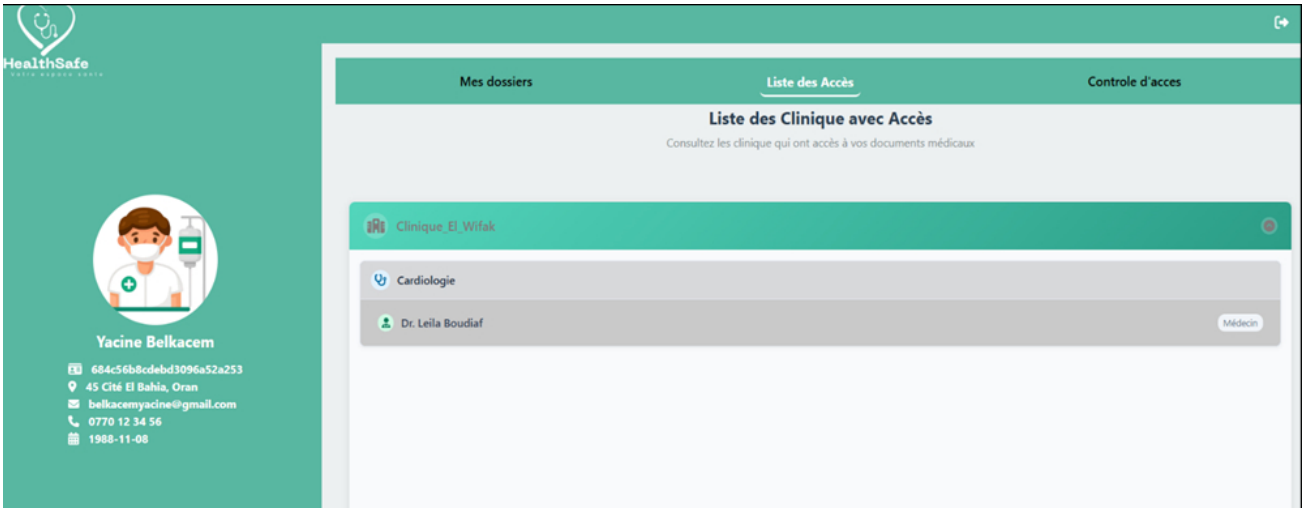


FIG. 4.14 : Interface de la liste des accès

4.2.11 Interface de mes patients dans l'espace "établissement de santé"

La Figure 4.15 représente l'interface dédiée à l'établissement de santé. Elle permet à l'établissement de santé de consulter la liste des patients ayant accordé l'accès au personnel médical.

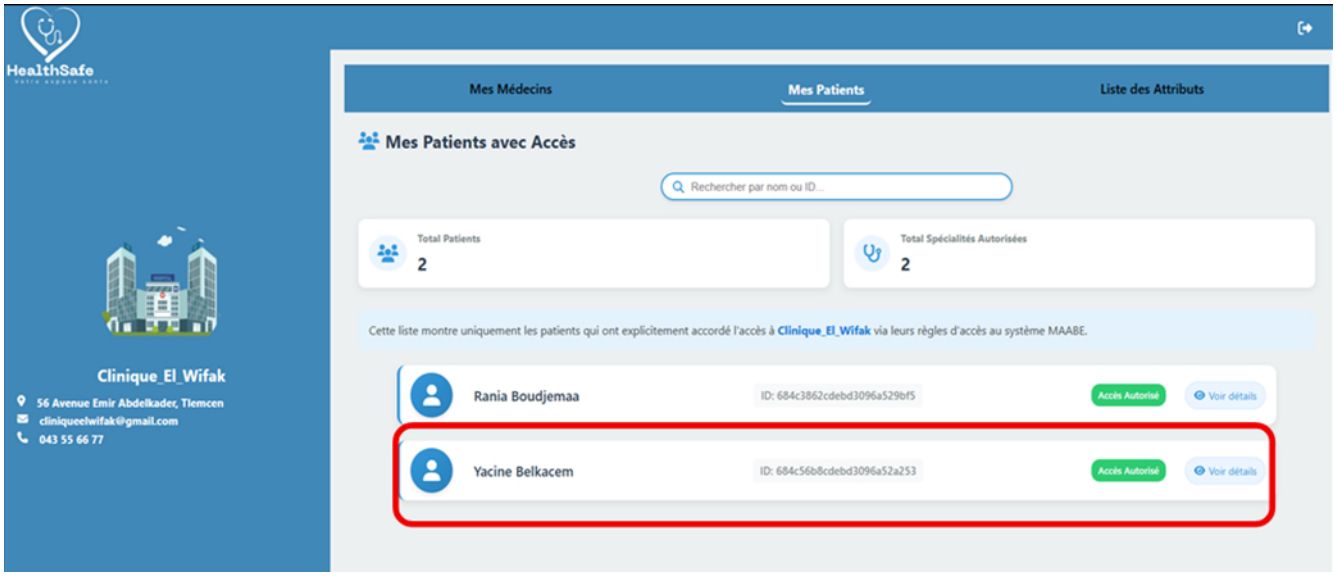


FIG. 4.15 : Interface de mes patients dans l'espace clinique

4.2.12 Interface de connexion du personnel médical

La Figure 4.16 représente l'interface de connexion d'un personnel médical. Si l'authentication est réussie le personnel médical se redirige vers son espace.

FIG. 4.16 : Interface de connexion d'un personnel médical

4.2.13 Interface de l'espace "personnel médical"

Il s'agit de l'interface affichée au personnel médical pour consulter les dossiers. Il doit d'abord saisir l'ID du patient, puis cliquer sur le bouton *"Vérifier l'accès"*, ensuite sur le bouton *"Déchiffrer"*. En cas d'accès autorisé, lorsque le personnel médical clique sur le bouton *"Déchiffrer"*, les dossiers du patient correspondant à l'identifiant saisi s'affichent.

La Figure 4.17 illustre un accès réussi par un personnel médical au dossier d'un patient. Néanmoins, si le personnel médical n'a pas les droits d'accès, une alerte s'affiche pour lui indiquer qu'il n'est pas autorisé à consulter les dossiers de ce patient comme montre la Figure 4.18.

