

République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université des Sciences et de la Technologie Houari Boumediene



Faculté d’Informatique
Spécialité: Big Data Analytics

Module : Stratégie de sécurité pour l'aide à la décision.

Confidentialité des données dans le BigData

Présenté par:

- BENABED Anfel
- AMINE Ishak
- SAID Faten Racha
- ABDELBAKI Feriel
- KHERROUBI Kenza
- YACEF Yasmina
- BOUKERSI Yasmine
- ATTATFA Faiza

Table des matières

1	Introduction générale	3
2	Partie théorique	4
2.1	Confidentialité	4
2.1.1	Définition de la confidentialité	4
2.1.2	Les types de confidentialité :	4
2.1.3	Le droit à la confidentialité :	5
2.2	Généralité sur le Big Data	5
2.2.1	Définition de la Big Data	5
2.2.2	Différent type de la big data:	7
2.2.3	Où trouve-t-on le Big Data et à quoi sert-il ?	8
2.2.4	Coexistence entre le Big Data et la confidentialité	8
2.3	Les risques et violations liées aux confidentialités des données dans le BIG DATA :	8
2.3.1	L'automatisation de la discrimination	9
2.3.2	Une augmentation des fuites de données	9
2.3.3	La fin de l'anonymat et de la confidentialité	9
2.3.4	Les abus gouvernementaux	10
2.3.5	La vente aux enchères des données	10
2.4	Que faire en cas de violation de données ?	11
2.4.1	Dans quel délai notifier ?	11
2.4.2	Comment notifier ?	11
2.5	Comment garantir la confidentialité des données dans le big data ?	13
2.5.1	Mieux définir et contrôler les droits d'accès	13
2.5.2	Interroger et partager des données chiffrées	14
2.5.3	Identification	16
2.5.4	Authentification	16
2.6	L'importance de garantir la confidentialité	16
3	Application Desktop et site web	17
3.1	Présentation du projet	17
3.2	Environnement de travail	18
3.2.1	Les langages de programmation	18
3.2.2	Les outils de programmation	18
3.2.3	Outils de gestion de projet/ organisation	19

3.3	Description des techniques utilisées	20
3.3.1	Création et configuration de la connexion à la base de données	20
3.3.2	Algorithme de cryptage et décryptage de données	20
3.4	Description des pages de l'application web	22
3.4.1	L'authentification	22
3.4.2	La page de l'administrateur de l'hôpital	23
3.4.3	La page du médecin	26
3.4.4	La page de la secrétaire	31
3.4.5	La page de l'administrateur Général	37
3.5	Description des fenêtres du logiciel	41
3.5.1	Authentification	41
3.5.2	Fenêtres de l'administrateur	43
3.5.3	Fenêtres de la secrétaire	47
3.5.4	Fenêtres du médecin	55
3.5.5	Fenêtres du ministère	62
4	Conclusion	66

List of Figures

1	les 3V du big data	6
2	types de données	7
3	principe de fonctionnement de chiffrement symétrique	14
4	principe de fonctionnement de chiffrement asymétrique	15

1 Introduction générale

L'exploitation de la donnée au service de la prise de décision par l'homme s'enracine dans les pratiques des Etats, ayant guidé les développements mathématiques et technologiques bien avant les derniers progrès en informatique, les algorithmes à la mode, la naissance du terme « Big Data » et sa propagation dans le monde des entreprises.

Cependant, aucune définition précise ou universelle ne peut être donnée au Big Data. Étant un objet complexe polymorphe, sa définition varie selon les communautés qui s'y intéressent en tant qu'usager ou fournisseur de services. Une approche transdisciplinaire permet d'appréhender le comportement des différents acteurs.

Le big data ne dérive pas des règles de toutes les technologies, il est aussi un système technique dual. En effet, il apporte des bénéfices mais peut également générer des inconvénients. Le Big Data a également été un grand allié des politiques de sécurité, car les menaces peuvent être identifiées à partir du comportement des personnes, bien qu'elles puissent souvent être fausses. nous intéressons dans notre projet à la confidentialité des données dans le Big Data ,ce dernier est organisé en deux parties : 1. Première partie : nous représentons une vue générale sur le big data, la confidentialité des données et la manière dont on doit la garantir.

2. deuxième partie : nous représentons le fonctionnement de notre application, et nous terminons par une brève conclusion.

2 Partie théorique

2.1 Confidentialité

Lorsque l'on partage des informations personnelles ou confidentielles bien évidemment on souhaite qu'elles restent dans le cadre privé ce qui est l'objectif de la confidentialité.

2.1.1 Définition de la confidentialité

Le but de la « Confidentialité » est d'assurer la protection des données en empêchant la divulgation non autorisée d'informations. Seules les personnes ayant l'autorisation légitime d'accéder aux informations requises devraient y être autorisées. Dans l'ensemble, l'objectif de la confidentialité est d'empêcher que des données sensibles ne tombent entre de mauvaises mains.

2.1.2 Les types de confidentialité :

- Confidentialité journalistique:
les journalistes parfois sont tenus de respecter l'anonymat de leur sources
- Confidentialité légale :
les avocats sont obligés par la loi de ne pas divulguer les informations concernant leur clients
- Confidentialité en médiation:
Les locataires sont tenus, dans la plupart des cas de l'exercice de leurs activités à la confidentialité à l'intérieur des assemblée du comité ou assemblée générale.
- Confidentialité médicale:
Les communications entre un médecin et un patient dans un cadre médical professionnel sont également confidentielles.
- Confidentialité informatique:
En informatique, la confidentialité fait partie, avec l'intégrité, la disponibilité des exigences fondamentales de la sécurité informatique.
Tout document classifié transféré par voie électronique doit donc être chiffré afin d'empêcher des personnes non autorisées d'en lire le contenu.

- Confidentialité de la correspondance:
une lettre marquée « confidentielle » ne peut être divulguée par son récipiendaire sans l'accord exprès de son envoyer .
- Confidentialité religieuse:
Comme la confession : les prêtres catholiques sont soumis au secret « professionnel ».
- Confidentialité militaire:
Des niveaux d'habilitation d'accès aux informations dites « secrètes » sont établis par l'autorité aux personnes physiques ainsi qu'à des personnes morales devant accéder à ces informations.

2.1.3 Le droit à la confidentialité :

La confidentialité et le respect de la vie privée est à la fois un droit humain et une obligation professionnelle. La divulgation des informations sensibles est punie par la loi : Article 301 du code pénal : « ...toutes autres personnes dépositaires, par état ou professions ou par fonctions permanentes ou temporaires, des secrets qu'on leur confie, qui hors le cas ou la loi les obligent ou les autorisent à se porter dénonciateurs, ont révélé ces secrets, sont punis d'un emprisonnement d'un à six mois et d'une amende de 500 à 5000 DA...».

2.2 Généralité sur le Big Data

Suite à l'explosion quantitative des données numériques, les chercheurs obligés de trouver de nouvelles manières de voir et d'analyser le monde. Il s'agit de découvrir de nouveaux ordres de grandeur concernant la capture, la recherche, le partage, le stockage, l'analyse et la présentation des données, ainsi est né le « Big Data ». Le Big Data change notre vision du monde faisant passer de la démarche analogique au savoir numérique, c'est sans doute une carte décisive pour les pays émergents. Pour révolutionnaire qu'il soit, il demeure une création humaine, limitée d'abord par nos capacités de compréhension

2.2.1 Définition de la Big Data

Le Big Data, données massives ou méga-données est un concept permettant de stocker un nombre indicible d'informations sur une base numérique. Ils désignent un ensemble très volumineux de données qu'aucun outil classique

de gestion de BDD ou de gestion de l'information ne peut vraiment travailler. Aujourd'hui, nous produisons environ 2.5 trillions d'octets de données tous les jours provenant de partout (messages envoyés, vidéos publiées...) Ces données sont baptisées Big Data.

On définit souvent le Big Data par les 3V qui caractérisent : le volume, la variété et la vélocité avec laquelle les données sont générées, collectées et traitées, c'est ce qui différencie les mégadonnées des données traditionnelles.

Les 3 v du Big Data

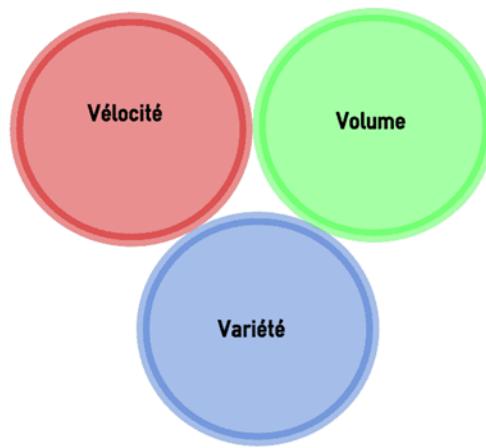


Figure 1: les 3V du big data

le volume

Le volume correspond à la masse d'informations produite chaque second.

la vélocité

La vélocité équivaut à la rapidité de l'élaboration et du déploiement des nouvelles données. Par exemple, si on diffuse des messages sur les réseaux sociaux, ils peuvent devenir « viraux » et se répandre en un rien de temps. Il s'agit d'analyser les données au cours de leur lignée (appelé parfois analyse en mémoire) sans qu'il soit indispensable que ces informations soient entreposées dans une base de données.

la variété

Seulement 20% des données sont structurées puis stockées dans des tables de bases de données relationnelles similaires à celles utilisées en gestion compt-

abilisée.

Les 80% qui restent sont non-structurées. Cela peut être des images, des vidéos, des textes, des voix, et bien d'autres encore... La technologie Big Data, permet de faire l'analyse, la comparaison, la reconnaissance, le classement des données de différents types comme des conversations ou messages sur les réseaux sociaux, des photos sur différents sites etc. Ce sont les différents éléments qui constituent la variété offerte par le Big Data.

2.2.2 Différent type de la big data:

Le Big Data englobe 3 types de données : données structurées, semi-structurées et non-structurées afin de les exploiter et les utiliser dans de différents projets.

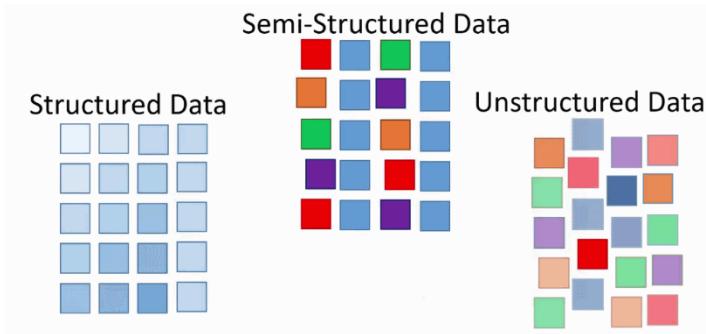


Figure 2: types de données

Données structurées : Dans la plupart des cas, elles sont traitées par des machines et ont un format fixe. Ce type de données est constitué d'informations déjà gérées par l'organisation dans des bases de données et des feuilles de calcul stockées dans des bases de données SQL, des data lakes et des data warehouses.

Données non structurées : sont des informations qui ne sont pas organisées et qui n'ont pas de format prédéterminé, car il peut s'agir de quasiment n'importe quoi. Par exemple, elles comprennent les données recueillies à partir des réseaux sociaux et elles peuvent être placées dans des fichiers texte conservés dans des clusters de type Hadoop ou des systèmes NoSQL.

Données semi-structurées : peuvent contenir les deux types de données, comme c'est le cas des journaux de serveur Web. Il s'agit des données qui, bien qu'elles n'aient pas été classées dans un dépôt (base de données) particulier, contiennent des informations essentielles ou des balises séparant les différents éléments au sein des données.

2.2.3 Où trouve-t-on le Big Data et à quoi sert-il ?

-Le Big Data est engrangé dans tous les systèmes dans de différents secteurs. Il peut s'agir d'améliorer les opérations, de proposer un meilleur service client, de créer des campagnes marketing personnalisées basées sur les préférences, augmenter le chiffre d'affaires...

-Grace au Big Data, les entreprises peuvent profiter d'un avantage compétitif face à leurs concurrents n'exploitant pas les données. Elles peuvent prendre des décisions plus rapides et plus précises s'appuyant directement sur les informations.

-Le Big Data est utilisé dans le domaine de la recherche médicale. Il permet notamment d'identifier des facteurs de risques de maladies ou de réaliser des diagnostics plus fiables et plus précis

-L'industrie de l'énergie s'en sert pour découvrir des zones de forage potentielles et de surveiller leurs opérations ou les réseaux électriques.

-Les entreprises de transports gèrent leurs chaînes logistiques et optimisent leurs itinéraires de livraison grâce aux données collectées et exploitées

2.2.4 Coexistence entre le Big Data et la confidentialité

Dans un monde actuel connecté, les consommateurs sont de plus en plus enclins à partager leurs informations sur Internet.

Aujourd'hui, la valeur de la data n'est plus à démontrer et intéresse aussi bien les entreprises que les cybercriminels qui visaient uniquement à collecter des données d'utilisateurs. Etre en mesure de traiter et d'analyser les informations échangées par les individus tout en s'assurant qu'elles soient bien protégées, est le défi à relever à la fois par les entreprises et les fournisseurs de services. A l'heure du Big Data, comment gérer les flux massifs de données et être assurées du niveau de confidentialité nécessaire ?

