REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

MINISTRE DE L'ENSEIGNEMENT SUPERIEUR

ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE SAAD DAHLEB BLIDA

Faculté des sciences

Département : Informatique

Mémoire

Pour l'obtention du diplôme de

Master

En informatique

Option : sécurité des systèmes d'information

Présenté par :

Ait Ziane Meriem

Bouchelarem Lina yesmine

THEME

Le contrôle d'accès pour la protection des données personnelles médicales informatisées

Soutenu le : 14/09/2020

Devant le jury composé de :

M.Douga Yacine	**Examinateur**
Mme.Cheriguene Soraya	**Examinatrice**
Mme.Boustia Narhimene	**Promotrice**

L'organisme d'accueil : CERIST

Encadré par : M.Meziane Abdelkrim

Année Universitaire 2019/2020

Remerciement

Nos remerciements vont d'abord au Créateur de l'univers qui nous a doté d'intelligence, et nous a maintenu en santé pour mener à bien cette année d'étude.

Notre gratitude s'adresse à Mme Boustia Narhimene pour son encadrement, son orientation, ses conseils et la disponibilité qu'elle nous a témoignée pour nous permettre de mener à bien ce travail.

Nous tenons à exprimer nos vifs remerciements à Mr Meziane Abdelkrim, maitre de recherche et responsable de la division systèmes d'information et systèmes multimédias. Il a toujours été disponible, à l'écoute de nos questions et grâce à son encouragement on a pu avancer dans ce travail.

On tient également à remercier Dr Ait Ziane Sarrah et Dr Belabbassi Hanene, médecins à l'hôpital de Douera au service de médecine physique et de réadaptation, pour leur soutien, les informations et leur temps qui nous ont accordé.

Nous tenant à remercier sincèrement les membres du jury pour l'intérêt qu'ils ont porté à notre recherche en acceptant d'examiner notre travail.

On n'oublie pas nos parents pour leur contribution, leur soutien et leur patience.

Enfin, nous adressons nos plus sincères remerciements à tous nos proches et amis, qui nous ont toujours encouragés au cours de la réalisation de ce mémoire.

Dédicace

Avec l'expression de ma reconnaissance, je dédié ce modeste travail à ceux qui, quels que soient les termes embrassés, je n'arriverais jamais à leur exprimer mon amour sincère.

A l'homme, mon précieux offre du dieu, qui doit ma vie, ma réussite et tout mon respect : mon cher père Kamel.

A la femme qui a souffert sans me laisser souffrir, qui n'a jamais dit non à mes exigences et qui n'a épargné aucun effort pour me rendre heureuse : mon adorable mère Houria.

A mes frères Sofiane et Meziane et mon fiancé Yacine qui n'ont pas cessé de me conseiller, encourager et soutenir tout au long de mes études. Que dieu les protège et leurs offre la chance et le bonheur.

A l'homme le plus courageux et la femme la plus douce que j'ai connu, malheureusement ils ne sont plus avec nous mais ils sont toujours dans nos cœur : mon cher oncle zizi Mahdi ALLAH Yerahmo et mon adorable jida Fetta allah yerhamha.

A ma grand-mère, mes oncles et mes tantes sans oublier ma belle-famille Bensmaili. Que dieu leur donne une longue et joyeuse vie.

A tous les cousins, les cousines (Ait Ziane et Amimi) et les amies que j'ai connu jusqu'à maintenant.

Merci pour leurs amours et leurs encouragements.

Sans oublier ma moitié, mon binôme Lina pour son soutien moral, sa patience et sa compréhension tout au long de ce projet.

A.Meriem

Dédicace

Je dédie ce modeste travail :

A mes chers parents,

Aucune dédicace ne saurait exprimer mon respect, mon amour éternel et ma considération pour les sacrifices que vous avez consenti pour mon bien être. Je vous remercie pour tout le soutien et l'amour que vous me portez depuis mon enfance et j'espère que votre bénédiction m'accompagne toujours. Que ce modeste travail soit l'exaucement de vos vœux tant formulés, le fruit de vos innombrables sacrifices, bien que je ne vous en acquitterai jamais assez.

A mes chères et adorables sœurs,

Ines ma complice, Houyem la douce au cœur si grand, Zahoua ma petite sœur que j'adore.

Merci d'être toujours là, je vous souhaite une vie pleine de bonheur et de succès et que Dieu, le tout puissant, vous protège et vous garde.

A toute ma famille et mes amis, et spécialement Meriem mon binôme, mon amie fidèle, je te suis très reconnaissante, et je ne te remercierai jamais assez pour ta profonde amitié.

B. Lina yesmine

Résumé

La sécurité revêt un aspect crucial dans le développement et la gestion des systèmes informatiques modernes, et plus particulièrement le contrôle d'accès.

Le contrôle d'accès représente l'une des stratégies de sécurité des systèmes informatiques. De nombreuses techniques ont été proposées pour le contrôle d'accès. Une des techniques les plus utilisées exprime les autorisations d'accès à travers le concept de rôle, dans ce cas les décisions d'accès sont basées sur le rôle auquel l'utilisateur est rattaché.

Dans ce projet nous avons proposé un modèle de contrôle d'accès basé sur les rôles qui répond aux besoins du service rééducation fonctionnelle de l'hôpital de Douera.

Le DMP est un dossier très sensible, qui nécessite un très haut niveau de sécurité, pour cela notre application contient également un système de protection qui consiste à sécuriser les données d'une façon unique pour se protéger et afin de mettre l'utilisateur dans un environnement de confiance.

Abstract

Security is a crucial aspect in the development and management of modern IT systems, especially access control.

Access control is one of the security strategies for computer systems. Many techniques have been proposed for access control. One of the

most widely used techniques expresses access permissions through the concept of role, in which case access decisions are based on the role to which the user is attached.

In this project we have proposed a role-based access control model that meets the needs of the functional rehabilitation department of Douera hospital.

The DMP is a very sensitive file, which requires a very high level of security, for this our application also contains a protection system which consists in securing the data in a unique way and in order to put the user in a trust environment.

ملخص

يـــعد الأمـــــن جانبًا مهمًا في تطوير وإدارة أنظمة تكنولوجيا المعلومات الحديثة، وخاصة التحـكم في نظام الدخـــول.

يعد نظام الدخـــول إحدى استراتيـجيات الأمان لأنظـمة الكمبيـوتـــر. تم اقـتراح العـديد من التـقـنـيـات للتحكم في نظام الدخول. واحدة من أكثر التقـنـيات المستخدمة على نطاق واسع تعبر عن أذونات الدخول من خلال مفـهوم الدور ، وفي هذه الحالة تعتمد قـرارات الدخول على الدور الذي يرتبط به المسـتـــخدم.

في هذا المشروع ، اقترحنا نموذجًا للتحكم في نظام الدخول قائمًا على الأدوار يلبي احتياجات قسم إعادة التأهيل الوظيفي في مستشفى دويرة.

الملف الطبي هو ملف حساس للغاية ويتطلب مستوى عاليًا جدًا من الأمان، لذلك يحتوي تطبيقنا أيضًا على نظام حماية يتمثل في تأمين البيانات بطريقة فريدة من أجل وضع المستخدم في بيئة الثقة.

Table des matières

Chapitre 3: RBAC, le contrôle d'accès adapté à notre DMP

Chapitre 4 : L'implémentation et l'aspect sécuritaire

Table des figures

Introduction générale :

Dans le contexte d'un système d'information hospitalier, il est primordial de fournir tous les moyens permettant de maîtriser les risques et les menaces pouvant toucher de près ou de loin aux informations liées à la santé des patients. Ces informations doivent être protégées contre les manipulations, les accès non autorisés et les abus.

Le besoin des personnes à vouloir protéger leurs données sensibles est appelé en anglais la *privacy*. Cette notion varie considérablement selon les pays, les cultures, et les juridictions. La *privacy* est particulièrement importante dans le domaine de la santé, les accès non autorisés et l'utilisation malveillante des données médicales peuvent provoquer des préjudices conséquents pour les patients.

La clé de la protection des informations personnelles est de s'assurer que seules les personnes ayant droit peuvent y accéder. Le contrôle d'accès représente donc l'un des principaux mécanismes qui assure cette protection. À travers un modèle de contrôle d'accès, sont déterminées les données auxquelles un utilisateur peut accéder suivant une certaine politique de sécurité.

Problématique :

La tenue du dossier médical du patient relève de la responsabilité de tous les professionnels de la santé au sein d'un établissement de santé. Négliger cette responsabilité va engendrer inévitablement des répercussions néfastes. Ainsi notre problématique s'articule autour de la question principale suivante : **Quel modèle de contrôle d'accès utiliser pour la protection des données personnelles médicales informatisées ?**

Objectif du projet :

L'objectif de notre projet de fin d'étude c'est de trouver une solution pour mieux protéger le dossier médical, qui est partageable entre le personnel du service de la rééducation fonctionnelle du CHU douera.

Organisation du mémoire :

Le présent mémoire est organisé comme suit :

- Le premier chapitre présente la sécurité des systèmes d'information et le système d'information hospitalier.

Le chapitre présente également les principaux modèles de contrôle d'accès classiques; en l'occurrence les modèles basés sur les politiques discrétionnaires (DAC), les politiques obligatoires (MAC), les politiques à base d'identité (IBAC), les politiques à base de rôle (RBAC) et les politiques à base d'attribut (ABAC)…

- Le deuxième chapitre s'intéresse au domaine de la santé et particulièrement aux dossiers médicaux partageables (DMP). Il décrit les différents besoins liés à leur sécurité et à la protection des données personnelles des patients (privacy) contenues dans ces dossiers.

- Dans le troisième chapitre, nous présentons le modèle de contrôle d'accès qu'on va implémenter dans notre application pour protéger le DMP.

- Le quatrième chapitre présente l'implémentation du modèle ainsi que l'aspect sécuritaire qu'on a ajouté pour renforcer la sécurité du DMP.

Chapitre 1

Contrôle d'accès aux systèmes d'information

Aujourd'hui, avec l'avancement des technologies de l'information et de la communication, la protection des données contre les atteintes à la confidentialité, à l'intégrité et à la disponibilité est devenue une exigence majeure. Afin d'assurer cette protection, les accès aux données doivent être contrôlés et ceux qui ne sont pas autorisés doivent être impérativement bloqués. Ceci est appelé le contrôle d'accès.