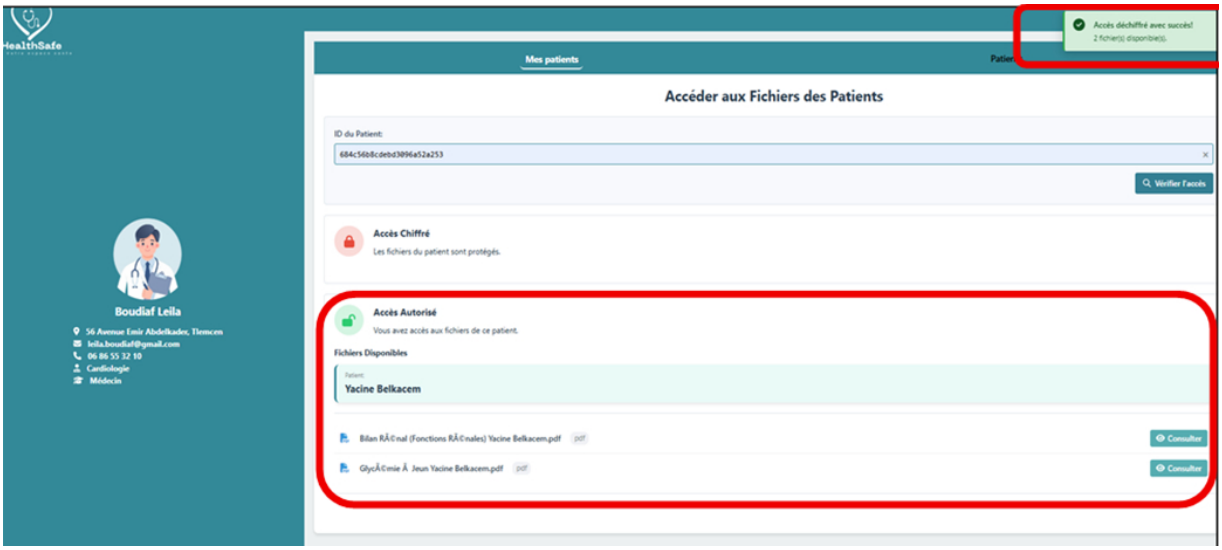


FIG. 4.17 : Interface d'un médecin qui a l'accès

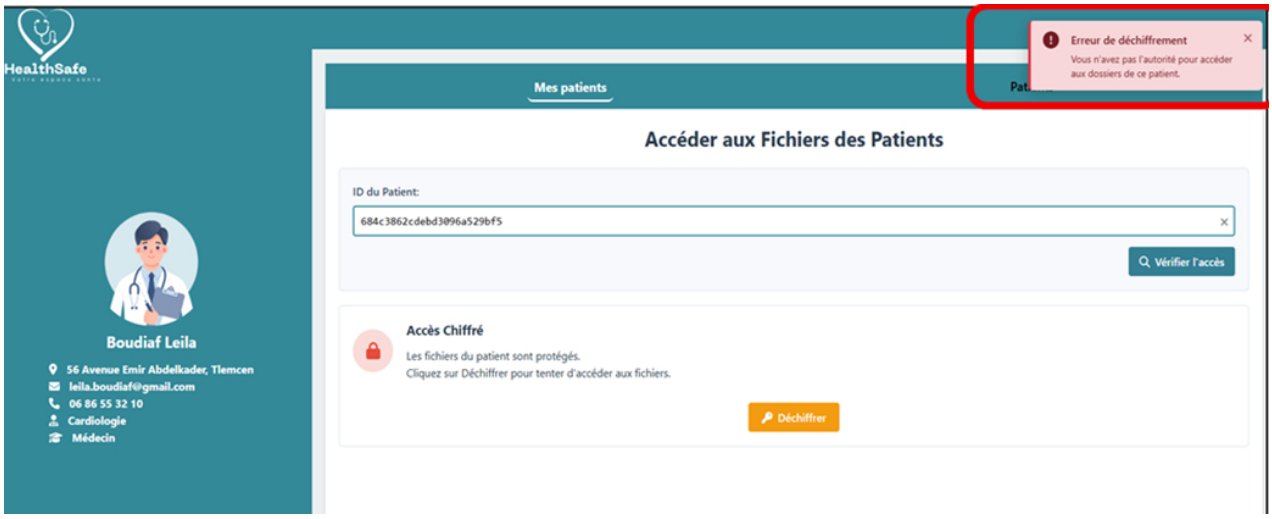


FIG. 4.18 : Interface d'un médecin qui n'a pas un accès

4.3 Conclusion

Ce prototype illustre la faisabilité d'un système sécurisé de gestion des données médicales, combinant le chiffrement AES, le contrôle d'accès par attributs (MA-ABE), le stockage dans le cloud et la traçabilité via blockchain. Ainsi, grâce aux mécanismes mis en œuvre, seuls les utilisateurs autorisés peuvent consulter les dossiers médicaux.

.

CONCLUSION GÉNÉRALE

À travers ce projet de fin d'études, nous avons tenté de proposer une solution technologique adaptée aux besoins actuels du domaine médical en matière de gestion sécurisée des données. Nous avons étudié les principaux aspects de la sécurité des systèmes d'information, analysé les menaces et les normes, puis conçu une architecture complète basée sur des technologies modernes comme le cloud et la blockchain.

Le développement de notre plateforme (HealthSafe) a montré qu'il est possible de renforcer la sécurité et la transparence dans la gestion des données médicales, tout en facilitant l'accès aux informations pour les patients et le personnel médical. L'intégration des mécanismes de sécurité, combinée à l'usage de la blockchain, permet d'assurer un meilleur contrôle d'accès, une traçabilité fiable, et une protection renforcée contre les risques.

Ce projet nous a permis de mettre en pratique nos connaissances techniques et d'acquérir une expérience concrète en conception et développement d'applications sécurisées. Bien que ce travail reste une base, il peut être amélioré et élargi par la suite pour intégrer encore plus de fonctionnalités et répondre à d'autres besoins spécifiques du secteur de la santé.