2.3 Les risques et violations liées aux confidentialités des données dans le BIG DATA :

Le Big Data apporte de nombreux bénéfices aux entreprises, mais représente également un risque de sécurité pour la confidentialité. Les milliers de données partagées par les individus exposent leur vie privée plus que jamais auparavant. Les données personnelles valent de l'or pour les marketeurs, les in-

stitutions financières, les employeurs ou les gouvernements. Les conséquences peuvent être désastreuses pour les individus, qui peuvent par exemple se voir refuser un emploi ou un crédit à cause de leurs données. Découvrez les cinq principaux risques pour la confidentialité liés au Big Data.

2.3.1 L'automatisation de la discrimination

Il y a trois ans, l'EPIC estimait que l'utilisation des analyses prédictives dans le secteur public et le secteur privé peuvent permettre aux gouvernements et aux entreprises d'évaluer la capacité d'une personne à obtenir un emploi ou un crédit. Or, cette utilisation nuit directement à la liberté d'association. Depuis lors, les choses n'ont fait qu'empirer. La discrimination est illégale, mais l'automatisation des prises de décision la rend difficile à prouver. En somme, le Big Data tend à automatiser la discrimination. Malgré les avancées réalisées dans le domaine du Big Data, les lois sur la protection n'ont pas évolué.

2.3.2 Une augmentation des fuites de données

À la suite des nombreuses fuites de données de géants du commerce comme Target, Home Depot, ou de sites comme eBay, ayant impacté des dizaines de millions d'individus, le public est très alerte quant aux fraudes de cartes de crédit et aux usurpations d'identité. Hélas, le risque reste toujours très élevé, notamment à cause de l'essor de l'internet des objets. Désormais, de très nombreux meubles sont connectés dans nos foyers, au même titre que les voitures et autres accessoires que nous portons au quotidien. Le nombre cibles potentielles pour les hackers est décuplé.

2.3.3 La fin de l'anonymat et de la confidentialité

De nos jours, il est de plus en plus difficile de faire quoi que ce soit sans que notre identité soit associée à nos actions. Même les données « désidentifiées » représentent un risque pour la confidentialité. Les standards de sécurité utilisés il y a encore un an ou deux ne sont plus suffisants. Les entreprises qui souhaitent rendre les données anonymes sont confrontées à une difficulté croissante. Il sera bientôt impossible d'empêcher les données de pouvoir être à nouveau associées aux individus. En plus d'être vulnérables aux fuites, les objets connectés sont de véritables machines à collecter les données les plus personnelles des utilisateurs. Les constructeurs peuvent changer les

conditions de confidentialité à tout moment, et il est difficile de convaincre un utilisateur d'arrêter d'utiliser sa télévision connectée ou sa voiture connectée à la suite d'un tel changement.

2.3.4 Les abus gouvernementaux

Selon l'EPIC, le nombre de bases de données gouvernementales américaines est plus élevé que jamais auparavant. Le FBI par exemple collecte des données personnelles comme le nom, les pseudonymes, l'origine ethnique, le genre, le lieu et la date de naissance, le numéro de sécurité sociale, le numéro de passeport, l'adresse, les numéros de téléphone, les photos, les empreintes digitales, les numéros de compte bancaire, et l'emploi des citoyens. En effet, l'agence s'est elle-même émancipée du Privacy Act de 1974.

2.3.5 La vente aux enchères des données

De nombreuses entreprises collectent et vendent les données des utilisateurs, permettant d'établir des profils d'individus. Les entreprises peuvent désormais savoir si une femme est enceinte, si une personne est homosexuelle ou si elle est atteinte d'un cancer avant même qu'elle ne le révèle à ses proches. Aucune loi ne protège réellement les consommateurs contre de tels agissements. Jusqu'à ce que des lois pour la protection de la confidentialité soient votées, ces pratiques continueront.

2.4 Que faire en cas de violation de données ?

En cas de violation du système de données, le responsable des données dispose de 72 heures maximum pour prévenir la CNIL et les personnes concernées. On entend par violation de données à caractère personnel :

- La destruction, la perte ou l'altération non désirée.
- La divulgation non autorisée de données à caractère personnel.

L'accès non autorisé à des données à caractère personnel transmises, conservées ou traitées d'une autre manière.

2.4.1 Dans quel délai notifier ?

La notification doit être transmise à la CNIL dans les meilleurs délais à la suite de la constatation d'une violation présentant un risque pour les droits et libertés des personnes. Si vous ne pouvez pas fournir toutes les informations requises dans ce délai car des investigations complémentaires sont nécessaires, vous pouvez procéder à une notification en deux temps :

- Une notification initiale dans un délai de 72 heures si possible à la suite de la constatation de la violation ;
- Si le délai de 72 heures est dépassé, vous devrez expliquer, lors de votre notification, les motifs du retard ;
- Enfin, une notification complémentaire dès lors que les informations complémentaires sont disponibles.

2.4.2 Comment notifier ?

- Dans tous les cas, vous devez documenter en interne l'incident en déterminant
- La nature de la violation
- Si possible, les catégories et le nombre approximatif de personnes concernées par la violation
- Les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés ;

- Décrire les conséquences probables de la violation de données ;
- Décrire les mesures prises ou que vous envisagez de prendre pour éviter que cet incident se reproduise où atténuer les éventuelles conséquences négatives.

Si la violation notifiée fait suite à une cyberattaque, il est conseillé de déposer plainte au commissariat de police ou à la gendarmerie la plus proche et de tenir à disposition des enquêteurs tous les éléments de preuves techniques en votre possession.

2.5 Comment garantir la confidentialité des données dans le big data ?

Pour garantir la confidentialité et la protection des échanges, le système d'information doit garantir les points suivants :

2.5.1 Mieux définir et contrôler les droits d'accès

Le contrôle d'accès est une technique de sécurité qui peut être utilisée pour déterminer les utilisateurs ou les programmes autorisés à voir ou à utiliser. Plusieurs approches du contrôle d'accès permettent d'assurer la confidentialité, chacune ayant ses propres forces et faiblesses :

- **Discretionary Access Control (DAC, Contrôle d'accès facultatif)** Dans un modèle DAC, les utilisateurs peuvent partager des informations de manière dynamique avec d'autres utilisateurs. Cette méthode offre un environnement plus flexible, mais elle augmente le risque de divulgation non autorisée d'informations. Les administrateurs ont plus de mal à faire en sorte que seuls les utilisateurs appropriés puissent accéder aux données.
- **Role-Based Access Control (RBAC)** Le contrôle d'accès basé sur les rôles instaure un contrôle d'accès basé sur la fonction ou la responsabilité des postes. Chaque employé a un ou plusieurs rôles qui lui permettent d'accéder à des informations spécifiques. Si une personne change de rôle, elle perd l'accès au rôle précédent. Les modèles RBAC offrent plus de flexibilité que le modèle MAC et moins que le modèle DAC. Ils présentent toutefois l'avantage de se fonder strictement sur la fonction du poste, et non sur les besoins individuels.
- **Mandatory access control (MAC, Contrôle d'accès obligatoire)** Dans un environnement MAC, toutes les capacités d'accès sont prédéfinies. Les utilisateurs ne peuvent pas partager d'informations, à moins que des administrateurs ne leur octroient ces droits. Les administrateurs doivent donc modifier ces droits en conséquence. Ce processus impose un modèle de sécurité rigide.
- **Attribute-based access control (ABAC)** Le contrôle d'accès basé sur les attributs (ABAC) est une approche différente du contrôle d'accès dans laquelle les droits d'accès sont accordés grâce à l'utilisation de

politiques composées d'attributs travaillant ensemble. ABAC utilise des attributs comme blocs de construction pour définir les règles de contrôle d'accès et les demandes d'accès.

2.5.2 Interroger et partager des données chiffrées

Le chiffrement désigne la conversion des données depuis un format lisible à un format codé. Les données chiffrées ne peuvent être lues ou traitées qu'après leur déchiffrement. Cette conversion correspond à la capture de données lisibles et à leur modification en données chiffrées. Le chiffrement implique l'utilisation d'une clé cryptographique, c'est-à-dire un ensemble de valeurs mathématiques convenues par l'expéditeur et le destinataire. Le destinataire utilise la clé pour déchiffrer les données et les transformer en texte brut lisible. Il y a deux principaux types de chiffrement :

- **Le chiffrement symétrique** Ce chiffrement fonctionne en principe avec une clé privée dans lequel l'émetteur du message chiffre les données grâce à cette clé qui est généralement une chaîne de caractères. Le message est chiffré et sans la clé il est impossible (le niveau d'impossibilité dépend du niveau de protection du chiffrement utilisé ainsi que de la complexité de la clé utilisée) de retrouver le message d'origine. L'émetteur doit donc transmettre la clé aux personnes à qui il désire transmettre le message s'il veut que son message puisse être lu. Donc la même clé est utilisée pour chiffrer ou déchiffrer un message.

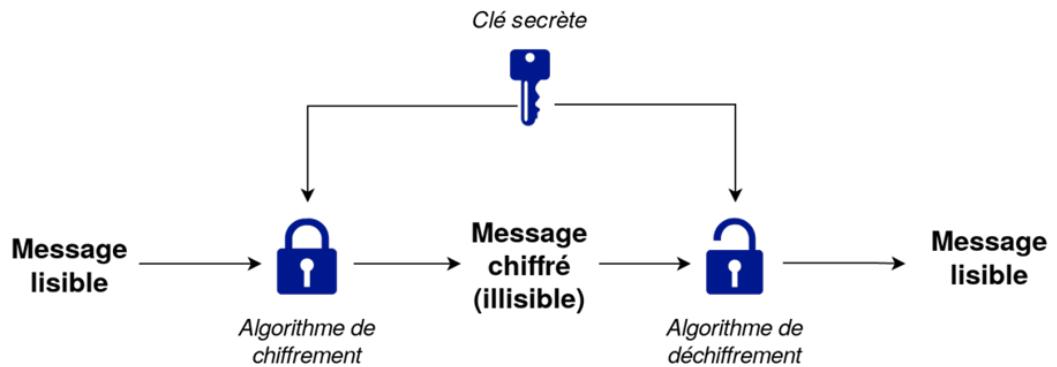


Figure 3: principe de fonctionnement de chiffrement symétrique

Il existe plusieurs algorithmes utilisés pour effectuer le chiffrement et le déchiffrement symétrique comme :

- Data Encryption Standard (DES).
- Triple-DES (3DES).
- Advanced Encryption Standard (AES).
- RC (Ron’s Cipher ou Ron’s Code).
- Blowfish et Twofish.
- International Data Encryption Algorithm (IDEA).
- Masques jetables.

- **Le chiffrement asymétrique** Le système de chiffrement par clés asymétriques repose sur l’association de deux clés de codage différentes : une clé publique et une clé privée. L’expéditeur utilise la clé publique pour chiffrer un message, et le destinataire utilise la clé privée pour le déchiffrer. Elles sont liées mais ne sont pas interchangeables ce qui garantit la protection des échanges chiffrés.

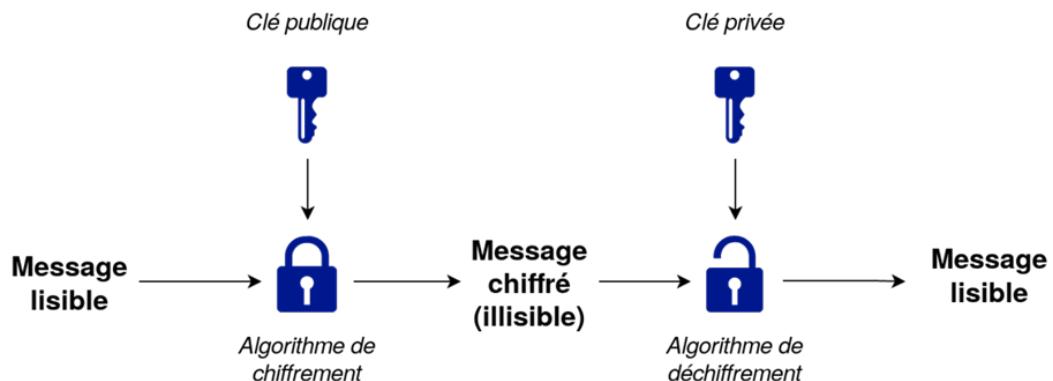


Figure 4: principe de fonctionnement de chiffrement asymétrique

Voici quelques algorithmes asymétriques :

- RSA.
- Diffie-Hellman.
- ECC (Elliptic Curve Cryptography).

2.5.3 Identification

L'identification est une phase qui consiste à établir l'identité de l'utilisateur. Elle permet répondre à la question : "Qui êtes vous ?". L'utilisateur utilise un identifiant qui l'identifie et qui lui est attribué individuellement. Cet identifiant est unique.

2.5.4 Authentification

L'authentification est la vérification de l'identité d'un utilisateur. L'utilisateur qui souhaite se connecter à un terminal et accéder aux données est-il vraiment celui qu'il prétend être ? Il ne suffit donc pas de se fier à l'identité que la personne ou la ressource informatique indique avoir. Il faut être capable de vérifier cette identité afin de s'assurer qu'il s'agit bien de la personne ou ressource informatique.

2.6 L'importance de garantir la confidentialité

Assurer la confidentialité des données implique une évaluation soigneuse du type de données collectées et de la façon de les acquérir, de les utiliser, de les stocker et de les communiquer. Et la protection des informations confidentielles, les identités des personnes représentées dans les bases de données contre tout accès non autorisé et toute fuite des données stockées.

3 Application Desktop et site web

3.1 Presentation du projet

Dans le temps, les hôpitaux cumulent un nombre important de données, ce qui rend leur traitement assez vite fastidieux. Il devient ainsi nécessaire pour eux de se tourner vers des outils et moyens d'automatiser leurs systèmes dans le but de faciliter leurs différentes opérations logistiques tout en leurs assurant une sécurité en terme de confidentialité de données.