Un modèle de contrôle d'accès veille à ce que les données ne soient accessibles que par des utilisateurs ayant le droit d'y accéder. Le développement d'un modèle de contrôle d'accès repose sur la définition des politiques d'accès qui déterminent quel utilisateur a le droit d'effectuer quelle action sur quelle donnée.

Dans ce premier chapitre, nous allons nous intéresser à la sécurité des systèmes d'information et le système d'information hospitalier, nous présentons également les principaux modèles de contrôle d'accès, en l'occurrence les modèles basés sur les politiques discrétionnaires, les politiques obligatoires, les politiques à base de rôle, d'identité ainsi que les politiques à base d'attribut.

1.1 Sécurité des systèmes d'information :

La notion de système d'information couvre l'ensemble des éléments qui participe à la collecte, au stockage, à la gestion, au traitement et à la diffusion de l'information au sein des organisations [1].

Il y a plusieurs propriétés à prendre en compte dans le développement des systèmes d'information. Une de ces propriétés est la sécurité qui permet aux utilisateurs d'avoir une confiance justifiée dans le système et dans les services qu'il délivre. Cette notion couvre des domaines allant de la sécurité physique à la sécurité logique.

La propriété de sécurité peut être analysée selon plusieurs sous propriétés :

– la confidentialité : l'information est disponible uniquement aux personnes et aux ressources autorisées.
– l'intégrité : l'information est précise et exhaustive.
– la disponibilité : le système doit être accessible et prêt à l'emploi,
– la traçabilité : l'information est suivie dans son évolution, son parcours.

La protection d'une information, ou sécurité informatique, est donc le produit de ces quatre composantes.

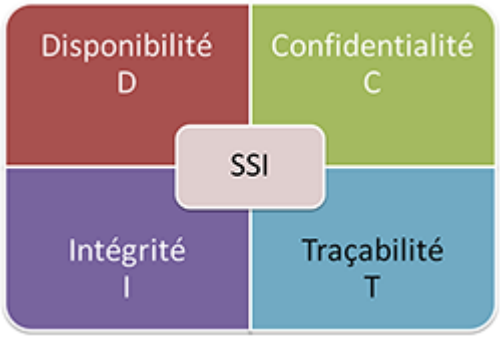


Figure 1-1: les propriétés de la sécurité des systèmes d'informations

1.2 Politique de sécurité :

Les ITSEC [2] définissent la politique de sécurité comme étant l'ensemble des lois, règles et pratiques qui régissent la façon dont l'information sensible et les autres ressources sont gérées, protégées et distribuées à l'intérieur d'un système spécifique. Une politique de sécurité s'occupe de spécifier simultanément les propriétés désirées et d'établir un cadre réglementaire permettant de modifier l'état de sécurité du système tout en garantissant ces propriétés et en assurant la protection. Cette politique peut se spécialiser selon trois axes [3]:

- Politiques de sécurité physiques qui définissent les procédures et les moyens qui permettent de protéger l'environnement physique des risques (incendies, inondations, vols, etc.).

- Politiques de sécurité administratives qui décrivent les procédures organisationnelles (répartition des tâches, séparation des pouvoirs, etc.).

- Politiques de sécurité logiques qui définissent les actions légitimes qu'un utilisateur peut effectuer. Elles s'intéressent aux fonctions d'identification et d'authentification.

1.3 Système d'Information Hospitalier (SIH) :

Un système d'information hospitalier est un système d'information appliqué au secteur de la santé, et plus particulièrement aux établissements de santé. C'est un système informatique destiné à faciliter la gestion de l'ensemble des informations médicales et administratives d'un hôpital. Le SIH est conçu par des hospitaliers, pour les hospitaliers. Un logiciel structuré autour du parcours de soins et du dossier patient.

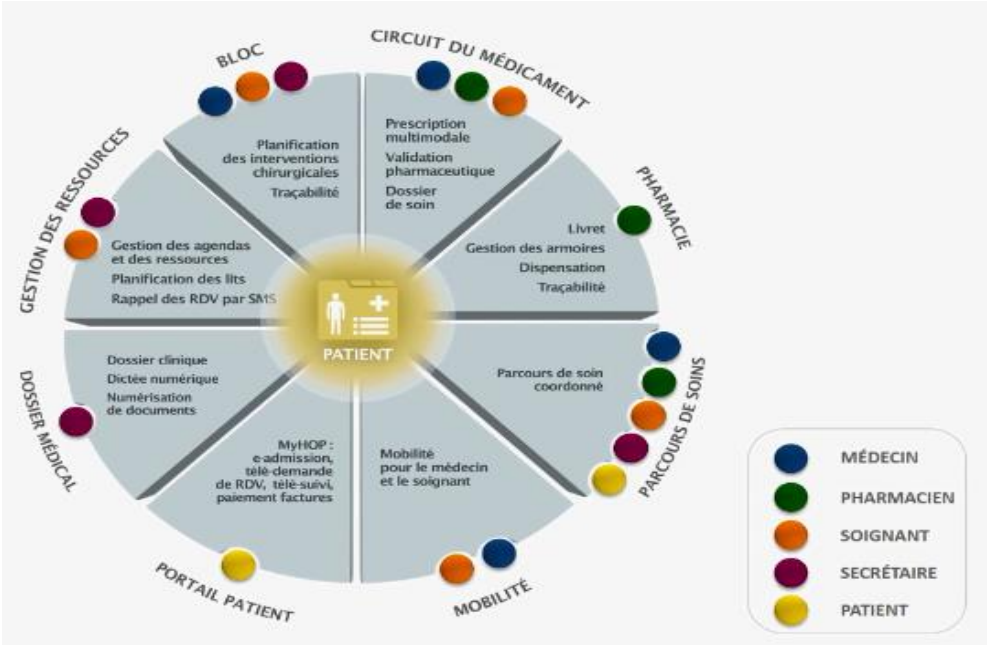


Figure 1-2: Représentation d'un SIH.

1.4 Gestions des identités :

1.4.1 Définition de l'identité :

Dans l'article «Trust Requirements in Identity Management» [4], l'identité est définie comme «un ensemble de caractéristiques propres par lesquelles une personne ou une organisation est connue ou reconnue. Ces éléments peuvent être définis, comme le nom, l'adresse, ou peuvent être innés comme les empreintes digitales. Pour l'identité d'une organisation, les caractéristiques sont acquises».

Le standard international ISO/IEC 24760-14[5], basé sur la recommandation UIT-T Y.2720 rédigée par l'Union Internationale des Télécommunications, étend la définition d'identité à l'«information utilisée pour représenter une entité dans un système d'information et de communication». Une entité représente une personne physique ou morale (organisation, entreprise, ...), une ressource (un objet tel qu'un matériel informatique, un système d'information ou de communication) ou un groupe d'entités individuelles.

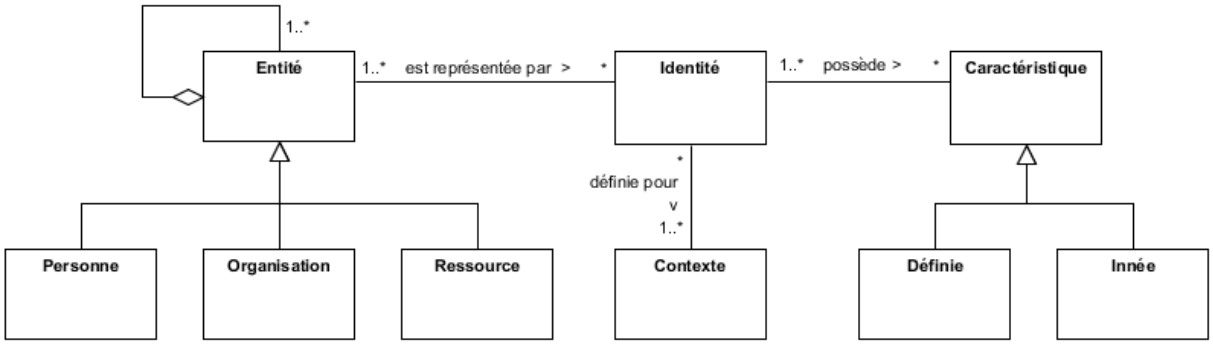


Figure 1-3: Diagramme de classe du concept d'identité

1.4.2 Cycle de vie de l'identité:

Le CLUSIF [6] définit la gestion des identités comme la gestion du «cycle de vie des personnes (embauche, promotion, mutation, départ, etc.) au sein de la société et les impacts induits sur le système d'information». Ces changements ont des conséquences sur les informations connues et gérées par le domaine d'identité de l'organisation.

Une identité peut être construite puis enregistrée auprès du fournisseur d'identité. Ensuite, lorsque la personne commence son contrat, l'identité qu'il doit présenter auprès des fournisseurs de service est activée, afin de lui permettre d'interagir avec les ressources utiles à sa mission. A la fin de ladite mission, l'identité peut être suspendue, donc temporairement inutilisable, s'il est prévu de la réutiliser pour un prolongement de contrat par exemple. Une autre possibilité consiste à archiver l'identité. Cela implique que les informations lui étant liées ne sont plus exploitables pour l'authentifier auprès du domaine. Par contre, l'ensemble, ou une sous-partie, des informations archivées peut être réutilisé pour construire une nouvelle identité (processus de restauration). Après un délai établi par l'organisation et par la loi, toutes les informations relatives à l'identité sont supprimées.