En conclusion, cette plateforme représente une démarche prometteuse vers une gestion numérique plus sûre et plus efficace des données médicales, dans un monde de plus en plus connecté.

BIBLIOGRAPHIE

BIBLIOGRAPHIE

[1] ISO/CEI 27001 :2013(FR). *Technologies de l'information — Techniques de sécurité — Code de bonne pratique pour le management de la sécurité de l'information*. Last access : 2025-05-17. 2013. URL : https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:fr.

[2] Bruce SCHNEIER. *Applied Cryptography : Protocols, Algorithms, and Source Code in C*. John Wiley & Sons Inc, 1996.

[3] NitinKumar SHINGARI et Beenu MAGO. "The Importance of Data Encryption in Ensuring the Confidentiality and Security of Financial Records of Medical Health". In : *Proceedings of IEEE International Conference on Interdisciplinary Approaches in Technology and Management for Social Innovation (IATMSI)*. T. 2. IEEE. Gwalior, India, 2024, p. 1-6. DOI : 10.1109/IATMSI60426.2024.10503174.

[4] Stallings WILLIAM. *Cryptography and Network Security : Principles and Practice*. Pearson, 2016.

[5] CNIL. *La gestion des droits d'accès aux données de santé*. Last access : 2025-05-17. 2023. URL : https://cnil.fr.

[6] U.S. Department of HEALTH & HUMAN SERVICES (HHS). *Health Insurance Portability and Accountability Act Security Rule*. Last access : 2025-05-17. 2022. URL : https://www.hhs.gov/.

[7] Erika Magonara Apostolos Malatras Rossen Svetozarov Naydenov Cosmin Ciobanu Georgios Chatzichristos IFIGENEIA LELLA Marianthi Theocharidou. *ENISA THREAT LANDSCAPE*. Rapp. tech. EUROPEAN UNION AGENCY FOR CYBERSECURITY, 2024.

[8] Agence du Numérique en SANTÉ. *Certification des Hébergeurs de Données de Santé (HDS)*. Last access : 2025-05-17. 2023. URL : https://esante.gouv.fr/labels-certifications/hds/certification-des-hebergeurs-de-donnees-de-sante.

[9] Kaspersky. *Cyberattack on Healthcare : How to Protect Your Systems*. Last access : 2025-05-17. 2021. URL : https://www.kaspersky.com.

[10] IBM Team. *Cost of a Data Breach Report*. Rapp. tech. IBM, 2024.

[11] IBM Security Team. *Cost of a Data Breach Report 2021*. Rapp. tech. Ponemon Institute, 2021.

[12] Extencia Team. *Resolver RAT : une menace pour les pharmaciens et médecins*. Last access : 2025-05-17. 2024. URL : https://www.extencia.fr/resolver-rat-protection-pharmaciens-medecins.

[13] WHO (World Health Organization). *Digital health and cybersecurity in healthcare*. Last access : 2025-05-17. 2020. URL : https://www.who.int.

[14] Thomas L. Norman. "Chapter 2 - Foundational Security and Access Control Concepts". In : *Electronic Access Control (Second Edition)*. Sous la dir. de Thomas L. Norman. Second Edition. Butterworth-Heinemann, 2017, p. 21-42. ISBN : 978-0-12-805465-9. DOI : https://doi.org/10.1016/B978-0-12-805465-9.00002-6. URL : https://www.sciencedirect.com/science/article/pii/B9780128054659000026.

[15] Sabrina De Capitani di Vimercati. "Discretionary Access Control Policies (DAC)". In : *Encyclopedia of Cryptography and Security*. Sous la dir. d'Henk C. A. van Tilborg et Sushil Jajodia. Boston, MA : Springer US, 2011, p. 356-358. DOI : 10.1007/978-1-4419-5906-5_817. URL : https://doi.org/10.1007/978-1-4419-5906-5_817.

[16] Bhavani Thuraisingham. "Mandatory Access Control". In : *Encyclopedia of Database Systems*. Sous la dir. de LING LIU et M. TAMER ÖZSU. Boston, MA : Springer US, 2009, p. 1684-1685. ISBN : 978-0-387-39940-9. DOI : 10.1007/978-0-387-39940-9_214. URL : https://doi.org/10.1007/978-0-387-39940-9_214.

[17] Ravi S. Sandhu. "Role-based Access Control". In : sous la dir. de Marvin V. Zelkowitz. T. 46. Advances in Computers. Elsevier, 1998, p. 237-286. DOI : https://doi.org/10.1016/S0065-2458(08)60206-5. URL : https://www.sciencedirect.com/science/article/pii/S0065245808602065.

[18] Vincent C. Hu et al. "Attribute-Based Access Control". In : *Computer* 48.2 (2015), p. 85-88. DOI : 10.1109/MC.2015.33.

[19] Melissa Chase. "Multi-authority Attribute Based Encryption". In : *Theory of Cryptography*. Sous la dir. de Salil P. Vadhan. Berlin, Heidelberg : Springer Berlin Heidelberg, 2007, p. 515-534.

[20] CHUM Team. *Transformation numérique en santé : enjeux et meilleures pratiques*. Rapp. tech. Centre hospitalier de l'Université de Montréal, 2023.

[21] CEI Team. *Logiciel de matériel logiciel – processus du cycle de vie du logiciel*. Rapp. tech. Commission électrotechnique internationale, 2015.

[22] S. Chacon et B. Straub. *Git : Distributed-is-the-new-centralized*. Last access : 2025-05-17. 2023. URL : https://git-scm.com/book/en/v2.

[23] Vue JS Team. *The Progressive JavaScript Framework*. Last access : 2025-05-17. URL : https://vuejs.org/.

[24] HTML Teamm. *HTML*. Last access : 2025-05-17. 2007. URL : http://glossaire.infowebmaster.fr/html/.

[25] CSS Tricks. *Astuces et bonnes pratiques CSS*. Last access : 2025-05-10. 2007. URL : https://css-tricks.com/.

[26] NIST Team. *Advanced Encryption Standard (AES)*. Rapp. tech. National Institute of Standards et Technolog (NIST), 2001.