De ce fait, nous avons réalisé un site web ainsi qu'un logiciel (application de bureau) afin de faciliter la gestion des différents hôpitaux à l'échelle nationale. Les principaux acteurs sont les suivants :

- **Administrateur** : propre à chaque hôpital, il a pour fonction d'enregistrer les différents fonctionnaires de son hôpital (inscrire leurs informations dans la base de donnée).
- **Medecin** : il existe plusieurs médecins par services et hôpitaux, il est possible pour un médecin de consulter les informations personnelles ou médicales de ses patients, ajouter une nouvelle consultation ou encore examiner les informations médicales de patients externes (provenant d'un autre service ou hôpital).
- **Secretaire** : propre à chaque service de l'hôpital, elle a comme possibilité de consulter les informations personnelles des patients, les modifier ou encore les archiver.
- **Ministere** : il peut consulter les données personnelles et médicales de tous les patients de tous les hôpitaux du pays

Remarque :

Nous sommes partis du principe que chaque hôpital peut disposer d'un logiciel de gestion différent. Nous avons donc créé des fenêtres avec des affichages qui diffèrent en fonction de l'hôpital auquel appartient le fonctionnaire. Ainsi, les données sont stockées de manière non structurés dans la base de données nationale comme le montre la capture d'écran ci-dessous prise d'une des tables de la base.

	idConsultation	taille	poids	tension	observation	diagnostic	dateConsult	idPatier
►	15	zABQtz0XchrD5gPHwaK9A==	YHpBVP4+gDz0PgjqdVR2j...	NULL	sz5hxXTidb5N7AGzEIRNsg==	NULL	2021-12-29	14
	23	8h9vwwoJ9x6RKRTa5DUvw==	9j2JuaJ/7E72lIZCQjhxpXA==	NULL	BSRk21T7wPKE5APshSVmqczfRidDBPsAKBtsW5...	NULL	2021-12-29	15
	24	zABQtz0XchrD5gPHwaK9A==	YHpBVP4+gDz0PgjqdVR2j...	NULL	iyCkmF9sU9rra49cadfoMQ==	NULL	2021-12-29	14
	25	Xosak3kgdaYokSZlp6GRw==	JRhCBkjK470Lpqk+h1t1Z...	NULL	x9mF9gAN9TLG/bzSStlwx566w2tyocHOzwMrd...	NULL	2021-12-29	40
	26	ksuMAbRALvvQR6W0jtTrg==	yYa3xVX/9D2Wbx55vIA...	NULL	OWzbtfmffj2vNBOK4cg8MFohz431MwC3B0b...	NULL	2021-12-29	17
	27	ZgrnPPEO6K5HP4fY0/GNDg==	S6dqxBICIRGB2zqkKCwA...	NULL	PRUEx5FjKFJ6S1r4UCKMyHdI/QexVajw8qGoQcr...	NULL	2021-12-29	18
	28	Ryjyy19j4js/j7WiybneW==	yYa3xVX/9D2Wbx55vIA...	NULL	iyCkmF9sU9rra49cadfoMQ==	NULL	2021-12-29	19
	29	MDgLyovXazCxREUET7ht5w==	ocAfeOztwVvejDmICO52F...	NULL	We9j7voKdn+72G1sfyKdDiwOxW6AcgYNJp+3...	NULL	2021-12-29	19
	30	MDgLyovXazCxREUET7ht5w==	+i+0CBpjRzRvc5CBozaSL...	NULL	W2t0XAfefQ+2kdfQfmlntSwOxW6AcgYNJp+3...	NULL	2021-12-29	42
	31	MDgLyovXazCxREUET7ht5w==	hkKJSDxa6kKKj0h+5EMt...	NULL	tZs7BRvJ1bjqMvD1ec/hVvASYUfnYt0y1e5oU...	NULL	2021-12-29	42
	32	NULL	NULL	WMVaXluc6bNwNN3...	NULL	UdNPhN...	2021-12-29	26
	33	NULL	NULL	BrDACzXRcktCS4782...	NULL	UdNPhN...	2021-12-29	28
	34	NULL	NULL	3/xqJzh5dTwWUS1c...	NULL	iyCkmF9s...	2021-12-29	31
	35	6kr5AzodVOL/SyDhjEl9Q==	WIB3FPagCvy9L213xxzrf...	NULL	PRUEx5FjKFJ6S1r4UCKMyHdI/QexVajw8qGoQcr...	NULL	2021-12-29	21
	36	1v8CZlt4b3uMzsnaRFZQg==	oUFkaEkx3yY80IkM2jqpQ...	NULL	iyCkmF9sU9rra49cadfoMQ==	NULL	2021-12-29	25
	37	NULL	NULL	OZrevHFw8/GhOLTU...	NULL	BDvYVQS...	2021-12-29	34
	38	NULL	NULL	WMVaXluc6bNwNN3...	NULL	r7Zo2F...	2021-12-29	37

Aussi, le temps de cryptage et de décryptage des données a été calculé et affiché à la console comme suit :

Temps de decryptage :25 ms

Temps de cryptage :21 ms

3.2 Environnement de travail

3.2.1 Les langages de programmation

- **Java** : Java est un langage de programmation généraliste basé sur les classes, orienté objet et conçu pour avoir le moins de dépendances d'implémentation possible.
- **PHP** : PHP, aussi appelé Hypertext Preprocessor, est un langage de programmation libre, orienté objet et qui est conçu pour produire des pages web dynamiques selon un serveur HTTP.

3.2.2 Les outils de programmation

- **Eclipse** : Eclipse est un projet, décliné et organisé en un ensemble de sous-projets de développements logiciels, de la fondation Eclipse visant

à développer un environnement de production de logiciels libre qui soit extensible, universel et polyvalent, en s'appuyant principalement sur Java.

- **SceneBuilder** : Un outil interactif de conception d'interface graphique pour JavaFX.
- **MySQL WorkBench** : MySQL Workbench (anciennement MySQL administrator) est un logiciel de gestion et d'administration de bases de données MySQL créé en 2004. Via une interface graphique intuitive, il permet, entre autres, de créer, modifier ou supprimer des tables, des comptes utilisateurs, et d'effectuer toutes les opérations inhérentes à la gestion d'une base de données.
- **Visual Code** : Visual Studio Code est un environnement de développement intégré (IDE).
Il est utilisé pour développer des programmes informatiques et des applications web/mobiles.
C'est un éditeur de texte qui peut être utilisé avec de nombreux langages de programmation, notamment Java, PHP, C++, Dart, Flutter...
Etc.
- **HTML** : le HTML sous son nom complet HyperText Markup Language, est un langage de balisage dans le but de concevoir des pages web.
- **CSS** : Cascading Style Sheets ou les feuilles de style est un langage qui décrit la page web.
- **PHPMyAdmin** : C'est une application de gestion et d'administration de bases de données MySQL créé en 1998 et qui est principalement en PHP.

3.2.3 Outils de gestion de projet/ organisation

- **Git/GitHub Desktop** : Un logiciel de gestion de versions décentralisé, il permet principalement de suivre l'évolution d'un code source et travailler à plusieurs sur un même projet.

- **Google Drive** : Un service de stockage et de partage de fichiers dans le cloud lancé par la société Google, il sert à synchroniser, partager et modifier les données entre plusieurs ordinateurs et/ou utilisateurs.
- **Google Sheets** : Un programme inclus dans le cadre de la suite Web gratuite Google Docs Editors proposée par Google, il permet de créer des feuilles de calcul, les modifier et travailler à plusieurs dessus.

3.3 Describtion des techniques utilisées

3.3.1 Création et configuration de la connexion à la base de données

Nous avons crée notre base de données en utilisant le serveur local Mamp qui permet de travailler avec le système de gestion de base de données MySQL. Nous avons établi la connexion de notre application au serveur de notre base de données en ayant renseigné plusieurs informations telles que le type de base de données, son nom ou encore le port de connexion, ci-dessous le code utilisé :

```
public static void main(String[] args) throws SQLException{
    //connexion à la base
    Connection myConn = DriverManager.getConnection("jdbc:mysql://localhost:3306/projetsecurite?serverTimezone=UTC", "root", "root");
    connection = myConn;
    System.out.println("Successfully connected to database");
    launch(args);
}
```

3.3.2 Algorithme de cryptage et décryptage de données

- **Principe du AES** : Le chiffrement AES « Advanced Encryption Standard », connu aussi sous le nom de Rijndael, est un standard de cryptage symétrique destiné à remplacer le DES (Data Encryptions Standard) qui est devenu trop faible au regard des attaques actuelles. L'AES opère sur des blocs de 128 bits qu'il transforme en blocs cryptés de 128 bits par une séquence de Nr opérations ou "rounds", à partir d'une clé de 128, 192 ou 256 bits. Suivant la taille de celle-ci, le nombre de rounds diffère : respectivement 10, 12 et 14 rounds. Il est ainsi

basé sur une même clef secrète qui est utilisée pour les opérations de chiffrement et de déchiffrement.

Cet algorithme devint un standard de chiffrement symétrique à partir de l'an 2000, approuvé et utilisé par la NSA « National Security Agency ». ».

- **Principe du RSA :** Le chiffrement à clé publique, également appelé chiffrement asymétrique, utilise deux clés différentes, mais mathématiquement liées, une publique et l'autre privée. La clé publique peut être partagée avec quiconque, tandis que la clé privée doit rester secrète. Dans le chiffrement RSA, tant la clé publique que la clé privée peuvent servir à chiffrer un message. Dans ce cas, c'est la clé opposée à celle ayant servi au chiffrement qui est utilisée pour le déchiffrement. Dans ce qui suit, nous présentons le projet sous ces deux formats soit, le site web puis l'application de bureau. Il est à noté que certaines différences peuvent être remarquées entre ces deux versions, elles comportent néanmoins, toutes les fonctionnalités principales.
- **Principe du hashage :** Une fonction de hachage cryptographique est une primitive cryptographique qui transforme un message de taille arbitraire en un message de taille fixe, appelé un condensé. Les fonctions de hachage cryptographiques sont employées pour l'authentification, les signatures numériques et les codes d'authentification de messages. Pour être utilisable en cryptographie, une fonction de hachage doit disposer de ces qualités :
 - rapide à calculer (parce qu'elles sont fréquemment sollicitées).
 - non réversible (chaque condensé peut provenir d'un très grand nombre de messages, et seule la force brute peut générer un message qui conduit à un condensé donné).
 - résistant à la falsification (la moindre modification du message aboutit à un condensé différent).
 - résistant aux collisions (il devrait être impossible de trouver deux messages différents qui produisent le même condensé).

La fonction de hashage utilisé est une API inclus dans PHP 5 et elle expose 4 fonctions simples :

- **password_hash()** : Pour hacher le mot de passe , elle prend en paramètre le mot de passe qu'on veut hacher puis la fonction de hachage à utiliser.
- **password_verify()** : Pour vérifier si le mot de passe introduit correspond au mot de passe haché , elle prend en paramètre le mot de passe introduis puis le mot de passe haché présent dans la base de données.
- **password_needs_rehash.**
- **password_get_info.**

3.4 Description des pages de l'application web

Avant de commencer la description des pages, on voudrait souligner que nous distinguerons ci-dessous dans la plus part d'entre elles, deux formes différentes (deux cas) de page selon l'hôpital correspondant et pour cela l'hors de l'authentification l'application distinguera la page à afficher selon une fonction qui prends en charge le code wilaya : Le cas 01 des wilayas de 01 à 29 et le cas 02 des wilays de 30 à 58.

3.4.1 L'authentification

Lors du lancement de l'application, une page d'accueil apparaîtra, celle-ci permettra à l'utilisateur de s'authentifier en introduisant les informations de son compte (son email, sa date de naissance ainsi que son mot de passe) enregistrées dans notre base de données. Selon sa fonction, l'application l'orientera vers ses sa propre page.

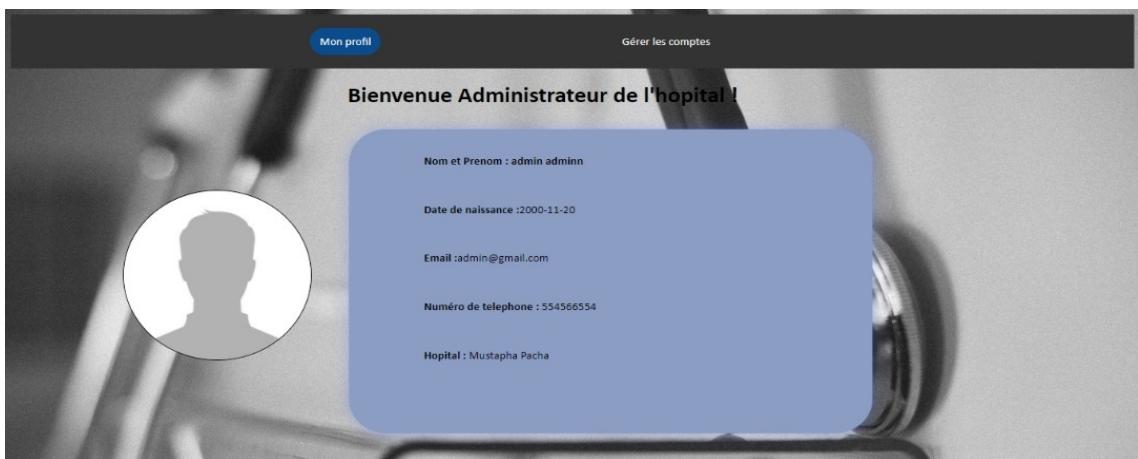
- Dans le cas où l'utilisateur ne remplit pas tous les champs requis du formulaire d'authentification, une erreur lui sera affichée.
- Dans le cas où l'utilisateur remplit mal un des champs du formulaire d'authentification, une erreur lui sera affichée.