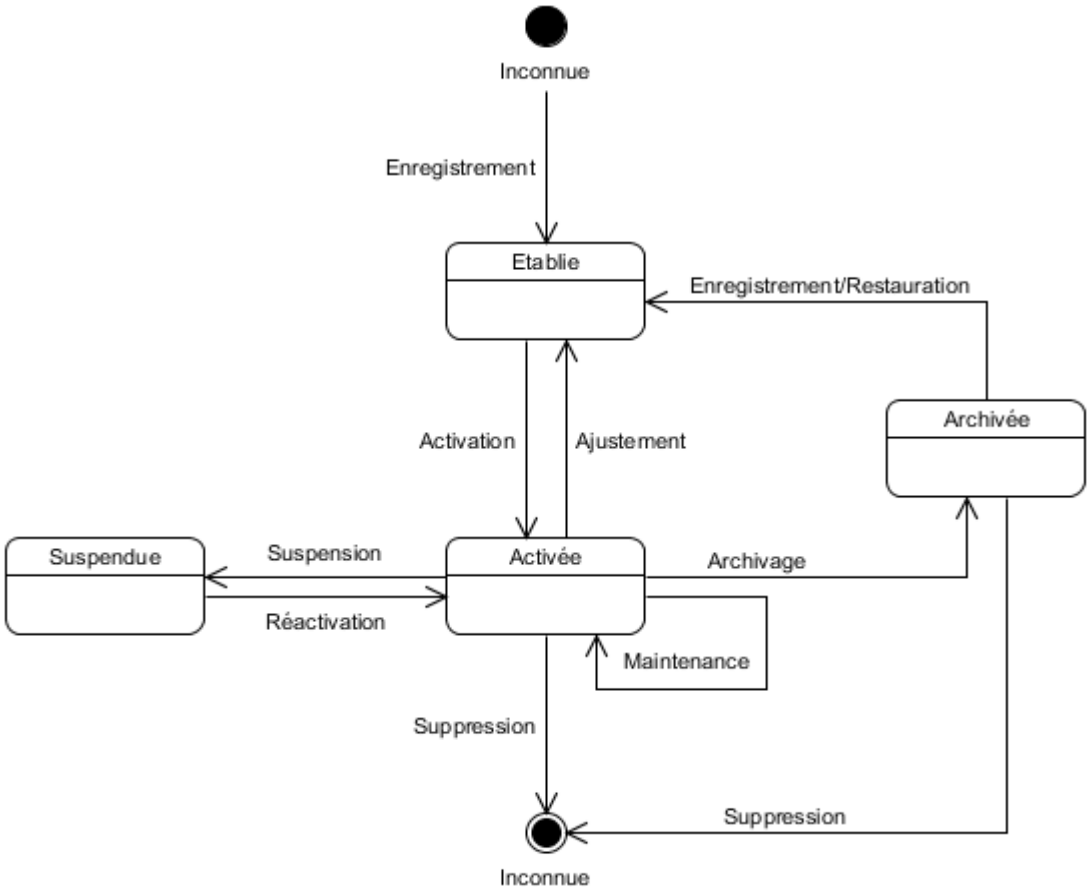


Figure 1-4: Cycle de vie d'une identité

1.5 Gestions des accès :

1.5.1 Définition gestion des accès :

Une organisation doit gérer les accès aux ressources dont elle dispose. La gestion des accès permet de s'assurer de mettre à disposition de chacune des personnes impliquées dans les projets de l'organisation, à tout instant, tous les moyens nécessaires à la réalisation de la mission qui leur a été confiée, et que ces moyens soient à chaque instant limités au juste nécessaire.

La gestion des accès qui comporte le contrôle d'accès est généralement réalisé par la séquence de processus AAA (Authentification, Authorization, Accounting) [7].

- Authentification : Avant d'accéder à une ressource ou un service, toute entité devra décliner son identité et prouver qu'elle est bien celle qu'elle prétend être. Le processus d'authentification permet alors de vérifier et de valider l'identité numérique de cette entité [8].

- Autorisation : Le processus d'autorisation détermine si une entité authentifiée préalablement à la permission d'accéder ou non à une ressource ou un service [8].

- Traçabilité (Accounting): Une traçabilité est obtenue à partir de la journalisation des événements. Chaque création, modification ou suppression d'un compte, chaque accès ou tentative d'accès donne lieu à une historisation afin de déterminer les utilisateurs du système et repérer les comportements malveillants [8].

1.5.2 Modèles classiques de contrôle d'accès :

Dans la littérature, il existe deux grandes catégories de politiques de contrôle d'accès :

- les politiques discrétionnaires (DAC ou Discretionary Access Control) : La caractéristique principale du DAC est le fait que ce sont les utilisateurs qui attribuent les permissions sur les ressources qu'ils possèdent. C'est le type de mécanisme utilisé principalement dans les systèmes d'exploitation

modernes. En effet, il est très léger en termes d'administration, étant donné que l'attribution des droits est faite par les utilisateurs et non pas par les administrateurs.

- les politiques obligatoires (MAC ou Mandatory Access Control) : le MAC délègue l'attribution des permissions à une entité tierce, typiquement un administrateur externe de la politique de sécurité. Ainsi, les utilisateurs du système ne peuvent pas intervenir dans l'attribution des permissions d'accès, même s'ils disposent de droits d'administration dans le système d'exploitation.

On peut aussi définir des variantes de ces politiques qui peuvent mieux s'adapter à des organisations particulières, comme par exemple les politiques basées sur la notion de l'identité (IBAC), sur les rôles (RBAC), sur la notion d'attributs (ABAC) ou celles basées sur la notion d'équipes (TMAC). Afin d'exprimer les propriétés de sécurité, ces politiques utilisent des éléments de modélisation particuliers tels que les sujets (entité active : processus, utilisateur) et les objets (entité passive : fichier, ressource).

1.5.2.1 Modèles de contrôle d'accès discrétionnaires :

Le contrôle d'accès discrétionnaire est un moyen pour contrôler l'accès d'un sujet à un objet. Ce modèle est également appelé IBAC (Identity Based Access Control) car les décisions d'accès sont généralement basées sur l'identité du sujet (nom d'utilisateur, mot de passe, jeton, etc.). Dans le modèle DAC, le sujet propriétaire d'un objet peut changer les permissions d'accès à l'objet à sa discrétion (d'où le nom), comme il peut transmettre ces permissions à d'autres sujets. L'implantation de ce modèle a donné lieu à la constitution de matrices d'accès initialement introduite par Lampson [9] et qui a été généralisée en 1976 par Harison, Ruzzo et Ullman (HRU) [10]. Ce dernier est représenté par le triplet (S,O,Mso) où S désigne les sujets, O les objets, et Mso la matrice de contrôle d'accès. Dans le contexte d'un système d'information, les sujets incluent les utilisateurs et les processus exécutés pour le compte de ces utilisateurs. Les objets incluent les entités passives telles que

des fichiers ou des répertoires. Les actions correspondent généralement à des opérations élémentaires comme “lire“ ou “écrire“. Ainsi, A (S, O) définit l’ensemble des actions que le sujet S est autorisé à faire sur l’objet O.

	Fichier Salaires	Fichier Impôts
Alice	Lire, Écrire	
Bob		Lire
Jean	Lire	

Figure 1-5: Exemple d’une matrice d’accès

1.5.2.2 Modèles de contrôle d’accès obligatoires :

Les modèles obligatoires décrètent des règles incontournables. L’une des manières de faire est d’affecter, aux objets et aux sujets, des attributs qui ne sont pas modifiables par les usagers, et donc qui limitent leur pouvoir de gérer les accès aux informations qu’ils possèdent. Le premier a été développé par Bell et La Padula pour le département de défense américain et vise à assurer la confidentialité. Le deuxième, dit de Biba, s’intéresse à l’intégrité.

Ce modèle est basé sur une approche multi-niveaux. Le modèle de sécurité associé à MAC s’appelle le modèle de treillis et s’appuie sur l’association de différents niveaux aux sujets (niveaux d’habilitation) et aux objets (niveaux de classification). Chaque niveau est caractérisé par une classification cl (par exemple, non-classifié, confidentiel, secret, très-secret) et par un compartiment C défini dans un ensemble de catégories. Intuitivement, la classification d’un objet représente le danger que peut constituer la divulgation de l’information qu’il contient, tandis que l’habilitation d’un sujet reflète la confiance qui lui est accordée. Les niveaux de sécurité constituent un treillis avec une relation d’ordre partiel de dominance notée ‘≤’. Si n= (cl,C) et n’= (cl’,C’) sont deux niveaux de sécurité :

$n \leq n' \quad \Leftrightarrow \quad (cl \leq cl' \quad \text{et} \quad C \subseteq C')$

Les objectifs de sécurité du modèle de Bell-LaPadula sont :

-interdire toute fuite d'information d'un objet vers un autre ayant une classification inférieure,

-interdire à tout sujet possédant une certaine habilitation d'obtenir des informations d'un objet d'un niveau de classification supérieur.

Les règles de sécurité de ce modèle sont :

-un sujet ne peut accéder en lecture à un objet que si le niveau d'habilitation du sujet domine le niveau de classification de l'objet,

-un sujet ne peut accéder à la fois en lecture à un objet O et en écriture à un objet O' que si le niveau de classification de O' domine celui de O.

1.5.2.3 Modèles de contrôle d'accès à base sur l'identité(IBAC) :

Le contrôle d'accès basé sur l'identité (IBAC - Identity Based Access Control) est parmi les premiers modèles de contrôle d'accès. Ce modèle introduit les concepts fondamentaux de sujet, d'action et d'objet. [26]

L'objectif de ce modèle IBAC est de contrôler tout accès direct des sujets aux objets via l'utilisation des actions. Ce contrôle est basé sur l'identité du sujet et l'identificateur de l'objet, d'où le nom du modèle IBAC. [26]

Dans IBAC, une permission a le format suivant : un sujet a la permission de réaliser une action sur un objet. La politique d'autorisation qui permet de spécifier les permissions est définie grâce à l'utilisation d'une matrice de contrôle d'accès dans laquelle les lignes et colonnes de la matrice correspondent respectivement à l'ensemble des sujets et des objets du système d'information.[26]

	Objet 1	Objet 1	Objet 1
Sujet 1	rw	r	w
Sujet 2	r	-	rw
Sujet 3	w	-	r

Figure 1-6: Matrice de la politique d'autorisation IBAC

Cependant la limite de ce modèle est sa mise à l'échelle. En effet, la politique devient complexe à maintenir lorsque le nombre d'entités est important. Le

modèle RBAC introduit une abstraction de l'entité sujet qui devient rôle, permettant ainsi de réduire cette complexité. [26]

1.5.2.4 Modèles de contrôle d'accès à base de rôle (RBAC) :

La notion de rôle (RBAC) est un outil très puissant et très expressif servant à décrire et à représenter les fonctionnalités de n'importe quelle organisation. Dans un hôpital par exemple, les rôles suivants peuvent figurer : médecin, infirmière, secrétaire, opérateur, administrateur système, etc. Une politique telle que tous les droits d'accès sont attribués aux utilisateurs uniquement en fonction du rôle qu'ils jouent dans le système d'information est appelée politique par rôle. Un rôle désigne une entité intermédiaire entre utilisateurs et privilèges. Ces derniers ne sont plus associés, d'une façon directe aux utilisateurs mais à travers des rôles. Les deux relations {Rôle, Privilège} et {Utilisateurs, Rôle} définissent précisément les permissions accordées à chaque utilisateur. La notion de rôle permet de tirer les avantages suivants :

-Faciliter la compréhension de la structure de l'organisation et réduire la complexité de gestion des droits d'accès. Ainsi, les rôles peuvent être organisés de manière à former une hiérarchie permettant de raffiner progressivement les différentes permissions attribuées à chaque rôle.