[27] Vipul Goyal et al. "Attribute-based encryption for fine-grained access control of encrypted data". In : *Proceedings of the 13th ACM Conference on Computer and Communications Security*. CCS '06. Alexandria, Virginia, USA : Association for Computing Machinery, 2006, p. 89–98. DOI : 10.1145/1180405.1180418.

[28] Jean-Paul Delahaye. *Les blockchains, clefs d'un nouveau monde*. Last access : 2025-05-10. 2015. URL : https://www.pourlascience.fr/sd/informatique/les-blockchains-clefs-daposun-nouveau-monde-8354.php.

[29] Laurent Leloup. *Blockchain : La révolution de la confiance*. Eyrolles, 2017.

[30] SME Portal. *Blockchain sharing*. Last access : 10-10-2022. 2022. URL : https://www.kmu.admin.ch/kmu/en/home/facts-and-trends/blockchain.html.

Business Model Canvas (BMC)

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université Abou Bekr Belkaid Tlemcen

Business Model Canvas

BMC

N° de projet : 29

Faculté/Institut : Faculté des sciences

Département : Informatique

Nom du projet : HealthSafe

Thème : Etude et conception d'une plateforme sécurisée de gestion des données médicales des patients dans une clinique

Encadrant 1: LEHSAINI Mohamed

Co-encadrant 1: FEHAM Mohammed

Co-encadrant 2 : DEGDEG Hicham

Etudiantes : - MEGREZ RAYHANE

- HASNAOUI NOUR EL HOUDA

Année universitaire : 2024/2025

1- Proposition de valeur (Value Proposition)القيمة المقترحة

a. Quels problèmes résolvons-nous pour nos clients ?

ما هي المشاكل التي نحلها لعملائنا ؟

Nous répondons à plusieurs problèmes critiques rencontrés dans la gestion des données médicales au sein des cliniques et établissements de santé :

1. **Risque élevé de fuite de données sensibles**, en raison d'un manque de sécurité dans le stockage, l'accès ou le partage des dossiers médicaux.
2. **Non-conformité aux réglementations en vigueur** (RGPD, HIPAA…), exposant la structure à des sanctions juridiques et financières.
3. **Absence de traçabilité fiable :** il est difficile de savoir précisément qui a consulté ou modifié les données, quand et pourquoi.
4. **Manque de confiance des patients** concernant la protection et la confidentialité de leurs informations personnelles.
5. **Risque de perte de données médicales importantes**, notamment en cas de panne, d'attaque ou d'erreur humaine, faute de système de sauvegarde efficace.
6. **Failles dans la gestion des accès :** le personnel peut accéder à des dossiers sans contrôle ni restriction claire, ce qui compromet la confidentialité.
7. **Manque de transparence et d'intégrité** dans la gestion des dossiers médicaux, avec des modifications ou consultations non tracées.

b. Quels besoins de nos clients satisfont nos produits ou services ?

ما هي الاحتياجات التي يلبيها منتجاتنا أو خدماتنا لعملائنا؟

Notre solution répond aux besoins fondamentaux des cliniques, des professionnels de santé et des patients :

1. **Besoin de sécurité des données médicales :** garantir la protection contre les accès non autorisés, les fuites ou les pertes.
2. **Besoin de conformité réglementaire :** assurer le respect des lois nationales et internationales sur la protection des données.
3. **Besoin de traçabilité et de transparence :** pouvoir suivre avec précision toutes les opérations effectuées sur les dossiers médicaux.
4. **Besoin d'un contrôle d'accès structuré :** limiter l'accès aux informations sensibles selon des niveaux d'autorisation bien définis.
5. **Besoin de continuité de service :** garantir l'accès aux données à tout moment, même en cas de problème technique.
6. **Besoin de confiance numérique :** rassurer les patients sur la confidentialité et l'intégrité de leurs informations.
7. **Besoin d'évolutivité et de modernisation :** adopter une solution adaptée à l'évolution du secteur de la santé numérique.

c. En quoi notre offre est-elle différente de celle de nos concurrents ?
في ماذا تختلف عروضنا عن تلك التي يقدمها منافسونا؟

1. **Sécurité renforcée :** chiffrement avancé + gestion fine des accès.
2. **Adaptée au contexte local :** pensée pour les besoins des cliniques algériennes.
3. **Traçabilité complète :** chaque accès ou modification est enregistré.
4. **Conformité réglementaire :** respect des lois comme RGPD / HIPAA.
5. **Interface simple et intuitive :** facile à utiliser même sans expertise technique.
6. **Approche tout-en-un :** intégration unique de sécurité, conformité et gestion des droits.

d. Quelles est notre proposition unique de valeur ?
ما هو العرض الفريد للقيمة لدينا؟

Notre proposition unique de valeur réside dans une plateforme de gestion des données médicales qui garantit un haut niveau de sécurité, de traçabilité et de contrôle d'accès, tout en restant simple à utiliser.

Contrairement aux solutions classiques, notre approche intègre des mécanismes avancés de protection des données et de gestion des accès, adaptés aux exigences locales et internationales. Cette combinaison stratégique fait de notre solution une offre rare et innovante sur le marché algérien.

2- Segments de clients (Customer Segment) انواع العملاء :

a. Quels sont nos clients principaux ?
من هم العملاء او الزبائن الرئيسيون؟

Les cliniques privées, les cabinets médicaux et les médecins spécialistes qui ont besoin d'une solution fiable pour protéger, organiser et gérer les dossiers médicaux de leurs patients, tout en respectant les réglementations. Elles sont les premières à adopter des solutions digitales en Algérie (flexibilité et besoin de différenciation).

-**Exemple** : Les cliniques dentaires ou ophtalmologiques à Alger or Oran, qui sont des pays industrialisés à moderniser leur gestion.

b. Quels sont les différents segments de clients que nous visons ?
ما هي الفئات المختلفة من العملاء التي تستهدفها؟

En plus des cliniques privées, nous visons :

- ✓ **Les hôpitaux :** parce que les CHU (Centres Hospitalo-Universitaires) et hôpitaux publics ciblés sont par autoritaires les réformes (ex: digitalisation des dossiers patients).