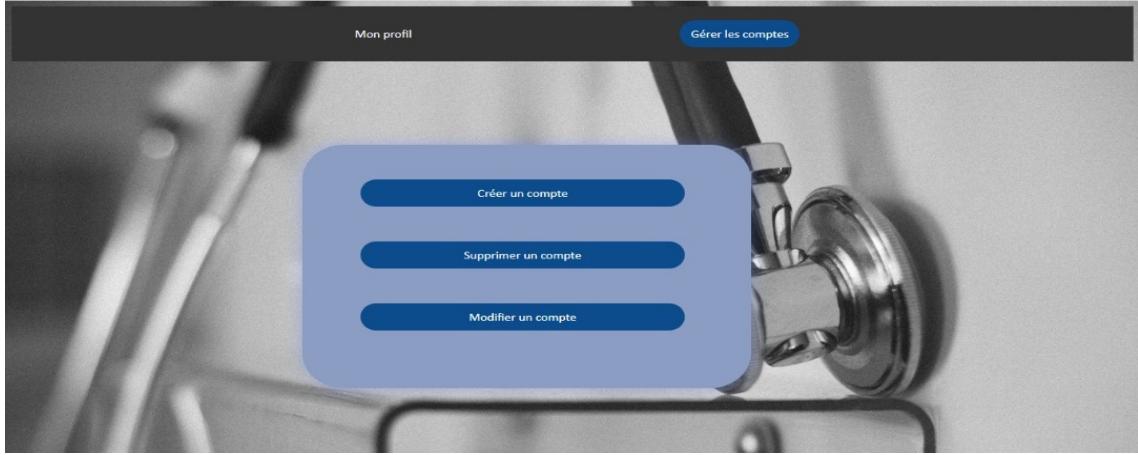
3.4.2 La page de l'administrateur de l'hôpital

Notre application web est gérée par des administrateurs, chaque hôpital possède un administrateur qui aura comme fonctionnalité l'ajout, la suppression ou la modification d'un compte.

Dans le cas où l'authentification réussie, la page du profil de notre administrateur hôpital apparaîtra comme suit :



En appuyant sur le bouton "Gérer les comptes", l'administrateur sera orienté vers un menu :



- Si l'utilisateur choisit l'option "création d'un nouveau compte", un formulaire lui sera affiché afin de remplir toutes les informations nécessaires :

Création d'un nouveau compte !

Introduisez un nom

Introduisez un prenom

Introduisez un email

Introduisez un mot de passe

Introduisez un numéro de téléphone

Choisissez une fonction

jj / mm /aaaa

Créer le compte

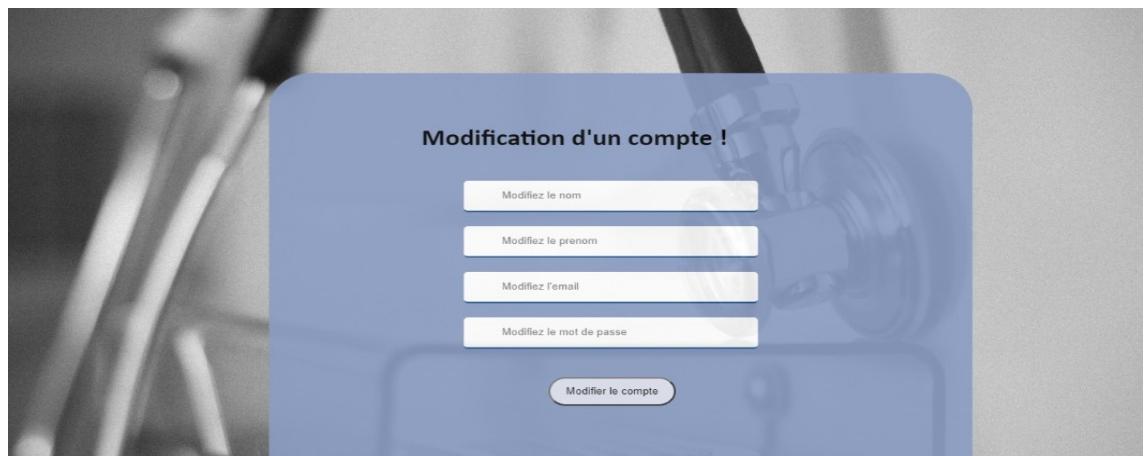
Le mot de passe introduit par l'administrateur sera crypté avec la fonction d'hachage pour être insérer dans la base de données:

	<input type="checkbox"/> Edit	<input type="checkbox"/> Copy	<input type="checkbox"/> Delete	idMedecin	email	nomUser	mdp	Nom	Prenom	
<input type="checkbox"/>	<input type="checkbox"/> Edit	<input type="checkbox"/> Copy	<input type="checkbox"/> Delete	13	ishakamine@gmail.com		\$2y\$10\$uDnFqwgIB7eowi6pBQnvO5ePhUZP1UPOZJ3icZX7iK...	AMINE	Ishak	778
<input type="checkbox"/>	<input type="checkbox"/> Edit	<input type="checkbox"/> Copy	<input type="checkbox"/> Delete	14	benabedanfel@gmail.com		\$2y\$10\$cjM0ErfIILuiXLvQVhCA/deSCb5yMF1fnAzwR38hY9Xh...	BENABED	Anfel	554
<input type="checkbox"/>	<input type="checkbox"/> Edit	<input type="checkbox"/> Copy	<input type="checkbox"/> Delete	15	saldracha@gmail.com		\$2y\$10\$M6mye6xGLOy6akEpilm.40XgvflLH7vcFjeGhcqnZ0...	SAID	Racha	775
<input type="checkbox"/>	<input type="checkbox"/> Edit	<input type="checkbox"/> Copy	<input type="checkbox"/> Delete	16	abdelbakiferiel@gmail.com		\$2y\$10\$q3LMF4tdGwOsVbcl.whAxeVcBE1J4rE/d4P8J/1MYl...	ABDELBAAKI	Feriel	554

- Par ailleurs, si ce dernier choisit l'option "Suppression d'un compte", il sera alors orienté vers une nouvelle page où il devra seulement remplir le champs de l'email pour que le compte soit supprimé :



- Enfin, si l'administrateur choisit l'option "Modification d'un compte", une nouvelle page lui sera ouverte qui demandera l'email correspondant au compte qu'il veut modifier et selon ce dernier, il sera orienté vers le formulaire correspondant :



3.4.3 La page du medecin

Une fois connecté le médecin sera directement dirigé vers son profil :

- Cas 01 :

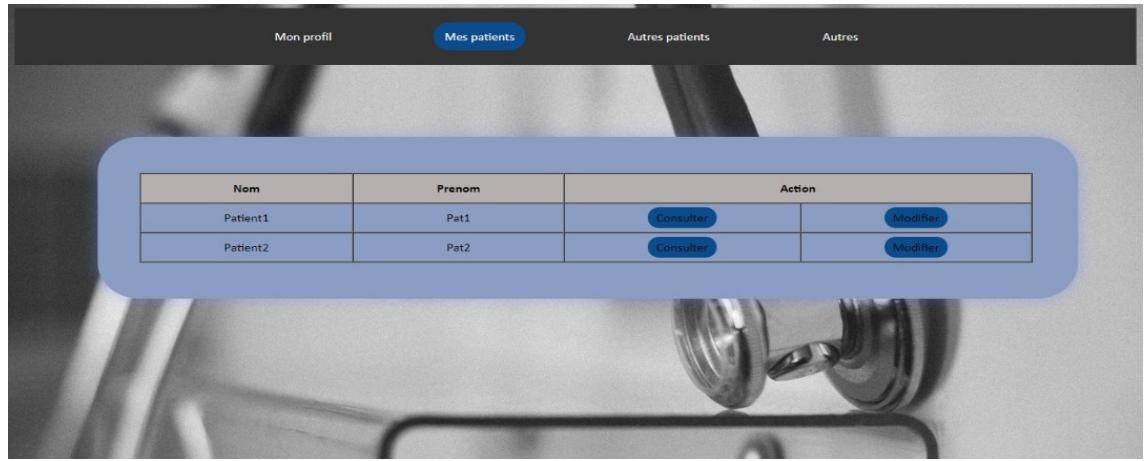


- Cas 02 :



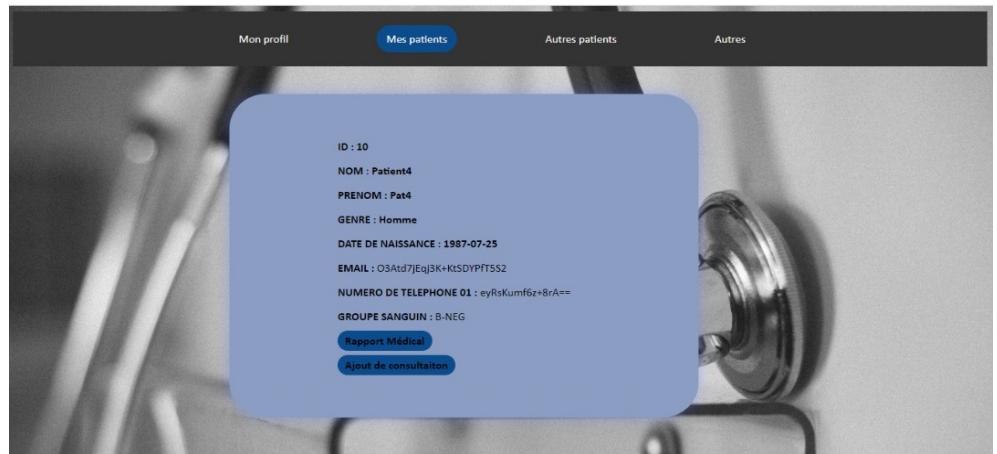
Il pourra par ailleurs, choisir une des différentes options qui lui sont proposées, entre consulter les informations personnelles ou médicales de ses patients et les modifier. Mais aussi, consulter ceux des patients externes (provenant du même service) et nous distinguons :

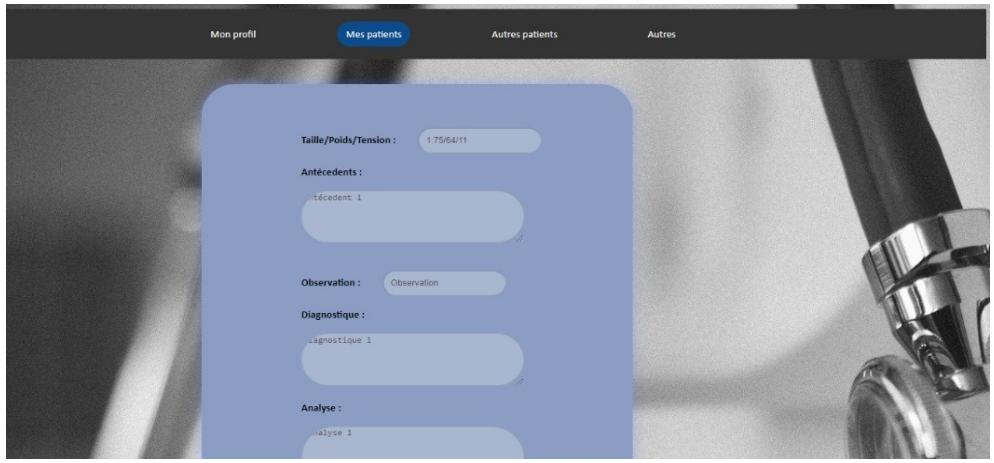
- **Mes patients** : Cette fenêtre contient un tableau de tous les patients du médecin avec deux possibilités :



- **Consulter** : Les informations personnelles du patient seront afficher avec un bouton qui le dérigera vers les informations médicales de ce dernier :

* Cas 01 :





* Cas 02 :

This screenshot shows a medical software interface. At the top, there are tabs: 'Mon profil' (My profile), 'Mes patients' (My patients) which is highlighted in blue, 'Autres patients' (Other patients), and 'Autres' (Others). Below the tabs, two blue callout boxes display patient information.