-Les différents rôles sont tirés directement de la structure de l'organisation considérée, ce qui facilite leur intégration dans la description de la politique de sécurité.

-Les politiques de sécurité à base de rôles sont plus faciles à administrer. En effet, l'intégration de nouveaux utilisateurs, la gestion des permissions ou même la définition de nouveaux objectifs dans la politique de sécurités en sont grandement facilités.

-La séparation claire entre la définition de la politique de sécurité et la structure de l'organisation permet d'améliorer considérablement la compréhension du système, et la séparation des pouvoirs au sein de l'organisation.

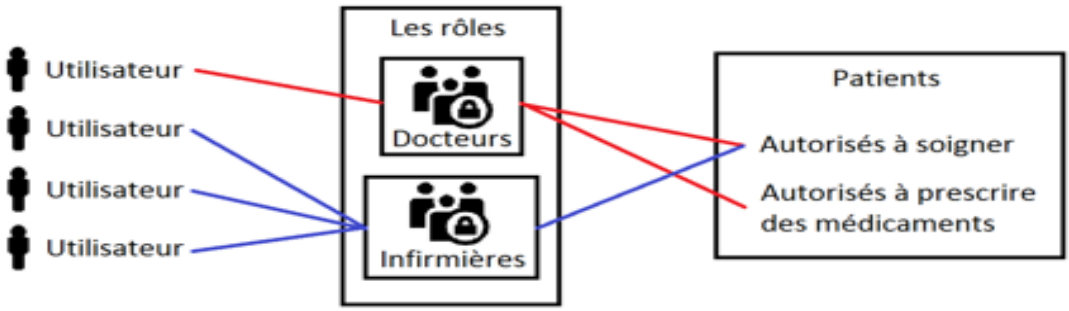


Figure 1-7: La notion de rôle dans RBAC

1.5.2.5 Modèles de contrôle d'accès basé sur les attributs (ABAC) :

ABAC est un modèle d'autorisation de «nouvelle génération» qui fournit un contrôle d'accès dynamique, sensible au contexte et aux risques. Il aide à atteindre une conformité réglementaire efficace.

Le modèle ABAC (Attribute Based Access Control) repose sur un ensemble d'attributs associés à un demandeur ou à une ressource à consulter pour prendre des décisions d'accès. Il existe plusieurs façons de définir ou d'utiliser des attributs dans ce modèle. Un attribut peut être la date de début du travail d'un utilisateur, l'emplacement d'un utilisateur, le rôle d'un utilisateur ou l'ensemble d'entre eux. Les attributs peuvent ou non être liés les uns aux autres. Après avoir défini les attributs utilisés dans le système, chaque attribut est considéré comme une valeur discrète et les valeurs de tous les attributs sont comparées à un ensemble de valeurs par un point de décision de politique pour accorder ou refuser l'accès.

Le modèle ABAC a été développé par Eric Yuan et Jin Tong, dans le but de pallier aux difficultés que rencontrent les architectures web services en termes de sécurité. En effet, les accès à l'information au niveau de ces architectures web services se font non seulement sur les systèmes distribués mais très dynamiquement. Les modèles classiques sont généralement destinés à un fonctionnement statique, ils ne permettent guère une évolution dynamique.

Enfin, il est essentiel de proposer une politique de sécurité pouvant fonctionner correctement avec ce type de modèle de contrôle d'accès, car la politique de sécurité est responsable de la sélection des attributs importants qui sont utilisés pour prendre des décisions d'accès.

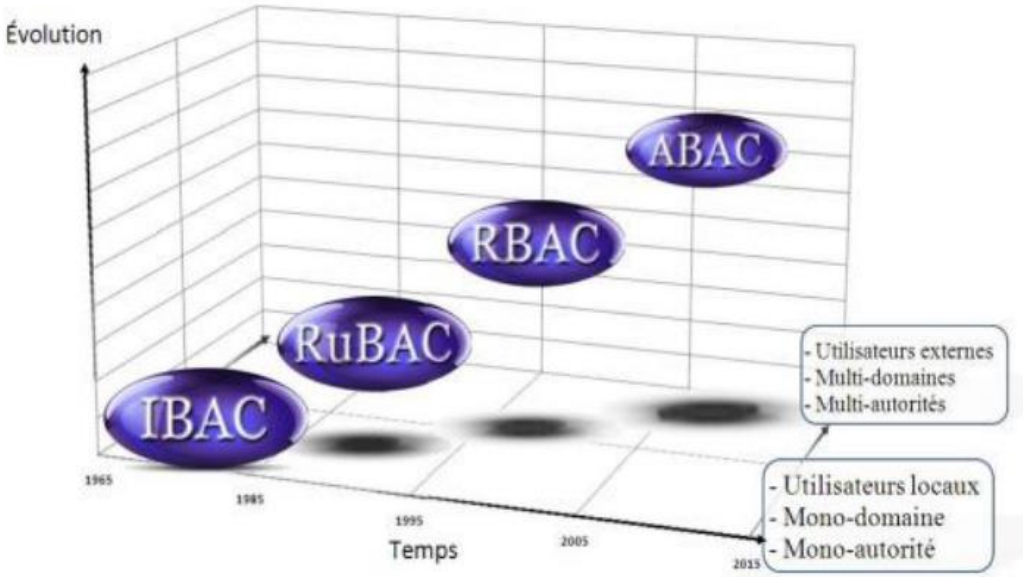


Figure 1-8: Évolution des modèles de sécurité [20]

1.5.2.6 Modèles de contrôle d'accès à base d'équipe (TMAC):

Le modèle TMAC a été formulé pour la première fois en 1997 par Thomas. Le but était de fournir un contrôle d'accès pour les systèmes d'information ayant des activités qui collaborent. L'entité de base, l'équipe, est une abstraction qui encapsule un ensemble d'utilisateurs, ayant des rôles différents et qui collaborent dans le but d'accomplir une tâche ou un objectif commun. Le contexte de collaboration d'une équipe donnée, doit tenir compte du :

-Contexte utilisateur : les utilisateurs qui forment l'équipe à un moment donné,

-Contexte objet : les instances des objets que l'équipe utilise pour accomplir sa tâche.

TMAC est un concept très récent utilisant un mélange des notions RBAC et TMAC. Il consiste en cinq entités : utilisateurs, rôles, privilèges, équipes et contextes. Comme dans TMAC, l'équipe est utilisée pour représenter un groupe d'utilisateurs, ayant des rôles spécifiques, et qui collaborent pour réaliser une activité. Elle est aussi un mécanisme qui associe les utilisateurs au contexte. Durant une session, les privilèges d'un utilisateur est l'union des privilèges de tous les rôles qu'il a activé. En plus, dans le contexte, sont incluses des informations concernant les données de l'activité de son équipe, ainsi que certaines informations contextuelles. Selon C-TMAC, l'accès aux ressources se fait comme suit :

Après son identification et son authentification, l'utilisateur sélectionne un sous-ensemble de rôles et d'équipes auxquels il a droit. L'ensemble des privilèges de l'utilisateur est combiné avec l'ensemble des privilèges de l'équipe comme indiqué dans les deux étapes suivantes :

Étape 1 : Considérons un utilisateur ayant activé un sous-ensemble de rôles et participant à un sous-ensemble d'équipes. Les privilèges de ses rôles sont dérivés par la formule suivante :

privilège-rôle = privilège-rôle-session ⊕ privilège-rôle-équipe.

-Le symbole ⊕ veut dire 'combiné avec'.

-La combinaison est soit une agrégation (union), soit un maximum/minimum, soit déterminée selon la structure de l'équipe.

-'privilège-rôle-équipe' est la combinaison de tous les rôles des utilisateurs appartenant à l'équipe.

Étape 2 : Les privilèges finaux sont dérivés à partir du contexte et des privilèges des rôles (étape 1) selon la définition suivante :

privilège-contexte = privilège-rôle ⊗ contexte-équipe

où ⊗ désigne l'opérateur de filtrage.

1.5.3 Les objective de contrôle d'accès :

Le contrôle d'accès a pour objectifs :

- De gérer et contrôler les accès logiques aux ressources informationnelles par des personnes ou des dispositifs.
- De détecter les accès non autorisés.
- De préciser les règles à observer en matière d'identification, d'authentification et d'autorisation d'accès des personnes ou des dispositifs.
- D'assurer la disponibilité de l'information en réduisant :

- ✓ les attaques de déni de service.
- ✓ La propagation d'un code malicieux entre systèmes informatiques.
- ✓ Les erreurs d'opération ou de configuration des applications.

- D'assurer l'intégrité de l'information en réduisant :
  - ✓ Les altérations par des utilisateurs non autorisés.
  - ✓ Les erreurs d'utilisation.

  - D'assurer la confidentialité de l'information en réduisant :
    - ✓ Les accès non autorisés.
    - ✓ Les diffusions non autorisées.

1.6 Conclusion :

Dans ce chapitre, nous avons présenté la sécurité des systèmes d'information et le système d'information hospitalier ainsi la gestion des accès et des méthodes de contrôle d'accès (DAC, MAC, RBAC, ABAC…).

.

Chapitre 2

Protection des données personnelles de santé

A l'heure d'aujourd'hui, les données numériques deviennent partie intégrante de nos vies. La santé numérique n'y a bien sûr pas fait abstraction. Auparavant, tous les documents médicaux étaient sous forme de piles de papiers interminables. Les communications entre médecins de différents domaines étaient compliquées et le risque de perte de dossiers médicaux était une réelle crainte. Avec l'avènement du numérique, la santé n'a pu échapper à sa numérisation. Cependant, même si l'informatique est apparue au grand public dans les années 90, le domaine de l'e-santé commence seulement à se développer à grande échelle. Selon le Directeur France de Sanofi, Mr. Guillaume Leroy, « en e-santé, nous n'en sommes qu'au début, mais le potentiel est énorme » (Sanofi, 2017).

Les données de santé doivent être protégées contre les manipulations, les accès non autorisés et les abus. Par conséquent, les aspects de sécurité, à savoir la confidentialité (que l'information soit accessible seulement aux personnes autorisées), l'intégrité (que l'information n'a pas été modifiée) et la disponibilité (que l'information soit accessible) doivent être examinés avec soin pour chaque activité de collecte, de stockage et d'échange d'informations, particulièrement lors de l'élaboration et de la mise en œuvre d'un DMP.