- ✓ **Les organismes de régulation ou d'assurance santé :** parce que Le ministère de la santé et de la CNAS (Caisse Nationale des Assurances Sociales) qui est à la validité de la conformité de votre solution (RGPD local, hébergement des visas).

- ✓ Les centres de diagnostic et laboratoires d'analyses médicales : Clients stratégiques en Algérie (ex: Bio24, Cerballiance), avec des besoins en stockage de contrats de sécurité.

- ✓ Assurances santé : Ex : Dar El Amal, MACIF, qui ont besoin d'indice aux visas pour le remboursement des soins.

c. Quels sont les besoins spécifiques de chaque segment de clients ?
ما هي الاحتياجات الخاصة لكل فئة من العملاء؟

1) **Cliniques privées, cabinets médicaux et médecins :** Besoins : Solution fiable pour les protéger, organisateur et gérer les dossiers médicaux des patients, tout en respectant les réglementations (RGPD, HDS). Elles sont les premières à adopter des solutions digitales en Algérie, avec un besoin de flexibilité et de différenciation.

2) **Hôpitaux :** Besoins : Numérisation des dossiers patients et standardisation des systèmes d'information. Les CHU (Centres Hospitalo-Universitaires) et HOHRC publics des hôpitaux ciblés sont par les against the autoritaires.

3) **Organismes de régulation et d'assurance santé :** Besoins : Validation de la conformité de la solution (RGPD local, hébergement des données). Le ministère de la Santé et de la CNAS (Caisse Nationale des Assurances Sociales) un rôle clé dans le processus.

4) **Centres de diagnostic et laboratoires d'analyses médicales :** Besoins : Stockage sécurisé des données et protection des informations sensibles. Clients stratégiques en Algérie (ex : Bio24, Cerballiance) avec des spécifiques revendications en matière de sécurité des données.

5) **Assurances santé :** Besoins : Accès aux données pour le remboursement des soins, pour les exigences de transparence et de conformité. Exemples : Dar El Amal, MACIF, qui des POP index pour le traitement des remboursements.

d. Comment pouvons-nous catégoriser nos clients en groupes distincts ?
كيف يمكن تصنيف عملائنا الى مجموعات مختلفة؟

- ❖ **Leur structure :** cliniques privées, hôpitaux, laboratoires, centres de diagnostic, institutions publiques de santé.
- ❖ **Leur rôle :** médecins généralistes et spécialistes, responsables informatiques, administrateurs, chercheurs, développeurs e-santé.

- **Leur besoin principal :** sécurisation des données médicales, conformité aux normes (RGPD, HIPAA…), gestion fine des accès, intégration de solutions technologiques (API, Blockchain, MA-ABE).

3- Relation avec les clients (Consumer Relationships) علاقة مع العملاء :

a. Quel type de relation chaque segment de clients attend il de nous ?
اي نوع من العلاقة يتوقعه كل فئة من العملاء منا؟

- **Les cliniques et les médecins :** Ils attendent de la confiance, la protection des données et un support technique continu.
- **Les hôpitaux et les institutions :** Ils privilégient la conformité légale et une communication officielle.
- **Les développeurs :** Ils ont besoin d'une documentation technique claire et d'une facilité d'intégration avec le système (via API).
- **Les autorités de régulation :** Ils attendent de la transparence, des rapports de sécurité et une conformité aux normes.

b. Comment entretenons-nous actuellement les relations avec nos clients ?
كيف نحافظ حاليًا على العلاقات مع عملائنا؟

- Nous offrons un support technique à distance (email, ...).
- Nous envoyons des mises à jour régulières du système.
- Nous disposons d'un guide d'utilisation détaillé.
- Nous restons en contact via des newsletters ou des réunions périodiques.

c. Comment pouvons-nous améliorer ou personnaliser nos interactions avec nos clients ?
كيف يمكننا تحسين أو تخصيص تفاعلاتنا مع عملائنا؟

- Intégrer un tableau de support dédié directement dans la plateforme.
- Proposer des formations personnalisées selon le profil du client (ex. : médecin, développeur).
- Mettre en place un système d'évaluation et de retours en temps réel.
- Ajouter des vidéos tutoriels courtes intégrées à l'interface pour guider les utilisateurs.

4-Canaux de distribution (Channels) قنوات التوزيع :

a- Par quels canaux nos clients veulent-ils être atteints ?
من خلال أي قنوات يفضل عملاؤنا أن يتم التواصل معهم؟

Cliniques et médecins : Email, WhatsApp (très utilisé en Algérie),téléphone, support direct via chat en ligne pour des réponses rapides.
Hôpitaux et institutions publiques : Courriel professionnel, consultations formelles, plateformes gouvernementales (ex: portails de la CNAS).

Centres de diagnostic et Laboratoires : Appels dirige (commerciaux dédiés), webinaires techniques, intégration via API.
Assurances Santé : Plateformes sécurisées (extranet), réunions, rapports sur les calculs**.**
Autorités de régulation : Rapports officiels (PDF signé), audits en présentiel, ateliers de conformité RGPD/HDS.

b- Quels canaux sont les plus efficaces pour atteindre chaque segment de clients ?
ما هي القنوات الأكثر فعالية للوصول إلى كل فئة من العملاء؟

- **Cliniques et médecins :** Email et téléphone pour une réponse rapide et efficace, WhatsApp et notifications SMS
- **Hôpitaux et institutions publiques :** Email et réunions formellesen présentiel et plateformes gouvernementales.
- **Laboratoires :** Technique de support dédiée (téléphone/courrier électronique) et intégration API.
- **Assurances Santé :** Extranet, consultations sécurisées et trimestrielles.
- **Autorités de régulation :** Email ,audits hybrides (présentiel et digital) et rapports mensuels automatisés.

c- Comment pouvons-nous intégrer différents canaux pour améliorer l'expérience clients ?
كيف يمكننا دمج مختلف القنوات لتحسين تجربة العملاء؟

- Centraliser le support client avec un système unique qui permet de suivre toutes les demandes via email, chat, et téléphone.
- **Notifications automatiques :** via email ou SMS pour tenir les clients informés des mises à jour système, des nouveaux standards ou de la disponibilité des services.
- Plateforme d'intégration API dédiée aux développeurs, afin de garantir l'accès et la gestion des données en toute sécurité.
- Suivi personnalisé et CRM : Permettre une gestion ciblée des relations avec chaque segment pour proposer des services ou des informations adaptées (par exemple, notifications de conformité ou de mise à jour de sécurité pour les hôpitaux).