The top callout box (Patient 1) contains the following details:

- ID : 7
- NOM : Patient1
- PRENOM : Pat1
- GENRE : Homme
- DATE DE NAISSANCE : 1990-10-15
- EMAIL : O3Atd7jEqjRk+K1SDYPT552
- NUMERO DE TELEPHONE 01 : eyRsKuic6Dy/qw==
- NUMERO DE TELEPHONE 02 : eydsKumY7Tu4rg==
- GROUPE SANGUIN : O-POS
- Rapport Médical
- Ajout de consultation

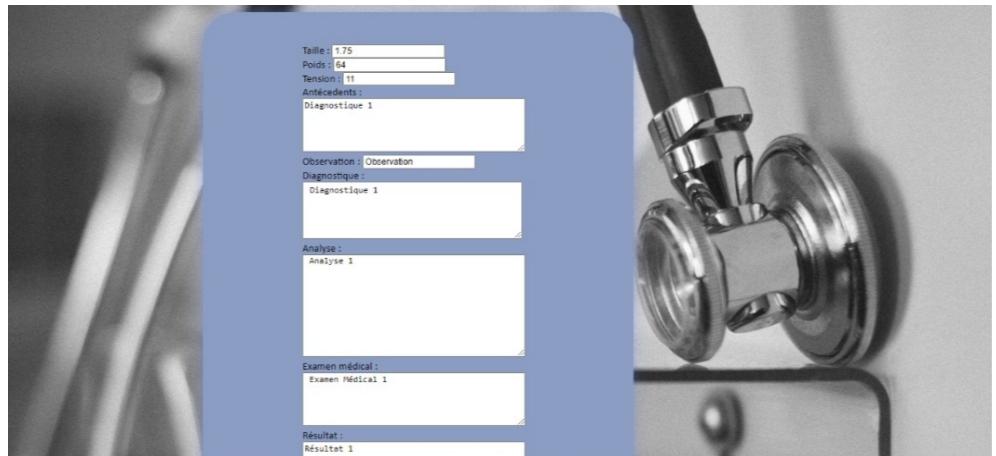
The bottom callout box (Patient 2) contains the following details:

- Taille/Poids : 1.72/65
- Tension : 9.8
- Maladies Chroniques : Malades Chroniques 1
- Observation : Observation
- Diagnostique : Diagnostique 1
- Analyses : Analyses 1

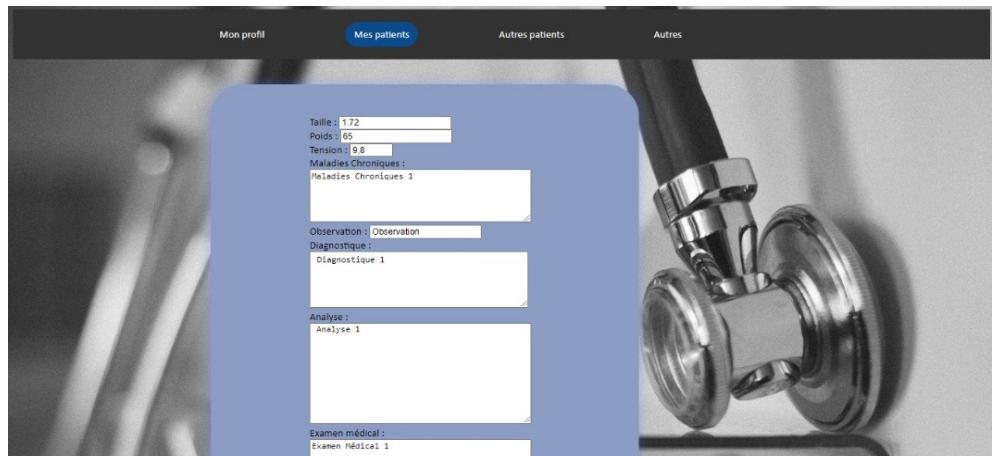
Remarque : Le rapport medical est d'abord décrypté avec la méthode AES avant de s'afficher à l'utilisateur.

- **Modifier :** La page des informations personnelles sera affichée sans aucune possibilité de modification mais en appuyant sur le bouton des informations médicales, un formulaire lui sera assigné afin de pouvoir les modifier :

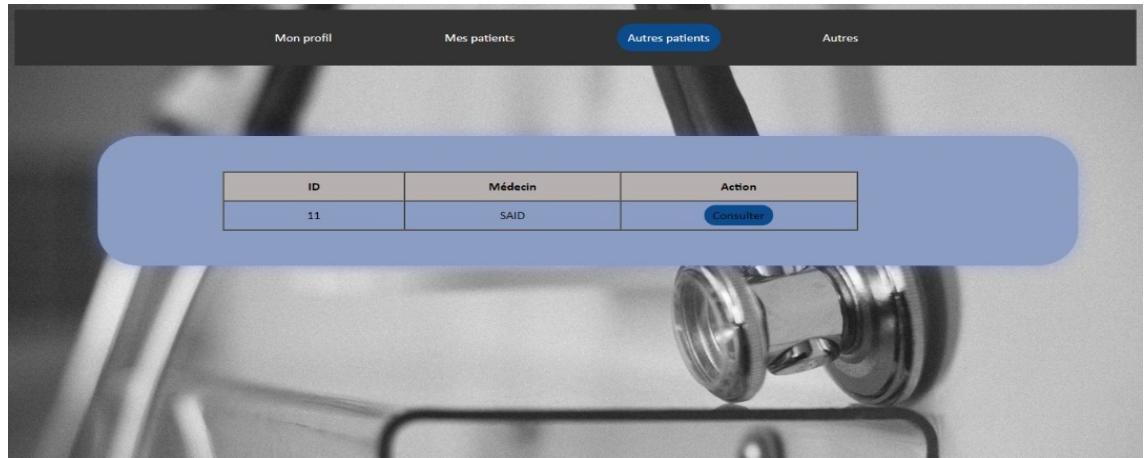
* Cas 01 :



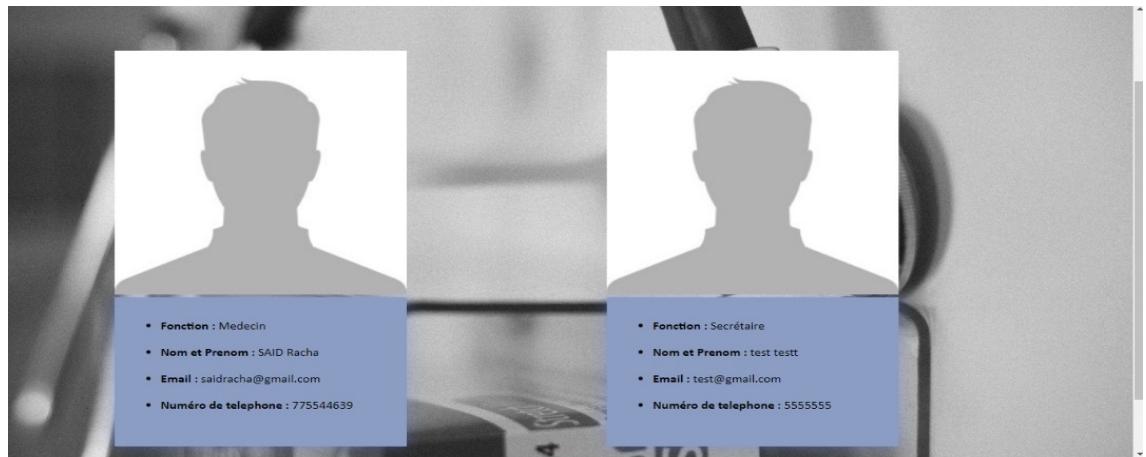
* Cas 02 :



- **Autres Patients :** Cette fenêtre contient un tableau de tous les patients externes à ce médecin mais du même service avec une possibilité de consultation du rapport medical seulement :



- **Autres** : En appuyant sur ce bouton, le medecin pourra voir les fiches des membres de son service :



3.4.4 La page de la secrétaire

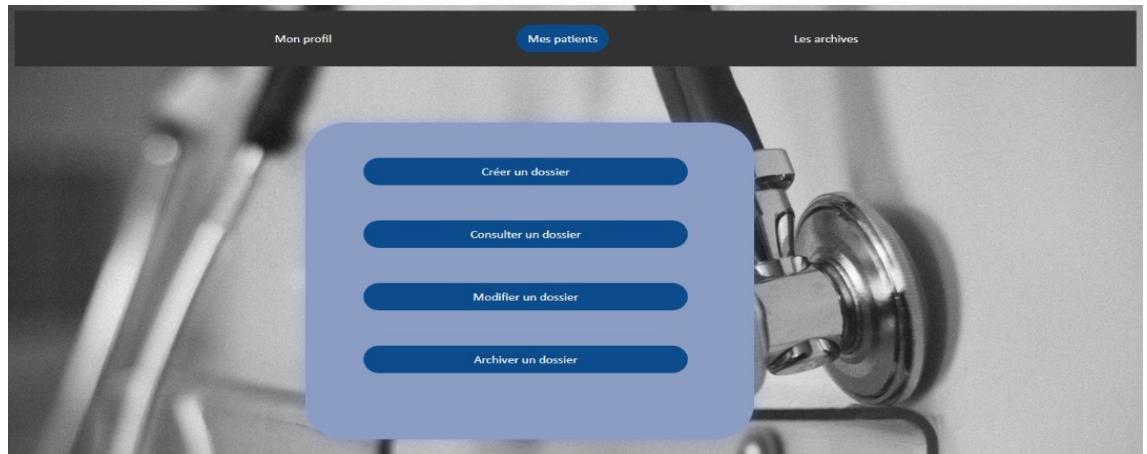
Pour chaque service d'un hôpital, il existe au moins une secrétaire, celle-ci pourra ajouter, consulter, modifier les informations personnelles des patients de son service ainsi qu'archiver un dossier.

Dans le cas où l'authentification réussie, une page du profil correspondant à la secrétaire apparaitra :



Nous distinguons para ailleurs, deux autres boutons :

- **Mes patients** : En cliquant sur ce bouton, une page contenant un menu apparaîtra :



La secrétaire alors aura libre choix de choisir l'option qu'elle voudra :

- **Créer un nouveau dossier** : Un formulaire de création sera affiché:

* Cas 01 :



A screenshot of a web-based patient registration form. The form fields include:

- Name :
- Prenom :
- Genre :
 - Homme
 - Femme
- Date de naissance : (35/nm/aaaa)
- Email :
- Numéro de téléphone 01 :
- Numéro de téléphone 02 :
- Email du médecin traitant :

* Cas 02 :

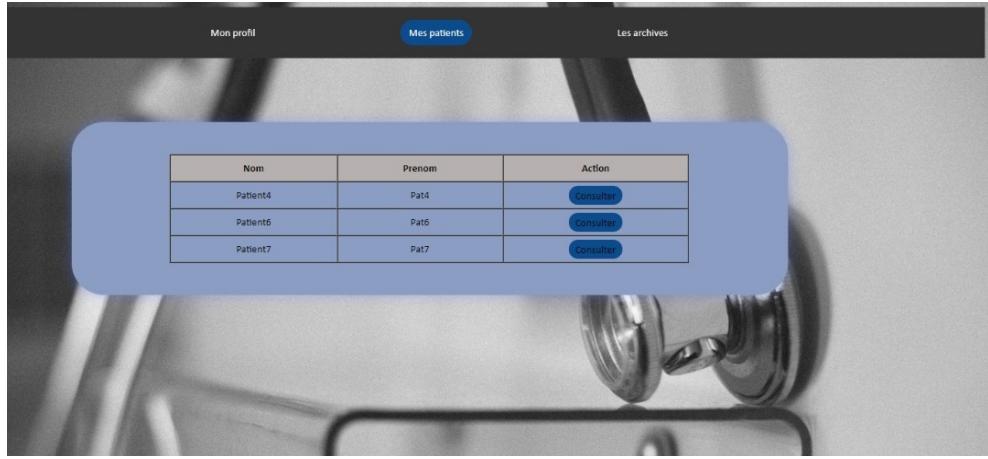


A screenshot of a web-based patient registration form titled "Création d'un nouveau dossier !". The form fields include:

Création d'un nouveau dossier !

- Name : Patient7
- Prenom : Pat7
- Genre :
 - Homme
 - Femme
- Date de naissance : 15/06/1975
- Email : patient7@gmail.com
- Numéro de téléphone 01 : 0776855445
- Email du médecin traitant :

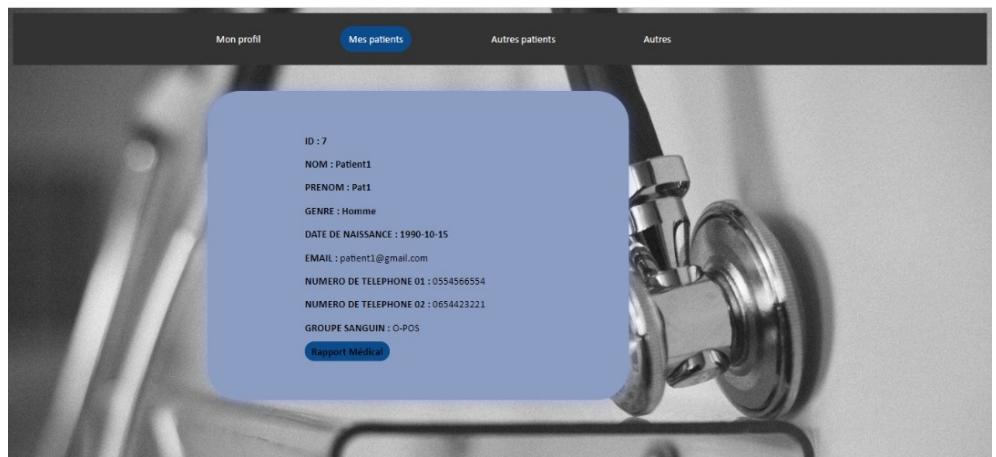
- **Consulter un dossier :** Une nouvelle page apparaitra contenant tous les patients de son service et elle pourra consulter le dossier qu'elle voudra en appuyant sur le bouton "consulter" :

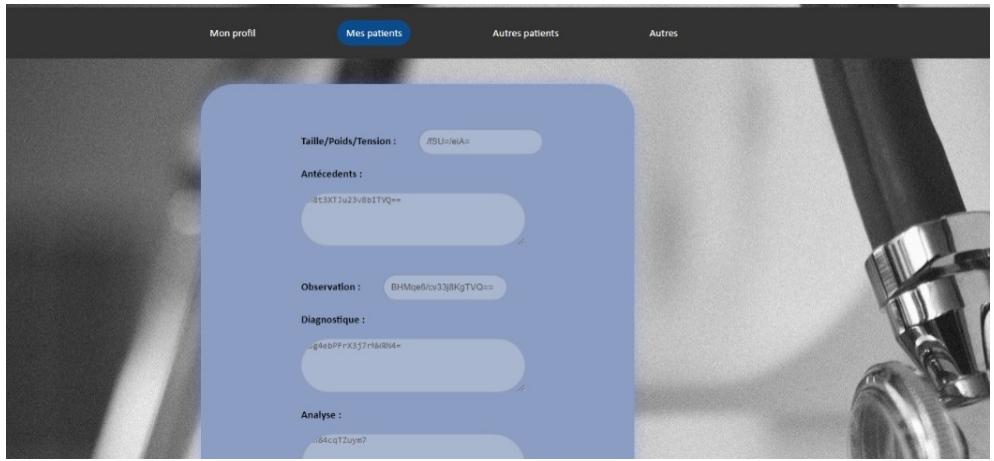


En appuyant sur le bouton "consulter", la secrétaire sera dirigée vers les informations personnelles des patients et en appuyant sur le boutons "", elle sera dirigée vers une autre fenêtre afin de consulter les informations médicales des patients :