Dans ce chapitre, nous allons nous intéresser à la sécurité des dossiers médicaux partageables (DMP) ainsi qu'à la protection des données personnelles des patients contenues dans ces dossiers.

2.1 Le dossier médical

2.1.1 Définition

Les Professeurs François KOHLER[1] et Eric TOUSSAINT[2] abordent le dossier médical sous l'angle d'une prise en charge harmonieuse et coordonnée des soins sans oublier l'aspect pédagogique de ce dernier (enseignement, recherche). [11]

« c'est l'ensemble des informations médicales, soignantes, sociales et administratives, qui permettent d'assurer la prise en charge harmonieuse et coordonnée d'un patient en termes de soins et de santé par les différents professionnels qui en assurent la prise en charge. C'est à partir du dossier que l'on assure la traçabilité de la démarche de prise en charge et c'est à partir de vues différentes des données qu'il contient que l'on élabore des bilans d'activité et des travaux de recherche. Enfin, les dossiers servent à l'enseignement » [12]

«Le dossier du patient est le lieu de recueil et de conservation des informations administratives, médicales et paramédicales, formalisées et actualisées, enregistrées pour tout patient accueilli, à quelque titre que ce soit. Le dossier du patient assure la traçabilité de toutes les actions effectuées. Il est un outil de communication, de coordination et d'information entre les acteurs de soins et avec les patients. Il permet de suivre et de comprendre le parcours du patient. Il est un élément primordial de la qualité des soins en permettant leur continuité dans le cadre d'une prise en charge pluri professionnelle et pluridisciplinaire. Le rôle et la responsabilité de chacun des différents acteurs pour sa tenue doivent être définis et connus».[1][13]

Le dossier médical est un outil constitué de documents (physiques ou/et informatisés) qui retrace les épisodes de la maladie et du parcours de soin d'une personne. Il est aujourd'hui considéré comme un outil capital d'exercice pour tout

[1] François KOLER : Informatique médicale, CHRU Nancy, instigateur du premier DESS information médicale

[2] Eric TOUSSAINT : historien belge, président du Comité pour l'abolition de la dette du Tiers Monde, membre du Conseil international du Fond Social Mondial

professionnel de santé.1 La documentation clinique que contient le dossier d'un patient comprend toute information liée aux soins prodigués à ce patient durant son séjour ou sa visite à l'hôpital. Elle est destinée à évaluer l'état de santé actuel du patient, ainsi qu'à aider à planifier les soins, à évaluer ceux qui sont prodigués et à en assurer la continuité. Elle doit absolument être exacte et complète.

2.1.2 Les différents types de dossiers médicaux

Il existe différents types de dossiers médicaux. Les plus connus sont, le dossier de spécialité, le dossier partageable et le dossier d'archives.

- **Le dossier de spécialité** ou (EMR electronic medical record) est l'équivalent du dossier médical que l'on retrouve actuellement sur support papier, il est spécifique à l'unité de soins. Il résume une relation entre un patient et un professionnel de la santé qui appartient à cette unité. Sa constitution tient compte du plan de travail et des contraintes de l'unité à laquelle il appartient.

- **Le dossier partageable** (DMP) est un affichage de l'ensemble des dossiers médicaux d'une personne, provenant de tous les systèmes de santé du réseau pour fournir une vue globale des antécédents médicaux d'un patient [14].

- **Le dossier archive,** est un dossier stable contrairement au dossier partageable qui est dynamique. Il est alimenté par les résumés des dossiers partageables après fermeture de chaque processus de soins. Ce dossier comprend, outre l'identification du patient, des informations cliniques de synthèse, permettant de caractériser le type du séjour, les pathologies diagnostiquées, les traitements, la modalité de sortie et la façon dont le suivi de ce patient sera effectué [03].

2.1.3 Le dossier médical partageable (DMP)

2.1.3.1 Définition

Le Dossier Médical Partagé (DMP) est un carnet de santé numérique gratuit, confidentiel et sécurisé qui conserve précieusement vos informations de santé en ligne. Un système vital qui permet de stocker les antécédents médicaux et de les rendre disponibles aux professionnels de la santé. Un DMP doit contenir au moins les mêmes informations que celles contenues dans les différents dossiers sur papier. En plus, il doit pouvoir contenir des informations multimédias.

2.1.3.2 Les parties constitutive du DMP

Le contenu d'un DMP comprend les trois volets :

- **Le dossier administratif :** Pour tout patient pris en charge dans un établissement de soins, l'administration hospitalière doit constituer un dossier administratif qui alimente le dossier du patient avec tous les éléments permettant d'identifier le patient, (sa position administrative, sa couverture sociale, sa date d'entrée dans l'établissement et sa date de sortie.)

- **Le dossier des professionnels de santé :** Il rassemble des informations de natures diverses : des informations médicales antérieures à l'hospitalisation ou à la consultation actuelle (identité, anamnèse, allergies, antécédents, traitements, etc.), des informations relatives à la personne et à ses habitudes de vie, des informations médicales produites au cours du séjour en établissement de santé (observations, comptes rendus d'examens, prescriptions, comptes rendus opératoires, anatomopathologie, feuilles de température, lettres de sortie, etc.), des informations relatives aux soins paramédicaux dispensés par les infirmiers et les autres professionnels de santé. Tout médecin hospitalier est concerné par la tenue de ce dossier, il doit y consigner toutes ses observations, ses interventions et les hypothèses qu'il formule en conclusion.

- **Le dossier de soins infirmier :** Il se définit comme «un document unique et individualisé regroupant l'ensemble des informations concernant la personne soignée. Il prend en compte l'aspect préventif, curatif, éducatif et relationnel du soin. Il comporte le projet de soins qui devrait être établi avec la personne soignée. Il contient des informations spécifiques à la pratique infirmière»

  Il est une composante essentielle du dossier du patient dont il fait partie intégrante.

  Il comporte le dossier de soins infirmiers ou à défaut les informations relatives aux soins infirmiers et les informations relatives aux soins dispensés par les autres professionnels de santé éventuellement organisées en « sous dossiers » Les sages - femmes doivent également y porter la trace de leurs interventions, observations et traitements instaurés.

2.1.3.3 Les enjeux du DMP

Le DMP rassemble en un même espace numérique tout l'historique des soins, les traitements suivis, les résultats d'examens, les antécédents médicaux, les comptes rendus d'hospitalisation… Il est évident que les dossiers médicaux partageables offrent une meilleur prise en charge du patient par rapport aux systèmes traditionnels de dossiers en papier et aux dossiers médicaux de spécialité stockés localement [15].

Le DMP facilite la coordination des soins entre les différents professionnels de santé, en permettant à chacun de disposer de toutes les informations à la base d'une véritable multidisciplinarité concertée de la décision médicale [16]. Il doit ainsi permettre d'éviter la répétition d'examens, les prescriptions inutiles ou les interactions entre médicaments. Il offre un meilleur suivi des événements de santé par une meilleure documentation des épisodes de soins. L'accès au dossier complet du patient facilite la création de diagnostics médicaux plus complets et plus précis. Les DMPs assurent la cohérence et la souplesse à travers des données standardisées pour faciliter aux fournisseurs de soins l'interprétation des notes non normalisées à partir d'enregistrement fractionnés [17].

2.1.3.4 Les obstacles des DMP

Le dossier médical présente des atouts non négligeables. En simplifiant et en sécurisant la mise en ligne des informations médicales du patient, le DMP est censé favoriser la coordination, la qualité et la continuité des soins entre tous les professionnels de santé. Mais il existe aussi des limites et des risques.

En effet, la plupart des médecins et des malades ont un manque de capacités techniques et beaucoup d'entre eux sont mal à l'aise avec l'utilisation des ordinateurs. Le personnel de santé doit également être conscient de l'importance de la sécurité des données qu'il manipule et notamment celles liées à la protection des données personnelles des patients, car la moindre erreur dans ce sens provoquerait la perte de confiance du patient et par conséquent la non utilisation du système.

2.1.3.5 Les principaux dangers liés à l'informatisation de données de santé

Les trois grands types de risques sont la disparition de données, l'accès illégitime aux données et la modification non désirée de données.
Si le dossier médical est altéré, cela peut avoir des conséquences graves sur le traitement du patient. On va lui donner des médicaments auxquels il est allergique, lui injecter une dose trop faible, une dose trop élevée, l'opérer au mauvais endroit. Cela peut dans les pires cas aller jusqu'au décès. Une telle altération peut être provoquée par accident, par dysfonctionnement d'un système, par malveillance, par des attaques ciblées.
La question de la confidentialité est aussi centrale. Un vol de données peut avoir de lourdes conséquences, par exemple, s'il vient à révéler une maladie grave. Si l'employeur apprend que la personne a une maladie incurable, cela peut entraîner une perte d'emploi. Si la maladie avait été cachée à des proches, cela peut créer des problèmes familiaux. Suite à une divulgation massive de données, certaines personnes malveillantes peuvent s'en servir comme leviers pour cibler des patients et leur faire de la publicité sur internet : "(Je sais que vous êtes diabétique), voici la nouvelle pompe à insuline". Pire, certains font du rançonnage ciblé : "J'ai accédé à vos données de santé, je sais que vous avez le Sida, versez-moi cette rançon si vous ne voulez pas que je le divulgue sur votre compte Facebook." Les données de santé

sont, avec les données bancaires, les plus cotées, hélas, sur le marché noir de la donnée.

2.2 Sécurité du DMP

2.2.1 Propriétés de sécurité

La confidentialité, l'intégrité, la disponibilité et la sécurité des données restent des enjeux de taille pour le secteur de la santé connectée.

2.2.1.1 Confidentialité

La confidentialité est un enjeu majeur dans le domaine médical. Elle assure que l'information soit accessible seulement aux personnes autorisées. Elle a pour objectif essentiel de protéger des informations à caractère personnel concernant l'identité de l'usager, sa pathologie, ses problématiques personnelles et familiales, dans le souci du respect de l'individu. L'information médicale est considérée parmi les plus confidentiels de tous les types de renseignements personnels. La protection de cette confidentialité est donc indispensable pour maintenir la protection des données personnelles.

2.2.1.2 . Disponibilité

Le secteur de la santé n'a pas échappé à la transformation digitale ces dernières années. Ce secteur, qui fonctionne 24h/24 et 7j/7, nécessite que les données et services soient disponibles en continu.