5-Partenaires clés (Key Partnerships) : الشراكة الرئيسية

a. Qui sont nos partenaires clés ?
من هم شركاؤنا الرئيسيون؟

A. **Fournisseurs de technologie :** Entreprises spécialisées en blockchain et en cryptographie.

B. **Partenaires d'intégration API :** Entreprises fournissant des solutions pour connecter des plateformes médicales.
C. **Institutions gouvernementales :** Assurer la conformité avec les normes de santé.
D. **Développeurs en santé numérique :** Intégration de la solution dans les applications de santé.
E. **Partenaires logistiques et cloud :** Stockage sécurisé des données.

b. Quels sont les partenariats qui nous aident à réduire les coûts, à accéder à de nouvelles ressources ou à améliorer notre proposition de valeur ?
ما هي الشراكات التي تساعدنا على خفض التكاليف أو الوصول إلى موارد جديدة أو تحسين قيمتنا المقترحة؟

- **Partenariats avec le cloud :** Réduction des coûts grâce au stockage des données.
- **Partenariats technologiques :** Accès à des solutions avancées.
- Partenariats avec les autorités de régulation : Assurer la conformité.
- **Partenariats avec des entreprises de santé :** Intégration de solutions dans des applications de santé.

c. Comment pouvons-nous aligner nos intérêts avec ceux de nos partenaires ?
كيف يمكننا مزامنة مصالحنا مع تلك لشركائنا؟

- ✓ **Objectifs communs :** Définir des objectifs partagés avec les partenaires.
- ✓ **Récompenses basées sur la performance :** Offrir des incitations basées sur la réussite du projet.
- ✓ **Collaboration stratégique :** Participation à des événements communs.
- ✓ **Partage de ressources :** Programmes de formation pour les partenaires afin de renforcer la relation.

6-Activités clés (Key Activities) : الأنشطة الرئيسية

a. Quelles sont les actions principales que nous devons entreprendre pour livrer notre proposition de valeur ?
ما هي الأنشطة الرئيسية التي يجب علينا القيام بها لتقديم قيمتنا المقترحة؟

- ✓ **Développement technologique :** Mettre à jour la plateforme en utilisant des technologies avancées.
- ✓ **Sécurisation des données :** Garantir la protection des données médicales.
- ✓ **Conformité réglementaire :** Respecter les lois en matière de protection des données.
- ✓ **Support client :** Fournir un support technique continu.

- ✓ **Partenariats stratégiques :** Établir des relations avec des entreprises et organisations technologiques et réglementaires.

b. Quelles sont les opérations essentielles pour notre entreprise ?

ما هي العمليات الأساسية لشركتنا؟

- ✓ **Gestion de la plateforme :** Maintenance continue et mise à jour de la plateforme pour assurer sa performance et sa sécurité.
- ✓ **Gestion de la plateforme :** Maintenance continue de la plateforme.
- ✓ **Suivi de conformité :** S'assurer du respect des réglementations.
- ✓ **Accompagnement client :** Offrir formation et assistance.
- ✓ **Développement de nouvelles fonctionnalités :** Innover pour répondre à l'évolution des besoins.

c. Quelles sont les activités qui créent le plus de valeur pour nos clients ?

ما هي الأنشطة التي تخلق أكبر قيمة لعملائنا؟

- ✓ **Garantie de la sécurité :** Protection des données médicales.
- ✓ **Facilité d'intégration :** Permettre une intégration fluide avec d'autres systèmes.
- ✓ **Conformité réglementaire :** Aider les clients à respecter les normes légales.
- ✓ **Support personnalisé :** Offrir un accompagnement adapté à chaque client.
- ✓ **Optimisation des processus :** Simplifier la gestion des données médicales et améliorer l'efficacité.

7- Ressources clés (Key resources) :الموارد الرئيسية

a. Quels sont nos actifs matériels, immatériels et humains essentiels ?

ما هي الأصول المادية وغير المادية والبشرية الأساسية لدينا؟

- **Matériels :** serveurs cloud (ex. AWS, Firebase), infrastructures de stockage.
- **Immatériels :** code source de la plateforme, algorithmes de chiffrement (MA-ABE, AES), licences logicielles, base de données patients.
- **Humains :** développeurs (frontend, backend, blockchain), experts en cybersécurité, consultants juridiques (RGPD), support technique.

b. Quels sont les outils, les technologies ou les partenariats dont nous avons besoin pour réussir ?

ما هي الأدوات والتكنولوجيا أو الشراكات التي نحتاجها لتحقيق النجاح؟

1- **Technologies :**
   - ❖ Blockchain (Ganache, Solidity) pour la traçabilité et l'intégrité.
   - ❖ MA-ABE (Multi-Authority Attribute-Based Encryption) pour le contrôle d'accès basé sur les attributs.
   - ❖ AES pour le chiffrement des données.
   - ❖ Vue.js (interface), Node.js (serveur), MongoDB (stockage), Cloudinary (fichiers médias).

2- **Outils:** Charm-Crypto, GoFE, Postman, GitHub, Docker.

3- **Partenariats :** cliniques, hôpitaux, autorités sanitaires, éditeurs e-santé, hébergeurs certifiés HDS.

c. Quels sont les principaux avantages concurrentiels de nos ressources ?

ما هي المزايا التنافسية الرئيسية لمواردنا؟

- Sécurité avancée grâce à l'intégration combinée de MA-ABE, AES et Blockchain.
- Adaptabilité de la plateforme à différents types d'établissements (cliniques, hôpitaux, développeurs).
- Respect des normes légales et réglementaires (RGPD, ISO 27001).
- Équipe technique spécialisée et architecture scalable.
- Possibilité d'intégration API avec d'autres systèmes de santé ou ERP.

8- Charges et coûts (Coste structure) : التكاليف

a. Quels sont les coûts fixes et variables associés à notre modèle économique ?