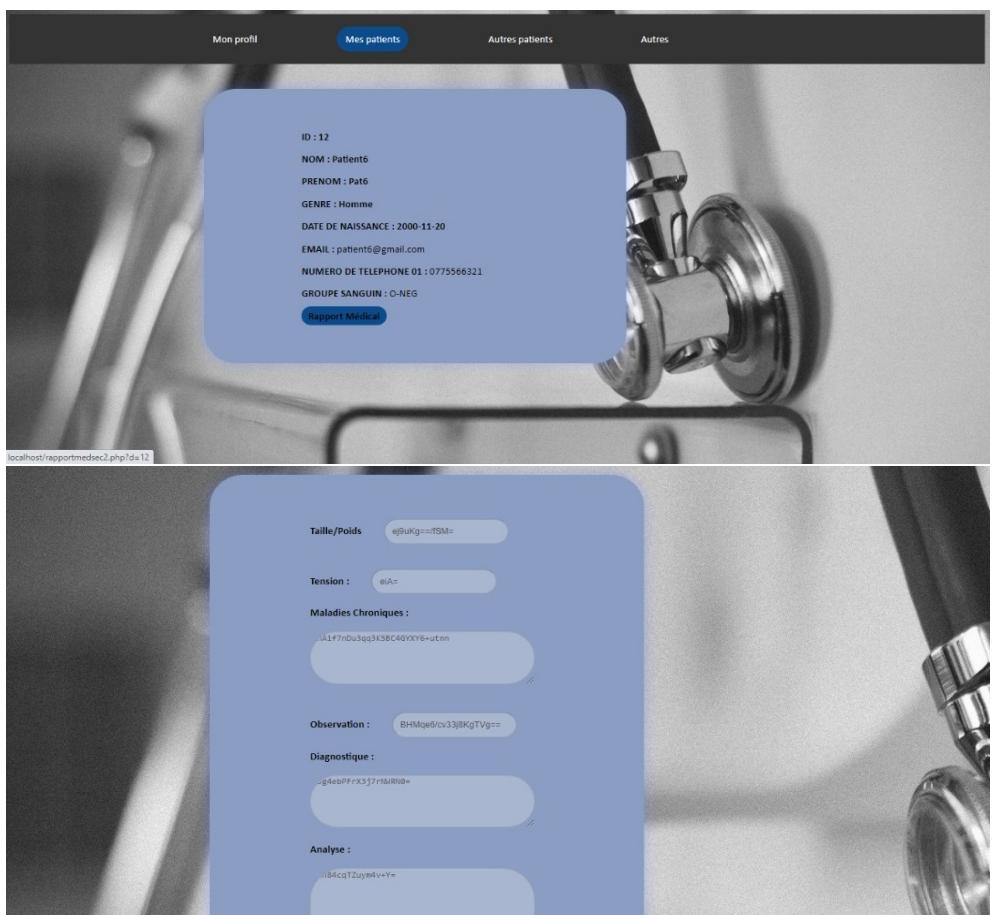
Remarque : Dans la consultation du rapport medical, la secrétaire recevra des données crypté avec la méthode AES.

* Cas 01 :





* Cas 02 :



- **Modifier un dossier :** Un formulaire de modification de dossier sera ouvert mais seulement les informations personnelles :

* Cas 01 :

PRENOM : Pat1
GENRE :
Homme

DATE DE NAISSANCE : 1990-10-15
EMAIL :
patient1@gmail.com

NUMERO DE TELEPHONE 01 :
0554566554

NUMERO DE TELEPHONE 02 :
0654423221

GROUPE SANGUIN :
O-POS
Médecin en charge :
ishakamine@gmail.com
Enregistrer la modification Annuler

* Cas 02 :

Mon profil Mes patients Les archives

NOM : Patient4
PRENOM : Pat4
GENRE :
Homme

DATE DE NAISSANCE : 1987-07-25
EMAIL :
patient4@gmail.com

NUMERO DE TELEPHONE 01 :
0554455563

GROUPE SANGUIN :
B-NEG
Médecin en charge :
benabedanfel@gmail.com
Enregistrer la modification Annuler

- **Archiver un dossier :** En cas de guerrison, de mort..etc, le dossier du patient correspondant pourra etre archiver et cela en appuyant sur le bouton "archiver" :

Mon profil Mes patients Les archives

ID	Nom	Prenom	Action
10	Patient4	Pat4	Archiver le dossier
12	Patient6	Pat6	Archiver le dossier
13	Patient7	Pat7	Archiver le dossier

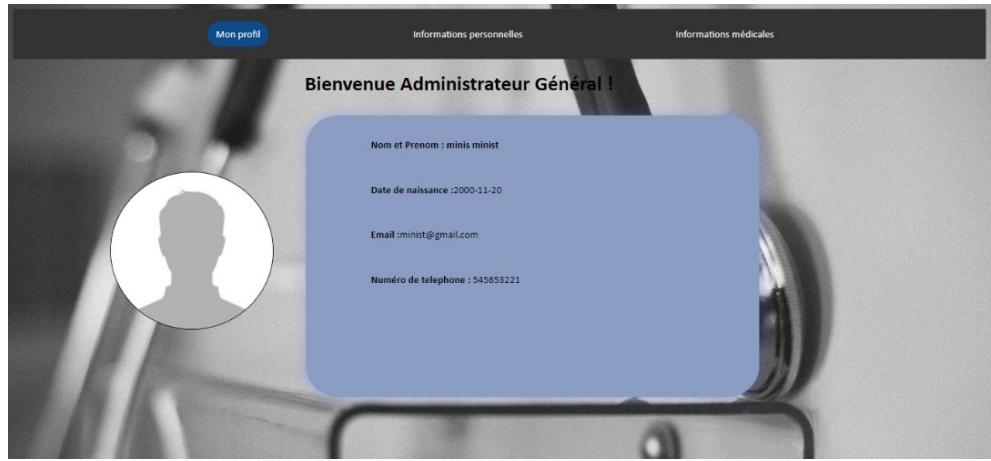
- **Les archives :** Une nouvelle page s'affiche qui contient tous les dossiers qui ont été archivé avant un bouton "désarchiver" en cas d'erreur :

Mon profil Mes patients Les archives

ID	Nom	Prenom	Action
10	Patient4	Pat4	Désarchiver le dossier

3.4.5 La page de l'administrateur Général

L'administrateur général, autrement appelé le ministère sera dirigé comme chaque utilisateur de l'application vers son profil :



Il pourra par ailleurs, choisir une des différentes options qui lui sont proposées, entre consulter les informations personnelles des patients et consulter les informations médicales des patients et nous distinguons :

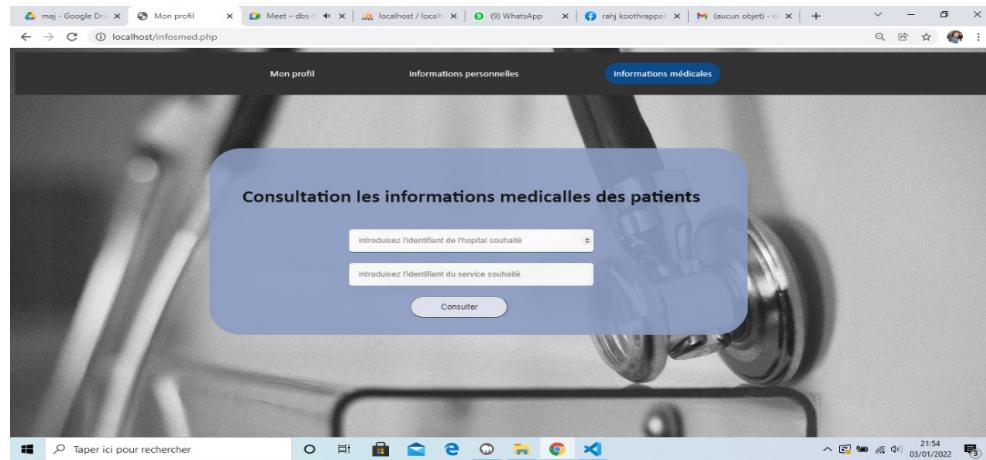
- **Consulter les informations personnelles des patients :** Un formulaire lui sera alors affiché afin de remplir l'ID de l'hôpital ainsi que celui du service correspondant au patient :



Une fois les champs remplis, il sera alors dirigé vers la page où il pourra choisir le dossier personnel du patient voulu pour le consulter :

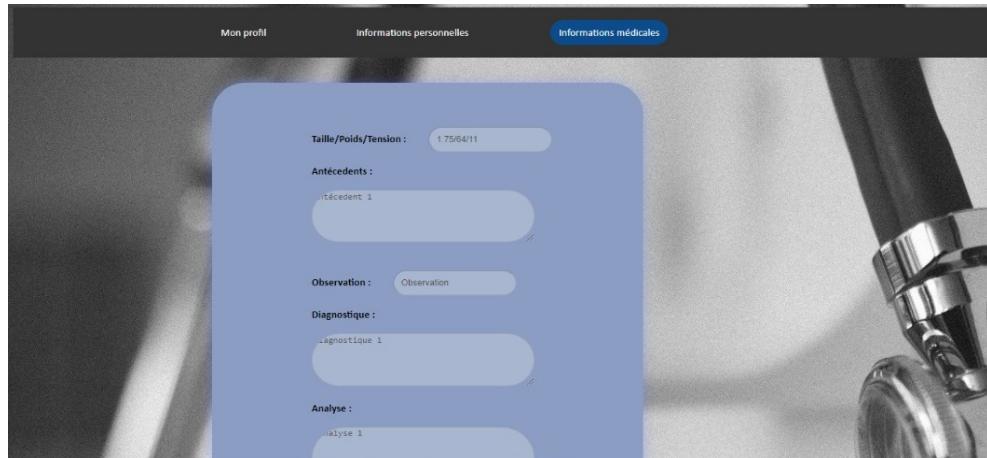


- **Consulter les informations médicales des patients :** Un formulaire lui sera alors affiché afin de remplir l'ID de l'hôpital ainsi que celui du service correspondant au patient :



Une fois les champs remplis, il sera alors dirigé vers la page où il pourra choisir le dossier medical du patient voulu pour le consulter :





Remarque : Le rapport medical est d'abord décrypté avec la méthode AES avant de s'afficher à l'utilisateur.

3.5 Description des fenêtres du logiciel

3.5.1 Authentification

Lors du lancement de notre application, une interface d'accueil apparaîtra, celle-ci permettra à l'utilisateur de s'authentifier en introduisant les informations de son compte (son email, sa date de naissance ainsi que son mot de passe) enregistrées dans notre base de données. Selon sa fonction, l'application l'orientera vers ses fonctionnalités.



-Dans le cas où l'utilisateur ne remplit pas tous les champs requis dans notre interface d'accueil, une alerte se déclenchera.



-Dans le cas où l'utilisateur introduit un email, une date de naissance ou encore un mot de passe incorrect, une alerte se déclenchera.



Dans le cas où l'utilisateur se trompe en choisissant sa fonction dans la choice-box, une alerte se déclenchera.



3.5.2 Fenêtres de l'administrateur

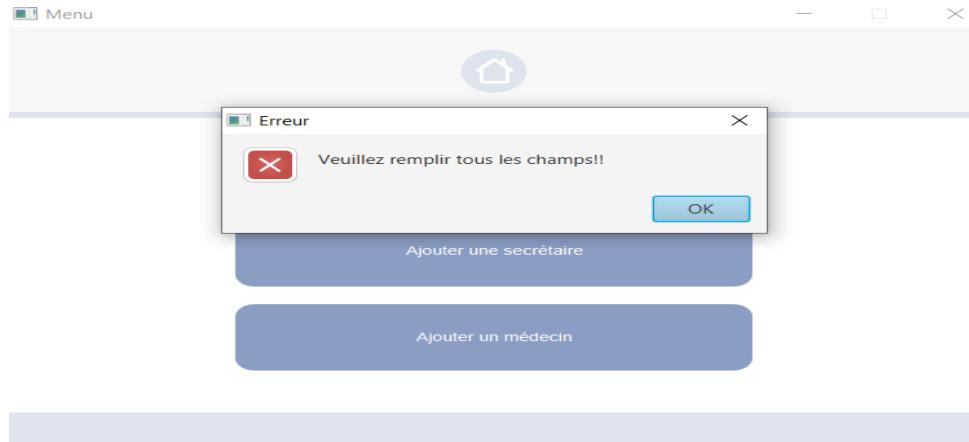
Notre application est gérée par des administrateurs, chaque hôpital possède un administrateur qui aura comme fonctionnalité l'ajout d'une secrétaire ou d'un médecin dans le service qu'il souhaite.

Dans le cas où l'authentification réussie, le menu principal apparaitra :



L'administrateur de l'hôpital en question pourra ainsi ajouter une secrétaire ou un médecin dans le service souhaité. **a. Ajout secrétaire**

S'il clique sur le bouton « Ajouter une secrétaire » sans introduire l'identifiant du service souhaité, une alerte se déclenchera.