La disponibilité se réfère à la propriété que l'information doit être accessible et utilisable à la demande par une entité autorisée. La disponibilité de l'information médicale est également essentielle pour une prestation efficace de soins. Les systèmes informatiques de santé doivent rester opérationnels en cas de catastrophes naturelles, d'attaques par déni de service ou de pannes du système. L'indisponibilité peut rapidement devenir une question de vie ou de mort et ne peut tout simplement pas se chiffrer en heures ni même en minutes. Les pannes,

lorsqu'elles surviennent, ne doivent pas durer plus de quelques secondes avant que l'accès aux données soit rétabli.

2.2.1.3 Intégrité

L'intégrité assure que l'information soit exacte et qu'elle n'a pas été modifiée de façon non autorisée. Dans un système de santé, les données sont collectées et utilisées par plusieurs fournisseurs de soins, les cliniques, les hôpitaux, les centres de réadaptation, etc. Par conséquent, les données peuvent être modifiées volontairement ou involontairement. Par exemple, une impulsion de 74 qui est involontairement enregistré comme 47 ou une mauvaise manipulation lors d'un choix à partir d'un menu déroulant. D'où la nécessité d'avoir un DMP qui dispose d'outils pour alerter le clinicien qu'un résultat erroné a été saisie [18].

2.2.2 Moyens de sécurité

Les professionnels et établissements de santé sont tenus de respecter les obligations relatives aux traitements de données à caractère personnel, en leur qualité de responsable du traitement. Parmi ces obligations, la sécurité des données constitue un impératif.

Toute personne prise en charge par un professionnel ou un établissement de santé a droit au respect de sa vie privée et au secret des informations la concernant. Les professionnels de santé, ainsi que ceux intervenant dans le système de santé, sont soumis au secret médical.

Les professionnels de santé doivent prendre toutes précautions utiles pour empêcher que les données ne soient modifiées (*intégrité de l'information*), effacées par erreur (*disponibilité*), ou que des tiers non autorisés aient accès au traitement (*confidentialité*). Ils sont donc tenus de mettre en œuvre :

- *des mesures de sécurité physique* par un accès contrôlé aux locaux hébergeant les serveurs et par la mise en œuvre d'une procédure d'habilitation permettant de restreindre l'accès aux seules personnes habilitées, et

- *des mesures techniques* par la protection des serveurs par des firewalls, filtres anti-spam et anti-virus. Le chiffrement des informations stockées, cela signifie que

l'information sur la santé ne peut être lue que par les personnes qui utilisent un système qui peut les décrypter avec une clé. Le contrôle d'accès, pour limiter l'accès aux renseignements aux personnes autorisées.

Afin de garantir la sécurité et la confidentialité des données, il est recommandé aux directeurs d'établissements de santé, publics comme privés, de sensibiliser leur personnel aux bonnes pratiques à adopter. L'absence de déploiement de mesures de sécurité technique ou la négligence dans le déploiement de mesures adaptées sont considérées comme des atteintes graves à la protection de la vie privée des personnes.

2.2.2.1 Contrôle d'accès

Au cours d'un processus de soins médicaux, des quantités d'informations volumineuses sont créées, et l'accès à ces informations devient par la suite capital pour la prise en charge des patients. L'information médicale est très personnelle et sa divulgation à des personnes non autorisées peut avoir des conséquences irrévocables pour les patients et pourrait mettre leur santé ou même leur vie en danger.

Les systèmes de santé sont classés comme étant des systèmes critiques du point de vue de la sécurité et notamment du contrôle d'accès. D'autres systèmes souvent décrits comme étant critiques comme, la signalisation ferroviaire, les systèmes de contrôle d'une centrale nucléaire et les systèmes financiers sont différents des systèmes de santé en ce qui concerne la gestion des accès. Pour la plupart des systèmes critiques, la règle d'accès par défaut est «en cas de doute - bloquer", tandis que pour les systèmes de santé, c'est toujours «en cas de doute - permettre " [19]. En effet, il est plus important de fournir les meilleurs soins aux patients (qui dépendent de l'accès des cliniciens à l'information) que de protéger ses données personnelles. Le contrôle d'accès dans le domaine médical doit alors trouver un équilibre entre la confidentialité et la disponibilité. Une politique trop "souple" pourrait permettre l'accès inapproprié, mais une politique trop «serrée» peut empêcher un accès indispensable et pousser les utilisateurs à contourner les règles de sécurité, ce qui peut conduire à des conséquences graves [20].

L’accès non autorisé aux DMP peut être effectué par des utilisateurs non autorisés à y accéder comme des pirates, mais aussi par des utilisateurs autorisés qui violent les conditions d'utilisation appropriées. Par exemple, un infirmier qui accède aux données d’un patient suite à un oubli de session ouverte du médecin traitant de ce dernier…etc.

2.3 Conclusion

Dans ce chapitre, nous avons présenté les principes de sécurité et de protection des données personnelles relatifs au domaine de la santé et particulièrement au dossier médical partageable. Notre objectif étant d’étudier la sécurité des informations médicales d’un patient, nous avons donc, au cours de ce chapitre, abordé plus en détail la protection des données personnelles.

Chapitre 3

RBAC, le contrôle d'accès adapté à notre DMP

Nous nous intéressons dans ce chapitre au modèle du contrôle d'accès que nous allons implémenter dans notre application.

Le contrôle d'accès a pour rôle de contrôler qui peut accéder aux DMPs et la façon dont ces derniers peuvent être manipulés. Plusieurs modèles de contrôle d'accès ont alors été conçus pour satisfaire les exigences des établissements de santé en matière de permissions.

Comme on a précisé précédemment, notre travail consiste a développé une application sécurisée pour aider le personnel de médecine physique et réadaptation du CHU Douera uniquement, et chaque membre du personnel est assigné à un rôle qui est déterminé par ses responsabilités et ses fonctions. Donc chaque membre a un rôle bien précis et des permissions différentes de celle des autres membres.

Pour cela et après avoir fait le tour sur les différents modèles de contrôle d'accès, nous avons jugé que le modèle RBAC est le modèle qui nous convient le mieux et qui répond à toutes nos attentes.

3.1 Définition :

Le contrôle d'accès basé sur les rôles (« Role-Based Access Control » (RBAC) en anglais) est un modèle de contrôle d'accès à un système d'information dans lequel chaque décision d'accès est basée sur le rôle auquel l'utilisateur est associé. Un rôle découle généralement de la structure d'une entreprise. Les utilisateurs exerçant des fonctions similaires peuvent être regroupés sous le même rôle. Un rôle,

déterminé par une autorité centrale, associe à un sujet des autorisations d'accès sur un ensemble d'objets.

Ce modèle est également appelé contrôle d'accès non discrétionnaire (« nondiscretionary access control » en anglais) et constitue une nouvelle possibilité de choix entre les systèmes à contrôle d'accès obligatoire (MAC) et contrôle d'accès discrétionnaire (DAC). [21]

3.2 Le modèle RBAC et ses avantages :

La mise en œuvre d'un Contrôle d'accès basé sur les rôles optimise l'efficacité opérationnelle, protège les données des risques de fuite ou de vol, réduit le travail d'administration et d'assistance informatique, et aide à répondre aux besoins d'audit.

L'approche RBAC simplifie considérablement la gestion des autorisations dans un système de contrôle d'accès, tout en offrant une grande flexibilité dans la spécification et l'application des politiques de contrôle d'accès dans les entreprises. En effet, dans le modèle RBAC, les utilisateurs peuvent être assignés à des rôles qui sont déterminés par leurs responsabilités et leurs fonctions. Ils peuvent être facilement transférés d'un rôle à un autre sans modifier la structure d'accès existante. Et aussi, les rôles peuvent être assignés à des nouvelles autorisations et permissions. [22]

Les permissions sont affectées à des rôles spécifiques au lieu d'être affectées directement à des utilisateurs comme c'est le cas dans les autres modèles. Ensuite, les rôles sont affectés aux utilisateurs selon leurs fonctions dans la structure de l'organisation généralement.

Les utilisateurs doivent pouvoir accéder aux données dont ils ont besoin pour faire leur travail – leur accorder un accès à des données qui ne leur sont pas utiles nuit à la sécurité et augmente le risque de fuite, vol, altération ou piratage des données. Les hackers n'aiment rien autant qu'accéder à un seul compte et se déplacer

latéralement sur le réseau pour rechercher des données qu'ils pourraient vendre. Si vous avez mis en place un RBAC efficace, les hackers se heurtent à un mur dès qu'ils tentent de sortir de la bulle du rôle de l'utilisateur qu'ils ont piraté.

Bien évidemment, la situation est grave lorsqu'il s'avère qu'un compte a été piraté. Mais cela pourrait être tellement pire si cet utilisateur avait accès à toutes les données sensibles. Même si l'utilisateur concerné travaille aux ressources humaines et a accès à des informations personnellement identifiables, le hacker n'aura pas la possibilité de se déplacer facilement pour accéder aux données des équipes financières et de direction.

Le RBAC réduit également la charge de travail informatique et d'administration de l'organisation et améliore la productivité des utilisateurs. Même si cela semble peu logique au premier abord, cela tombe sous le sens si l'on prend la peine d'y réfléchir. L'informatique n'a pas à gérer des droits personnalisés pour chaque utilisateur, et les utilisateurs concernés accèdent plus facilement aux bonnes données.

Gérer de nouveaux utilisateurs et des utilisateurs invités peut être difficile et prendre du temps, mais si un RBAC définit ces rôles avant qu'un utilisateur ne rejoigne le réseau, le problème est résolu d'emblée. Dès que des invités et nouveaux utilisateurs rejoignent le réseau, leur accès est prédéfini.