ما هي التكاليف الثابتة والمتغيرة المرتبطة بنموذجنا الاقتصادي؟

1- Coûts fixes :

- Hébergement cloud (ex. Firebase, MongoDB Atlas) :
  - ✓ International (Firebase, MongoDB Atlas) : **25 000 à 50 000 DA/mois**.
  - ✓ Local (serveurs certifiés HDS) : **15 000 – 30 000 DA/mois**.
- Licences logicielles et outils de développement (API, bibliothèques MA-ABE, etc.) : **10 000 à 20 000 DA /mois.**
- Salaires de l'équipe technique et support :
  - ✓ 3 développeurs, 1 expert en sécurité et 1 support : **450 000 à 700 000 DA/mois**.
- Maintenance de la plateforme : **35 000 DA/mois** (20 % du développement de développement annuel).

2- Coûts variables :

- Volume de stockage selon le nombre de patients : **30 000 DA/mois** (1 pour 1 000 patients).
- Coût d'usage de la blockchain (transactions) : **10 000 à 20 000 DA/mois** (liste privée).
- Support client à la demande (tickets, assistance personnalisée) : **50 000 à 100 000 DA/mois** (100 tickets/mois à 500 à 1000DA/ticket).
- Formations ou prestations ponctuelles pour les utilisateurs : **30000 à 50 000 DA/session** (par clinique).

b. Quels sont les coûts les plus importants pour notre entreprise ?

ما هي التكاليف الأكثر أهمية لشركتنا؟

- Développement et maintenance de la plateforme sécurisée : **700000DA/mois**
- Mise en œuvre et intégration des technologies de sécurité (Blockchain, MA-ABE, AES) : **150 000 DA/mois**
- Hébergement sécurisé et conformité réglementaire (RGPD, HDS, etc.) : **30 000 à 50 000 DA/mois**
- Recherche et développement pour l'ajout de nouvelles fonctionnalités : **100 000 DA/mois**

c. Comment pouvons-nous réduire les coûts ou améliorer l'efficacité de nos opérations ?

كيف يمكننا خفض التكاليف أو تحسين كفاءة عملياتنا؟

- Automatiser certaines tâches (génération de clés, vérification d'accès…) :
  - ✓ Économie de **30 % sur le soutien client** (15 **000 – 30 000 DA/mois**).
- Utiliser des services cloud avec tarification à l'usage (scalabilité) :
  - ✓ De **20 % sur l'hébergement** (grâce à la tarification à l'usage).
- Mutualiser les ressources entre établissements de santé partenaires.
  - ✓ Partage des coûts avec partenaires (économie de **10 000 à 20 000 DA/mois**).
- Améliorer l'UX/UI pour réduire les demandes d'assistance.
  - ✓ Ampre de **40 % des tickets de soutien (20 000 à 40 000 D et D/mois**).
- Intégrer des outils open-source (comme Charm-Crypto, GoFE) au lieu de solutions payantes.
  - ✓ Économie de **50 % sur les licences** (**5 000 à 10 000 DA/mois**).

9- Revenus (Revenue) مصادر الدخل:

a. Quels produits ou services nos clients sont-ils prêts à payer ?

ما هي المنتجات أو الخدمات التي يكون عملاؤنا على استعداد لدفع ثمنها؟

- L'utilisation de la plateforme pour gérer les données médicales de manière sécurisée.
  - ➢ Fondamental : **15 000 DA/mois** (cliniques).
  - ➢ Pro : **30 000 DA/mois** (hôpitaux).
  - ➢ Entreprise : **60 000 DA/mois** (établissements de pays en développement).

- Les services de chiffrement et déchiffrement des fichiers (MA-ABE + AES) : **500 DA/opération.**

- Le support technique personnalisé et les formations : **1 000 DA/heure** (technique d'assistance).

- L'intégration de la plateforme avec leurs propres systèmes (via API) : **50 000 DA/projet**

- Les rapports de sécurité et de conformité réglementaire sur demande : **20 000 DA/mois** (audits RGPD/HDS).

b. Quels sont les différents moyens par lesquels nous pouvons générer des revenus ?

ما هي الطرق المختلفة التي يمكننا من خلالها تحقيق الدخل؟

- Abonnement mensuel ou annuel, selon la taille de la structure et le nombre d'utilisateurs : **60 % du chiffre d'affaires** (ex. 10 Criels Pro 300 000 DA/mois).

- Frais par opération de chiffrement ou déchiffrement utilisant MA-ABE et AES : **20 % du CA** (environ 1 000 opérations MA-ABE/mois 500 000 DA.

- Ventes additionnelles (Add-ons) : rapports personnalisés, espace de stockage supplémentaire, module blockchain dédié :
  - Stock supplémentaire : **1 000 DA/Go/mois**.

- Paiement à l'usage (Pay-as-you-go) selon la consommation réelle des ressources :
  - Module mobile de chaîne de blocs : **100 000 DA/mois**.

- Services de conseil pour l'intégration, la formation et la conformité réglementaire : **200 000 DA/projet** (intégration et formation).

c. Quel est notre modèle de tarification ?

ما هو نموذج التسعير لدينا؟

1- **Modèle SaaS** (Software as a Service) avec abonnement fixe + services à la carte :
   - # **Fondamental** : 15 000 DA/mois (500 Go, 10 utilisateurs).
   - # **ProPro :** 30 000 DA/mois (1 chiffre, support 24/7).
   - # **Entreprises** : 60 000 DA/mois (chaîne de blocs, API personnalisée, audits).

2- Tarification adaptée au type de client :

- **Cliniques :** 15 000 à 30 000 DA/mois**.**
- **Hôpitaux :** 50 000 – 100 000 DA/mois**.**
- **Laboratoires :** 20 000 à 40 000 DA/mois.

3- Formules multiples :

- Basic : gestion des données + stockage limité.
- Pro : chiffrement, rapports, support étendu.

4- Enterprise : toutes les fonctionnalités + support dédié + intégration avancée (API + blockchain).