Sinon, la fenêtre courante du menu se fermera et celle de l'inscription de la secrétaire se lancera.



Afin de garantir l'intégrité des données un certain nombre de conditions doivent être respectées.

-L'administrateur doit entrer toutes les informations nécessaires au remplissage de la base de donnée, autrement l'inscription est annulée et une alerte est déclenchée.



-Le mot de passe introduit et sa confirmation doivent être équivalente, autrement l'inscription est annulée et une alerte est déclenchée.



Si toutes les conditions sont vérifiées, un message de confirmation se lancera.



Le mot de passe de la secrétaire introduit par l'administrateur sera crypté avec le chiffrement asymétrique RSA pour être insérer dans la base de données.

Les données de la secrétaire une fois l'inscription effectuée seront vu dans la base de données comme ceci :

email	nomUser	mdp	datenaiss	idService	idHopital
amel.foudil@gmail.com	amel.foudil	[B@7d9846bb	2001-12-12	5	4
asma.chemem@gmail.com	asma.chemem	[B@14f26518	2000-12-18	6	4
benabedmaissa23@gmail.com	maissa.benabed	[B@470f25a5	2000-12-22	2	2
boukersi.yasmine@gmail.com	boukersi.yasmine	[B@1723c753	2000-12-17	8	3
feriel.abdelbaki23@gmail.com	feriel.abdelbaki	[B@43073791	2000-12-23	1	1
kherroubi.kenza@gmail.com	kherroubi.kenza	[B@22c49bf0	2000-12-10	7	3
racha.said25@gmail.com	racha.said	[B@2a375c7d	2000-11-09	3	1
yacef.yasmina@gmail.com	yasmina.yacef	[B@7f72451c	2000-12-09	4	2

a. Ajouter un médecin

Si l'administrateur clique sur le bouton « Ajouter un médecin » la fenêtre courante du menu se fermera et celle de l'inscription du médecin se lancera.



Les mêmes conditions que ceux vu dans le cas de l'ajout de la secrétaire doivent être vérifiées, si c'est le cas un message de confirmation se lancera.



Le mot de passe du médecin introduit par l'administrateur sera crypté avec le chiffrement symétrique AES pour être insérer dans la base de données.

3.5.3 Fenêtres de la secrétaire

Pour chaque service d'un hôpital, il existe au moins une secrétaire, celle-ci pourra ajouter ou consulter les informations personnelles des patients de son service.

Dans le cas où l'authentification réussie, un menu principal apparaitra.

Le menu en question dépend de la wilaya où se trouve l'hôpital où elle travaille, comme le montre le code suivant :

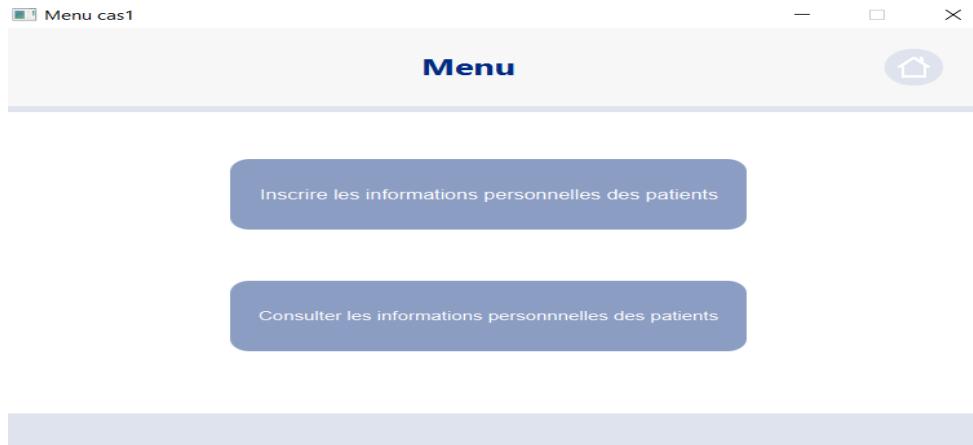
```

if(fonction.getValue().equals("Secrétaire"))
{
    ResultSet myRs3 = myStmt.executeQuery("SELECT wilaya, s.idHopital, s.idService FROM Secrétaire s, Hopital
    if(myRs3.next()){
        idH_Secrétaire = myRs3.getInt("idHopital");
        idS_Secrétaire = myRs3.getInt("idService");
        wilaya = myRs3.getInt("wilaya");

        //Cas 1 : 1<=Wilaya<=29
        //Cas 2 : 30<=Wilaya<=58
        if(wilaya<=29){
            Main.stage.close();
            Parent parent = FXMLLoader.load(getClass().getResource("Menu2Secrétaire_cas1.fxml"));
            Scene scene = new Scene(parent);
            Stage stage = new Stage();
            stage.setScene(scene);
            stage.show();
            stage.setResizable(false);
            Main.stage = stage;
            stage.setTitle("Menu cas1");
        }
        else{
            Main.stage.close();
            Parent parent = FXMLLoader.load(getClass().getResource("Menu2Secrétaire_cas2.fxml"));
            Scene scene = new Scene(parent);
            Stage stage = new Stage();
            stage.setScene(scene);
            stage.show();
            stage.setResizable(false);
            Main.stage = stage;
            stage.setTitle("Menu cas2");
        }
    }
}

```

Premier cas : $1 \leq \text{Wilaya} \leq 29$ (Dans l'exemple suivant notre secrétaire a été créée par l'administrateur de l'hôpital de Mustapha Pacha qui se trouve à Alger (16) au service de cardiologie).



a.Inscrire les informations personnelles des patients

Si la secrétaire clique sur le bouton « Incrire les informations personnelles des patients » la fenêtre courante du menu se fermera et celle de l'inscription des patients se lancera.

Ajouter un patient

Hôpital : Mustapha Pacha Service : Cardiologie **Inscription d'un patient**

Nom _____ Prénom _____
Date de naissance _____

Téléphone 1 _____ Téléphone 2 _____
Groupe Sanguin _____
Genre _____

Nom du médecin _____ Prénom du médecin _____

Afin de garantir l'intégrité des données un certain nombre de conditions doivent être respectées.

-La secrétaire doit entrer toutes les informations nécessaires au remplissage de la base de donnée, autrement l'inscription est annulée et une alerte est déclenchée.

Ajouter un patient

Hôpital : Mustapha Pacha Service : Cardiologie **Inscription d'un patient**

Menacer _____ Mina _____
08/12/1993 _____

Amara _____ Okba _____

Erreur
Veuillez remplir tous les champs!!

-La secrétaire doit entrer un médecin existant dans son service, autrement l'inscription est annulée et une alerte est déclenchée.



Si toutes les conditions sont vérifiées, un message de confirmation se lancera.



b.Consulter les informations personnelles des patients

Si la secrétaire clique sur le bouton « Consulter les informations personnelles des patients » la fenêtre courante du menu se fermera et celle de la consultation de la liste des patients se lancera.

Consulter les informations personnelles des patients

Liste des patients

Nom	Prénom	Téléphone 1	Téléphone 2	Nom du méde...	Prénom du méde..
Abbad	Farid	0778969878	0558787859	Amara	Okba
Arab	Redouane	0775414578	0775787777	Amara	Okba
Bekkar	Maroua	0665478958	0687598598	Amara	Okba
Menacer	Mina	0770101021	0552112587	Amara	Okba

[Consulter en détail](#)

Pour consulter toutes les informations personnelles du patient, la secrétaire choisi un patient en sélectionnant une ligne du tableau puis clique sur « Consulter en détail ».

Consulter les informations personnelles des patients

Liste des patients

Nom	Prénom	Téléphone 1	Téléphone 2	Nom du méde...	Prénom du méde..
Abbad	Farid	0778969878	0558787859	Amara	Okba
Arab	Redouane	0775414578	0775787777	Amara	Okba
Bekkar	Maroua	0665478958	0687598598	Amara	Okba
Menacer	Mina	0770101021	0552112587	Amara	Okba

[Consulter en détail](#)

Consulter les informations personnelles du patient

Hôpital : Mustapha Pacha **Service :** Cardiologie

Informations personnelles du patient

Menacer	Mina
08/12/1993	
0770101021	0552112587
O-POS	
Femme	
Amara	Okba

Deuxième cas : 30<=Wilaya<=58 (Dans l'exemple suivant notre secrétaire a été créée par l'administrateur de l'hôpital de Lakhdar Bouchama qui se trouve à Tipaza (42) au service de pédiatrie).

Menu cas2

Menu

Inscrire les informations personnelles des patients
Consulter les informations personnelles des patients

Si la secrétaire clique sur le bouton « Incrire les informations personnelles des patients » la fenêtre courante du menu se fermera et celle de l'inscription des patients se lancera.

Ajouter un patient

Hôpital : Lakhdar Bouchama **Inscription d'un patient**

Service : Pédiatrie

Nom	Prénom
Téléphone	Date de naissance
Groupe Sanguin	Email
Genre	
Nom du médecin	Prénom du médecin

La secrétaire introduit les informations du patient :

Ajouter un patient

Hôpital : Lakhdar Bouchama **Inscription d'un patient**

Service : Pédiatrie

Ziane	Sarah
0557878989	02/07/2012
A-POS	sarah.ziane@gmail.com
Femme	
Yamoun	Rachid

Les mêmes conditions que ceux vu dans le cas 1 doivent être vérifiées, si c'est le cas un message de confirmation se lancera.



Si la secrétaire clique sur le bouton « Consulter les informations personnelles des patients » la fenêtre courante du menu se fermera et celle de la consultation de la liste des patients se lancera.

Nom	Prénom	Téléphone	Email	Nom du médecin	Prénom du médecin
Abbas	Mounir	0557896589	abas.mounir@g...	Yamoun	Rachid
Akil	Amine	0775245787	akil.amine@g...	Yamoun	Rachid
Aouchiche	Sarah	0778789885	aouchiche.sara...	Yamoun	Rachid
Zenir	Yacine	0557789685	zenir.yacine@g...	Yamoun	Rachid
Ziane	Sarah	0557878989	sarah.ziane@g...	Yamoun	Rachid

Pour consulter toutes les informations personnelles du patient, la secrétaire choisit un patient en sélectionnant une ligne du tableau puis clique sur « Consulter en détail ».

Consulter les informations personnelles des patients

Hôpital : Lakhdar Boucham
Service : Pédiatrie

Liste des patients

Nom	Prénom	Téléphone	Email	Nom du médicin	Prénom du médicin
Abbas	Mounir	0557896589	abas.mounir@...	Yamoun	Rachid
Akil	Amine	0775245787	akil.amine@g...	Yamoun	Rachid
Aouchiche	Sarah	0778789885	aouchiche.sara...	Yamoun	Rachid
Zenir	Yacine	0557789685	zenir.yacine@g...	Yamoun	Rachid
Ziane	Sarah	0557878989	sarah.ziane@g...	Yamoun	Rachid

[Consulter en détail](#)

Consulter les informations personnelles du patient

Hôpital : Lakhdar Boucham
Service : Pédiatrie

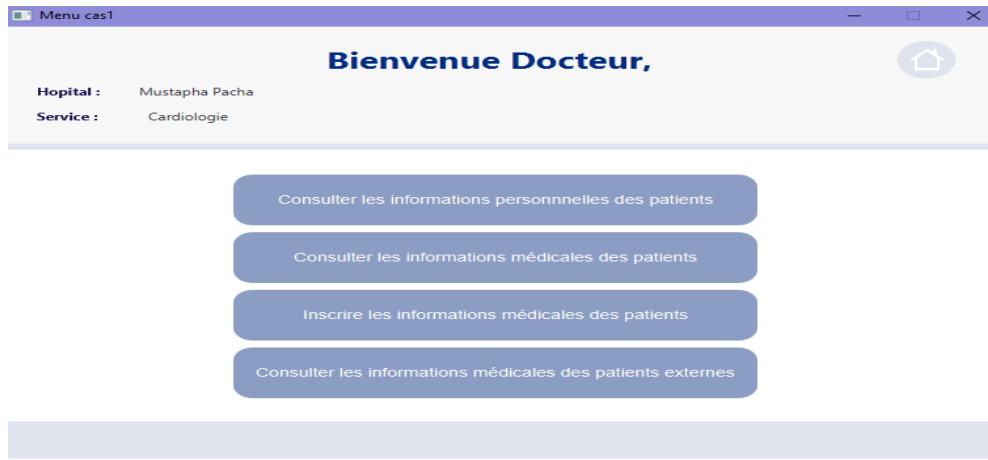
Informations personnelles du patient

Ziane	02/07/2012	Sarah
0557878989	sarah.ziane@gmail.c...	
A-POS	Femme	Rachid
Yamoun		

3.5.4 Fenêtres du médecin

a. Accueil

Une fois connecté, le médecin peut choisir une des différentes options qui lui sont proposées, entre consulter les informations personnelles ou médicales de ses patients, ajouter une nouvelle consultation ou encore examiner les informations médicales de patients externes (provenant d'un autre service ou hôpital). Il lui est également proposé (comme dans toutes les autres fenêtres) un bouton « Home » qui lui permettra de se déconnecter de sa session soit, revenir à la fenêtre d'authentification. Il est à noté que le nom de l'hôpital ainsi que le service auquel il appartient sont affichés également.



b. Consultation des informations personnelles des patients

Dans cette fenêtre sont affichés les données personnelles relatives à chaque patient du médecin connecté. Comme mentionné dans la présentation du projet, en fonction l'hôpital auquel appartient le médecin il existe un affichage différent des fenêtres de chaque fonctionnalité. Afin d'illustrer cette problématique, nous présentons deux cas d'affichage pour chaque fonctionnalité.