Pour les organisations possédant un nombre d'utilisateurs important avec une structure stable mais dans lesquelles la fréquence du changement du personnel est élevée, le modèle RBAC est considéré comme un système « idéal ». Dans un hôpital, par exemple, si des infirmières sont remplacées par d'autres infirmières, il n'est pas nécessaire d'affecter à ces dernières, une par une, l'ensemble des permissions qu'une infirmière doit avoir individuellement. Il suffit de lui affecter collectivement le même rôle des infirmières qu'elles remplacent. Il en va de même pour ajouter un nouveau patient, il suffit de lui affecter le rôle « patient » qui contient toutes les permissions nécessaires au lieu de lui affecter les permissions une à une comme dans d'autres modèles de contrôle d'accès. La Figure 3-1 représente le diagramme du modèle RBAC de base. Elle montre qu'un utilisateur

peut avoir de 0 à n rôles, chaque rôle peut avoir de 0 à n utilisateurs et/ou permissions, chaque permission peut être affectée de 0 à n rôles et chaque permission peut contenir une seule action sur un objet. [23]

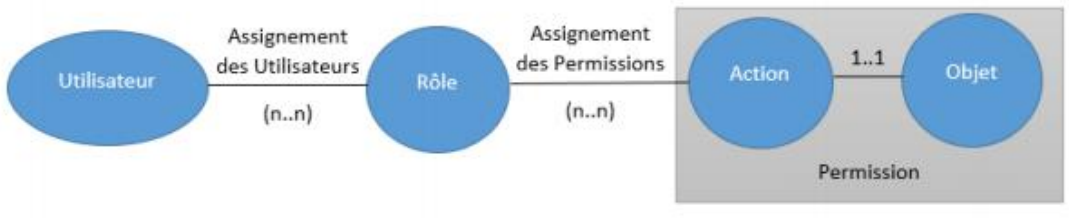


Figure 3-1: RBAC Basique

Le concept de session est aussi important pour le modèle RBAC, il consiste à affecter à un utilisateur des rôles actifs pour chaque session. Un utilisateur peut se connecter sur deux sessions différentes dans lesquels il n'y aurait pas nécessairement les mêmes autorisations d'accès.

3.3 Inconvénients RBAC :

- Expressivité limitée
  - ➔ Les sujets jouant le même rôle auront les mêmes permissions
  - ➔ Pas de permissions contextuelles
- Structuration limitée
  - ➔ Ne permet pas d'expliciter la structure d'une permission en fonction de l'application
- Modèle d'administration séparé du reste de RBAC
  - ➔ Notion de rôle administratif distincte des rôles standards

3.4 Caractéristique du RBAC :

Nous présentons ci-dessous un résumé sur les caractéristiques-clés du RBAC par rapport au MAC et DAC :

MAC:

- Basé sur l'administration.

- Règle le contrôle des flux d'information.

- Haut niveau de sécurité, d'où haute assurance, mais manque de flexibilité.

DAC:

- Basé sur la possession, flexible, plus largement utilisé.

- Ne fournit pas un haut niveau de sécurité, d'où faible assurance.

RBAC :

- Fournit une politique neutre/flexible.

- Satisfait le principe du moindre privilège.

- Satisfait la contrainte des séparations des devoirs.

- Caractéristiques administratives faibles.

- Capacité d'exprimer DAC, MAC, et les politiques spécifiques d'utilisateur en utilisant la hiérarchie des rôles et les contraintes.

- Peut être facilement incorporé dans les technologies courantes.

3.5 La famille des modèles RBAC

Parmi les différents modèles de RBAC, on cite une famille de quatre modèles conceptuels.

- Le modèle $RBAC_0$ ou « the flat model », qui présente les concepts et relations de base c.à.d. le noyau du modèle.

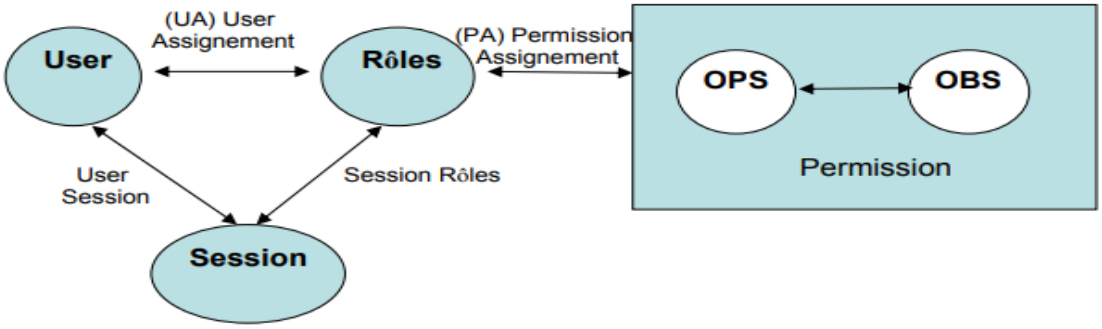


Figure 3-2: $RBAC_0$ Le modèle Basique

- Le modèle $RBAC_1$ ou « the hierarchical model », qui reprend le modèle

$RBAC_0$ et introduit la notion de hiérarchie entre rôles.

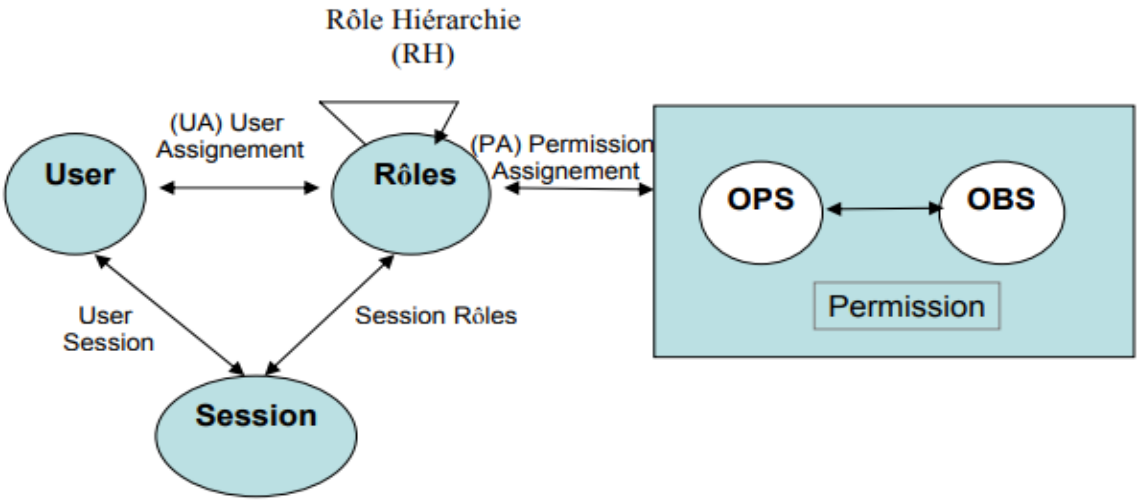


Figure 3-2: La hiérarchie $RBAC_1$

- Le modèle $RBAC_2$ ou « the constrained model », qui reprend le modèle $RBAC_0$ et introduit la notion de contrainte.

- Le modèle $RBAC_3$ ou « the symmetric model », qui reprend les modèles

$RBAC_1$ et $RBAC_2$ et prend en compte les interactions entre contraintes et hiérarchie.

La relation entre ces différents modèles est représentée dans la Figure 3-3. [25]

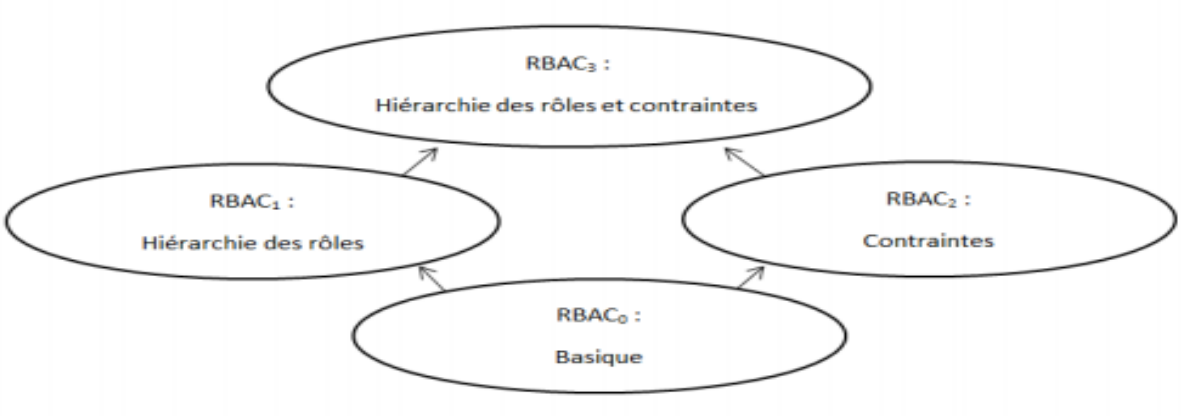


Figure 3-3: Relation entre les modèles RBAC

3.6 La modélisation du RBAC :

Le service de médecine physique et réadaptation du CHU Douera se compose de deux types de personnels, nous avons le personnel médical et le personnel administratif. Le personnel est représenté comme suit :

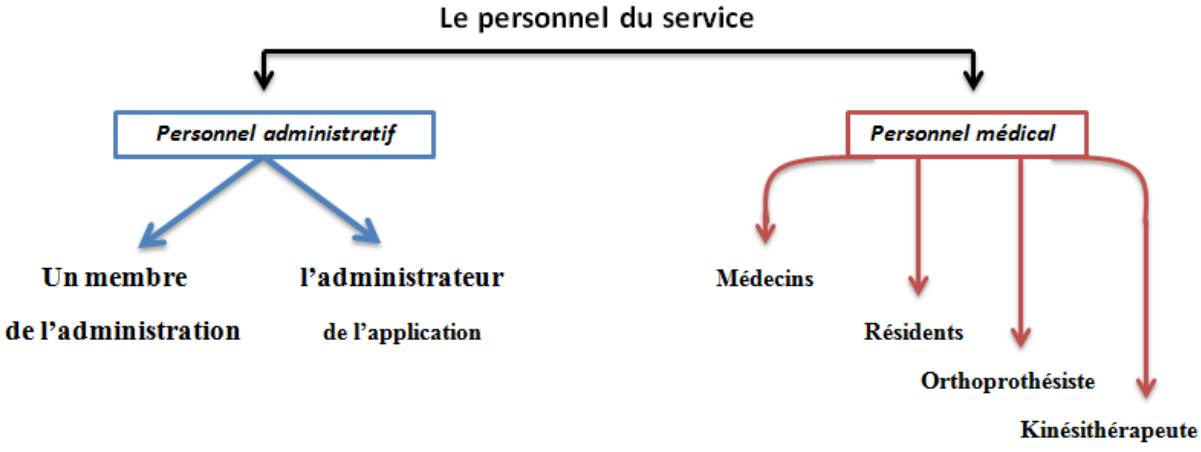


Figure 3-4: Représentation du personnel du service

Pour adapter le modèle RBAC au service, nous devons appliquer le modèle $RBAC_3$ qui combine les aspects de contraintes et de hiérarchies des rôles gérés par les deux autres modèles.