جامعة أبو بكر بلقايد
UNIVERSITY OF TLEMCEN

Business Model Canevas : BMC

Partenaires clés
Key Partnerships
الشراكة الرئيسية

- Fournisseurs Cloud (ex. FireBase, MongoDB Atlas).
- Plateformes Blockchain (ex. Ganache, solidité).
- Experts cybersécurité.
- Autorités réglementaires.
- Universités ou instituts de recherche.

Activités clés
Key Activities
الأنشطة الرئيسية

- Développement technique de la plateforme.
- Sécurisation des données (MA-ABE, AES).
- Intégration Blockchain.
- Support client.
- Réglementation de la Veille.

Ressources clés
Key resources
الموارد الرئيسية

- ♥ Technique d'Équipe (Go, Node.js, Vue.js).
- ♥ Technologies : Blockchain, MA-ABE, AES.
- ♥ L'informatique en nuage.
- ♥ Partenaires obligatoires.
- ♥ Documentation, API, support.

Proposition de valeur
Value Proposition
القيمة المقترحة

- ✓ Sécurisation des données médicales (avec MA-ABE et AES - Blockchain).
- ✓ Accès contrôlé selon rôle et institution.
- ✓ Intégration facile avec d'autres systèmes.
- ✓ Conformité RGPD / ISO.
- ✓ Interface intuitive pour tous les profils.

Relation clients
Consumer Relationship
علاقة مع العملاء

- Médecins : relation de confiance, technique de soutien personnalisée.
- Hôpitaux : contact formel, rapport régulier.
- Sustention par courrier électronique, interventions d'urgence, appui intégré.
- Amélioration prévue : vidéos courtes, système de rétroaction, support.

Canaux de distribution
Channels
قنوات التوزيع

- Site Web officiel.
- Courriel, WhatsApp, équipes.
- Démonstrations en ligne.
- Documentation intégrée.
- Combinaison supporte directement et outils en ligne.

Segment client
Customer Segment
انواع العملاء

- ❖ **Structures de santé privées** (cliniques, cabinets groupés).
- ❖ Hôpitaux (**'CHU'** Centres Hospitalo-Universitaires, **'EHS'** Établissement Hospitalier Spécialisé) et hôpitaux publics ciblés sont par autoritaires les réformes)
- ❖ Autorités de régulation.
- ❖ Les centres de diagnostic et laboratoires d'analyses médicales.
- ❖ **Assurances santé et mutuelles**.

Coûts
Coste sructure
التكاليف

- Hébergement cloud et stockage : (International : 25 000 à 50 000 DA/mois, Local : 15 000 à 30 000 DA/mois)
- Développement logiciel : 10 000 à 20 000 DA /mois.
- Sécurité et conformité : 450 000 à 700 000 DA /mois.
- Maintenance de la plateforme : 35 000 DA/mois.

Revenus (Revenue) :مصادر الدخل

- ❖ Abonnement mensuel : (freemium : 15000 DA/mois et pro :30000 DA/mois).
- ❖ Paiement par fonctionnalité (ex. stockage sécurisé) : 1 000 DA/Go/mois.
- ❖ Formations ou intégrations personnalisées : 200 000 DA/projet
- ❖ Licence pour institutions de santé : 100 000 à 250 00DA/an (Selon le type d'institution 'petites ou moyennes clinique, hôpitaux, laboratoires…')

Résumé

L'objectif de ce projet est de concevoir une plateforme sécurisée de gestion des dossiers médicaux, permettant une coopération sécurisée entre différents établissements de santé. Le système est conçu pour assurer la confidentialité, la traçabilité et la sécurité des données sensibles des patients en utilisant des techniques de chiffrement avancées, notamment MA-ABE (Multi-Authority Attribute-Based Encryption), qui permet un contrôle d'accès précis basé sur les attributs ainsi que la blockchain pour une sécurité renforcée. Le système adopte une approche distribuée en plusieurs couches : MongoDB Compass pour gérer les données des utilisateurs, la blockchain pour enregistrer de manière sécurisée les accès et les clés chiffrées à l'aide de MA-ABE et AES, un cloud multimédia pour héberger les dossiers médicaux, un serveur Node.js fait le lien entre les bases de données et l'interface utilisateur qui est développée avec Vue.js pour une interaction intuitive et réactive.

Keywords : Blockchain, MA-ABE, AES, Contrôle d'accès, HealthSafe

Abstract

The aim of this project is to design a secure platform for managing medical records, enabling secure cooperation between different healthcare establishments. The system is designed to ensure the confidentiality, traceability and security of sensitive patient data using advanced encryption techniques, including MA-ABE (Multi-Authority Attribute-Based Encryption), which enables granular access control based on attributes, and blockchain for enhanced security. The system adopts a distributed, multi-layered approach : MongoDB Compass to manage user data, the blockchain to securely record access and encrypted keys using MA-ABE and AES, a multimedia cloud to host medical records, a Node.js server provides the link between the databases and the user interface, which is developed using Vue.js for intuitive, responsive interaction.

Keywords : Blockchain, MA-ABE, AES, Access Control, HealthSafe

ملخص

الهدف من هذا المشروع هو إنشاء لوحة آمنة لإدارة الملفات الطبية، مما يسمح بالتعاون الآمن بين المؤسسات الصحية المختلفة. تم تصميم النظام لضمان السرية وإمكانية التتبع وأمن البيانات الحسية للمرضى باستخدام تقنيات التشفير المتقدمة، بما في ذلك MA-ABE (التشفير القائم على السمات المتعددة)، والذي يسمح بالتحكم في الوصول الحبيبي على أساس السمات و Blockchain لتعزيز الأمان. يعتمد النظام نهجًا للتوزيع والأسطح المتعددة: MongoDB Compass لتوزيع بيانات المستخدمين، و Blockchain للتسجيل الآمن تمامًا للوصول والكلمات المشفرة بمساعدة MA-ABE و AES، ووسائط متعددة جديدة لحفظ الملفات طبي، خادم Node.js يضمن الامتياز بين قواعد البيانات وواجهة المستخدم، التي تم تطويرها بمساعدة Vue.js من أجل تفاعل بديهي وسريع الاستجابة.

الكلمات المفتاحية: Blockchain, MA-ABE, AES, Access Control, HealthSafe