Premier cas :

Nom	Prénom	Téléphone 1	Téléphone 2	Nom du médecin	Prénom du médecin
Abbad	Farid	0557896525	0775896582	Amara	Okba
Abizar	Kamel	0778896525	0556892512	Amara	Okba
Arab	Redouane	0667589652	0552568957	Amara	Okba
Ladlani	Lydia	0778788747	0757874785	Amara	Okba

Deuxième cas :

Nom	Prénom	Téléphone	Email	Nom du médecin	Prénom du médecin
Abid	Imene	0773488652	abd.imene@gmail.com...	Nadir	Mohamed
amine	ishak	0667896589	amine.ishak@gmail.com...	Nadir	Mohamed
Atrouche	Hind	0557412365	atrouche.hind@gmail...	Nadir	Mohamed

Nous pouvons remarquer que les données personnelles de l'hôpital « Mustapha Pacha » sont représentés sous forme de tableau avec certaines colonnes différentes par rapport à ceux du « CNMS » comme la présence de deux numéros de téléphone au lieu d'un seul.

c. Consultation des informations médicales des patients

Dans cette fenêtre sont affichés les données médicales décryptés de la base de donnée par l'algorithme AES. Ces données sont relatives à chaque patient du médecin connecté. Tout comme la fenêtre précédente il existe deux cas différents pour cette fonctionnalité. Premier cas :

Informations médicales							
identifiant du patient		identifiant de la consultation					
Nom	Prénom	date consultation	Groupe sanguin	Taille	Poids	Observation	
Abbad	Farid	2021-12-29	O-POS	185	82	état stable	
Abizar	Kamel	2021-12-29	O-POS	190	78	Asthme sévère sous ...	
Abbad	Farid	2021-12-29	O-POS	185	82	état critique	
Ladlani	Lydia	2021-12-29	O-POS	162	59	Grossesse stable	

deuxième cas :

Nom	Prénom	Date consultation	Groupe sanguin	Tension	Diagnostique
Abid amine	Imene ishak	2021-12-29	O-POS	12 / 8	pression artérielle systolique pression artérielle diastolique

[Consulter en détail](#)

Comme nous pouvons le constater les deux cas présente la possibilité de faire une recherche en fonction de l'identifiant du patient ou identifiant de la consultation ainsi que la possibilité de consulter en détail les informations médicales. Néanmoins, il existe certaines différences comme l'affichage de la tension artérielle des patients dans le cas de l'hôpital « CNMS » à la différence de « Mustapha Pacha » qui lui affiche la taille ou encore le poids des patients.

d. Consultation en détail des informations médicales

Il est possible pour un médecin de consulter en détail chaque consultation faite en mentionnant l'identifiant de la consultation souhaitée puis en cliquant sur le bouton « consulter en détail » présent dans chacune des fenêtres de la fonctionnalité précédente. Afin de permettre cet affichage, les données sont décryptées de la base de données par l'algorithme AES puis exposés à l'écran.

Premier cas :

Antécédents		Analyse		Résultat	
infection chronique par le virus de l'hépatite B	opération de la vésicule biliaire	Abbad	185	Cm	Farid
		O-POS			82 Kg
					état stable

Deuxième cas :

Maladies Chroniques		Abid	Imene
Infection chronique par le virus de l'hépatite C			
bronchite chronique		O-POS	
vitiligo		12	cmHg
pression artérielle systolique			
Analyse	Résultat	Commentaire	
Chlamydia Trachomatis	resultat Chlamydia Trachomatis	commentaire Chlamydia Trachomatis	
Hépatite C	resultat Hépatite C	commentaire Hépatite C	

Comme le montre les fenêtres il existe certaines différences comme l'affichage maladies chroniques des patients dans le cas de l'hôpital « CNMS » à la différence de « Mustapha Pacha » qui lui affiche les antécédents des patients et uniquement les analyses et résultats des examens sans les commentaires du médecin.

e. Incrire les informations médicales des patients

L'application offre la possibilité au médecin d'ajouter de nouvelles consultations. Pour ce faire il lui est demandé de préciser l'identifiants du patient concerné puis remplir les champs de saisis affichés. Un message de confirmation est affiché lors de l'ajout de chaque consultation. De plus, les données enregistrées sont automatiquement cryptés par l'algorithme AES puis stockés dans la base de donnée nationale. **Premier cas :**

Antécédents		identifiant du patient	
		Taille	Cm
		Poids	Kg
Observation			
Résultat	Analyse		

Deuxième cas :

The screenshot shows a Windows application window titled "Inscrire informations médicales". At the top, it displays "Hopital : CNMS" and "Service : Chirurgie Cardio-Vasc". The main interface consists of several input fields and tables. On the left, there's a table for "Maladies Chroniques" (Chronic Diseases) with empty rows. To its right are fields for "identifiant du patient" (Patient ID), "Tension cmHg" (Blood Pressure in cmHg), and "Diagnostique" (Diagnosis). Below these are two tables: one for "Examens médicaux" (Medical Exams) and another for "Résultats" (Results) and "Commentaires" (Comments). Both tables have empty rows. At the bottom of the window is a "Valider" (Validate) button.

f. Consulter les informations médicales des patients externes

Il est possible pour un médecin de consulter les informations médicales de patients provenant d'autres services ou/et hôpitaux, il lui suffit uniquement de préciser l'identifiant de ces deux derniers.

The screenshot shows a Windows application window with a blue header bar. The main area contains the text "Veuillez introduire :" followed by two input fields, each with the number "1" typed into it. Below the input fields is a blue "Valider" (Validate) button. The entire window has a light gray background.

Néanmoins, afin de préserver la confidentialité des données des patients, un contrôle d'accès est appliqué tel que l'identité (le nom et prénom) des patients est masqué à l'affichage. Ainsi, seuls certaines informations médicales sont décryptées puis affichés à l'écran.

The screenshot shows a software window titled "Informations médicales". At the top, it displays "Hopital : Mustapha Pacha" and "Service : Cardiologie". Below this is a table with columns: Date consultation, Groupe sanguin, Taille, Poids, and Observation. The table contains six rows of data, with the last two rows being highlighted in grey. A search bar labeled "identifier du patient" and a "Consulter en détail" button are also visible.

Date consultation	Groupe sanguin	Taille	Poids	Observation
2021-12-29	O-POS	185	82	état stable
2021-12-29	O-POS	190	78	Asthme sévère sous traitement continu
2021-12-29	O-POS	185	82	état critique
2021-12-29	O-POS	162	59	Grossesse stable
2021-12-29	O-POS	158	49	Tachycardie induite par une arythmies
2021-12-29	O-POS	158	44	Stabilisation de son état

A la différence de la fenêtre affichée pour le médecin traitant les données présentés dans le tableau concernent les patients de tout le service sélectionné. Ainsi, contrairement au premier cas de consultation des informations médicales, le tableau comprend **deux dernières lignes supplémentaires** (données enregistrées par d'autres médecins du service).

g. Consulter en détail les informations médicales des patients externes

Il est également possible de consulter les informations médicales en détails, en cliquant sur le boutons « consulter en détail ». Comme mentionné précédemment, l'identité du patient est masquée. **Premier cas :**

The screenshot shows a software window titled "Détails informations médicales". It displays "Hopital : Mustapha Pacha" and "Service : Cardiologie". On the left, there is a section for "Antécédents" listing "infection chronique par le virus de l'hépatite B" and "opération de la vésicule biliaire". On the right, it shows physical measurements: "185 Cm" and "82 Kg", both with "O-POS" and "état stable" below them. At the bottom, there is a table comparing "Analyse" and "Résultat" for three tests: Acide Urique, Gazométrie artérielle, and Rubéole Anticorps IgG.

Antécédents			
infection chronique par le virus de l'hépatite B			
opération de la vésicule biliaire			

Analyse	Résultat
Acide Urique	resultat analyse Acide Urique
Gazométrie artérielle	resultat analyse Gazométrie artérielle
Rubéole Anticorps IgG	resultat analyse Rubéole Anticorps IgG

Deuxième cas :

Détails informations médicales

Hôpital : CNMS
Service : Cardiologie

Maladies Chroniques	
Infection chronique par le virus de l'hépatite C	O-POS
bronchite chronique	12
vitiligo	cmHg
	pression artérielle systolique

Analyse	Résultat	Commentaire
Chlamydia Trachomatis	resultat Chlamydia Trachomatis	commentaire Chlamydia Trachomatis
Hépatite C	resultat Hépatite C	commentaire Hépatite C

3.5.5 Fenêtres du ministère

a. Accueil

Afin de pouvoir consulter les informations personnelles ou médicales d'un service de n'importe quel hôpital du pays il faut préciser l'identifiants de ces derniers puis sélectionner la fonctionnalité souhaitée.

Menu

Introduire l'identifiant de l'hôpital souhaité

Introduire l'identifiant du service souhaité

Consulter les informations personnelles des patients

Consulter les informations médicales des patients

b. Consulter les informations personnelles des patients

L'application offre l'avantage de consulter l'échelle national les informations personnelles de tous les patients, il suffit de mentionner l'identifiant de l'hôpital et du service souhaité. **Premier cas :**

The application window has a title bar 'Liste des patients'. In the top left, it says 'Hopital : Mustapha Pacha' and 'Service : Cardiologie'. On the right are icons for home and back.

Table Data:

Nom	Prénom	Téléphone 1	Téléphone 2	Nom du médecin	Prénom du médecin
Abbad	Farid	0557896525	0775896582	Amara	Okba
Abizar	Kamel	0778896525	0556892512	Amara	Okba
Arab	Redouane	0667589652	0552568957	Amara	Okba
Ladiani	Lydia	0778788747	0757874785	Amara	Okba
Mohammed	Amina	0685425369	0574123698	Dahmani	Karima

Deuxième cas :

The application window has a title bar 'Liste des patients'. In the top left, it says 'Hopital : CNMS' and 'Service : Cardiologie'. On the right are icons for home and back.

Table Data:

Nom	Prénom	Téléphone	Email	Nom du médecin	Prénom du médecin
Abid	Imene	0773488652	abd.imene@gmail...	Nadir	Mohamed
amine	ishak	0667896589	amine.ishak@gmail...	Nadir	Mohamed
Atrouche	Hind	0557412365	atrouche.hind@gm...	Nadir	Mohamed

c. Consulter les informations médicales des patients

L'application permet également de consulter l'échelle national les informations médicales de tous les patients, il suffit de mentionner l'identifiant de l'hôpital et du service souhaité. Les données sont par la suite décryptées puis affichés à l'écran.

Premier cas :

Informations médicales

Hôpital : Mustapha Pacha
Service : Cardiologie

Nom	Prénom	Date consultation	Groupe sanguin	Taille	Poids	Observation
Abbad	Farid	2021-12-29	O-POS	185	82	état stable
Abizar	Kamel	2021-12-29	O-POS	190	78	Asthme sévère sous ...
Abbad	Farid	2021-12-29	O-POS	185	82	état critique
Ladiani	Lydia	2021-12-29	O-POS	162	59	Grossesse stable
Mohammed	Amina	2021-12-29	O-POS	158	49	Tachycardie induite ...
Mohammed	Amina	2021-12-29	O-POS	158	44	Stabilisation de son ...

[Consulter en détail](#)

Deuxième cas :

Informations médicales

Hôpital : CNMS
Service : Cardiologie

Nom	Prénom	Date consultation	Groupe sanguin	Tension	Diagnostique
Abid amine	Imene ishak	2021-12-29 2021-12-29	O-POS O-POS	12 8	pression artérielle systolique pression artérielle diastolique

[Consulter en détail](#)

Consulter en détail les informations médicales

De plus, il est possible de consulter l'échelle national les informations médicales en détail de tous les patients, il suffit de mentionner l'identifiant de l'hôpital et du service souhaité. Les données sont par la suite décryptées puis affichés à l'écran. **Premier cas :**

Détails informations médicales

Hôpital : Mustapha Pacha
Service : Cardiologie

Antécédents	Abbad	Farid
infection chronique par le virus de l'hépatite B	185	82
opération de la vésicule biliaire	Cm	Kg
	O-POS	état stable

Analyse	Résultat
Acide Urique	resultat analyse Acide Urique
Gazométrie artérielle	resultat analyse Gazométrie artérielle
Rubéole Anticorps IgG	resultat analyse Rubéole Anticorps IgG

Deuxième cas :

Détails informations médicales

Hôpital : CNMS
Service : Cardiologie

Maladies Chroniques	Abid	Imene
Infection chronique par le virus de l'hépatite C		
bronchite chronique		
vitiligo		
	O-POS	12 cmHg
		pression artérielle systolique

Analyse	Résultat	Commentaire
Chlamydia Trachomatis	resultat Chlamydia Trachomatis	commentaire Chlamydia Trachomatis
Hépatite C	resultat Hépatite C	commentaire Hépatite C

4 Conclusion

Dans le monde actuel rempli de données mais aussi rempli d'options, la perte la confiance des clients ou utilisateurs est le risque principal auquel toute organisation peu importe son secteur peut faire face vu la masse de données importante. C'est pourquoi, ces organisations prennent aujourd'hui des mesures pour mieux gérer et protéger les informations en leurs possession, en accordant la plus grande attention aux modalités de collecte, d'utilisation, de stockage et de partage des données. C'est un engagement obligatoire mais aussi de plus en plus difficile vu que nous, les humains génèrent d'énorme quantités de données et les estimations affirment que ces dernières sont en constante hausse.