La combinaison de ces deux aspects est utile pour l'application de contraintes sur la hiérarchie des rôles.

Les composants de notre modèle $RBAC_3$ sont les suivants :

- Utilisateur : l'ensemble du personnel du service.
- Rôle : l'ensemble des rôles, où un rôle est la spécialité de l'utilisateur
- Permission : l'ensemble des autorisations afin d'effectuer des opérations sur un ou plusieurs objets protégés
- Opération : l'ensemble des opérations
- Objet : l'ensemble des objets ou des ressources du DMP

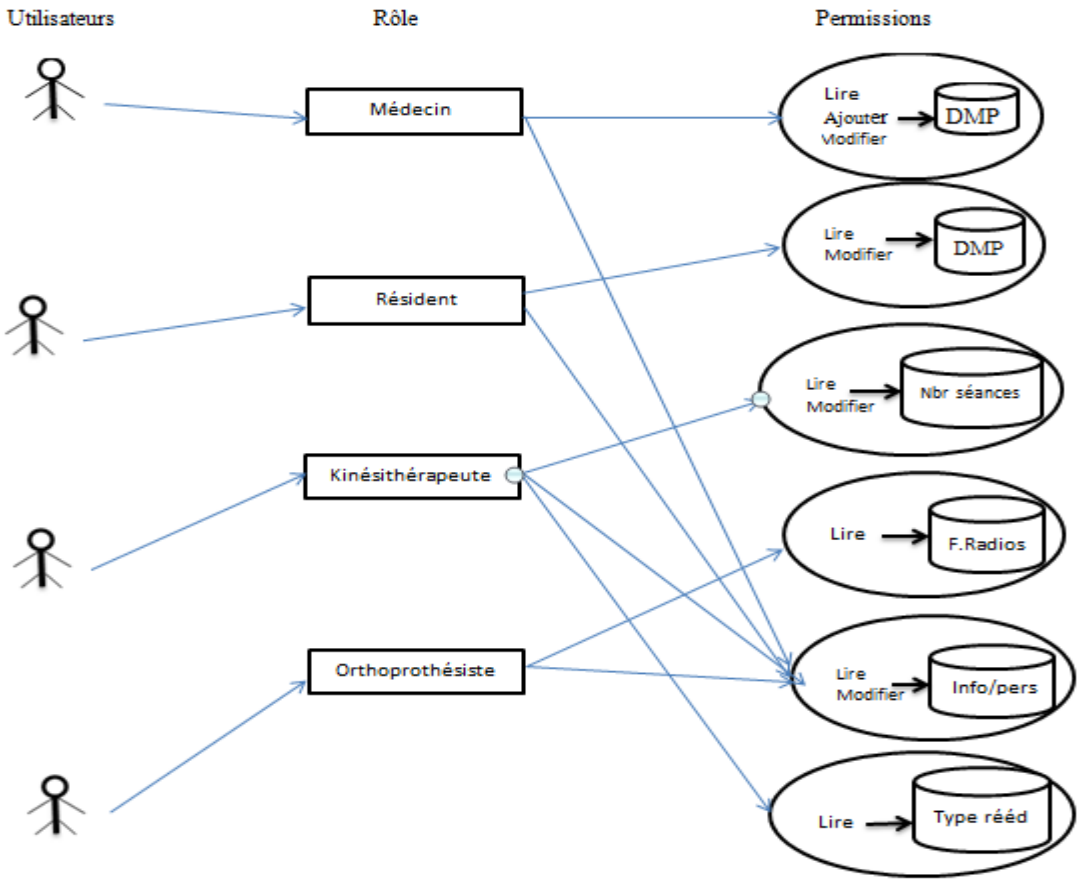


Figure 3-5: Modélisation du RBAC

3.6.1 La hiérarchie des rôles

Le concept de la hiérarchie des rôles permet à un rôle d'hériter des permissions de l'ensemble de ses sous-rôles.

Dans notre cas, le rôle « Médecin » hérite toutes les permissions du rôle «Résident». Il possède aussi des permissions spécifiques qu'un simple résident ne peut pas avoir. Le rôle « Médecin » c'est le rôle du plus haut niveau, il a toutes les permissions.

Dans notre cas il existe différents niveaux de rôles. Tant que le niveau est supérieur les permissions augmentent.

La figure suivante montre la hiérarchie des rôles dans le service et ses différents niveaux :

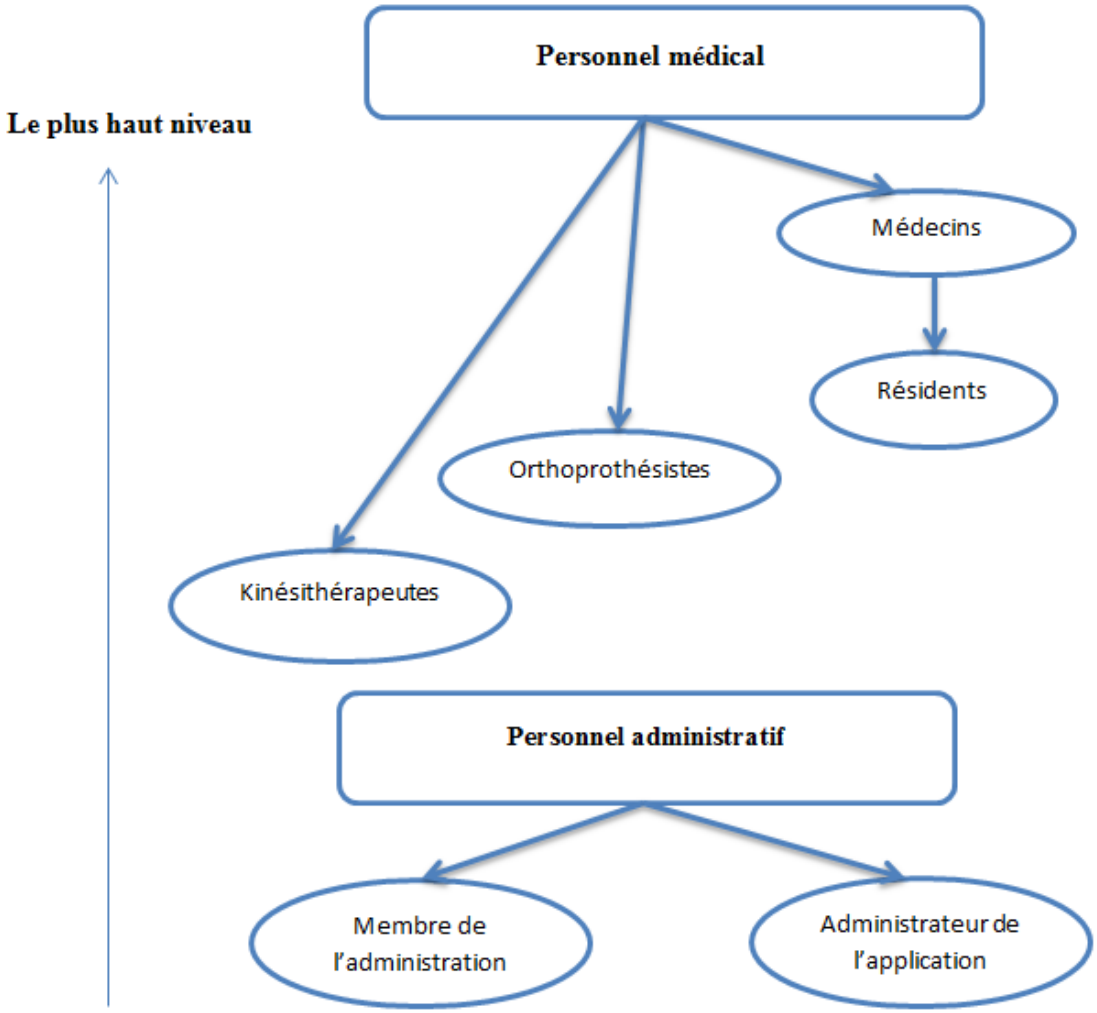


Figure 3-6: La hiérarchie des rôles dans le service

3.6.2 Les contraintes et cas d'exceptions

Les contraintes sont un aspect important du modèle RBAC. L'importance des contraintes se voit dans des rôles mutuellement disjoints.

Dans le service de médecine physique et réadaptation de CHU Douera existe différentes sortes de contraintes:

- Contraintes sur les affectations des rôles aux utilisateurs.
    - Un utilisateur ne peut pas avoir deux rôles disjoints au même temps.
      Les rôles disjoints à savoir : médecin, kinésithérapeute, orthoprothésiste, administrateur. Aucun d'eux ne peut prendre le rôle de l'autre.

- Contraintes sur les affectations des permissions aux rôles.
    - Dans le rôle « Médecin », on a toutes les permissions. Les médecins ont le droit d'accéder à tout le DMP.
    - Dans le rôle « Résident », on a la permission d'ajouter un patient, consulter ses informations personnelles, d'accéder aux fichiers de consultations mais on ne peut pas ajouter une nouvelle consultation ni modifier une.
    - Dans le rôle « orthoprothésiste», on a la permission qui permet de voir le dossier de radiologie et les informations personnelles uniquement.
    - Dans le rôle « kinésithérapeute», on a uniquement la permission d'accéder à la liste des patients qui nécessitent une rééducation et modifier le nombre des séances.
    - Dans le rôle « administration», on a la permission de voir les statistiques seulement.

- Contraintes sur les utilisateurs.
    - Tous les utilisateurs doivent être approuvés par l'administrateur de l'application.

. • Contraintes sur les rôles

    - Aucun rôle ne peut être affecté à des utilisateurs avant d'être approuvés.

- Contraintes sur les permissions :
    - Chaque permission correspond à un niveau d'habilitations de rôle précis.
- Cas d'exception :
    - En cas d'absence ou pendant les jours de congés, le médecin peut déléguer toutes ses permissions aux résidents.

3.7 Conclusion

Le contrôle d'accès représente l'une des stratégies de sécurité des systèmes informatiques. Cette stratégie a été conçue pour réduire le risque d'évènements non désirés. En effet, le contrôle d'accès permet d'autoriser ou d'interdire aux utilisateurs des actions sur des objets protégés.

Dans ce chapitre, nous avons présenté d'une façon détaillée le modèle RBAC qu'on va utiliser dans notre application.

Chapitre 4

L'implémentation et l'aspect sécuritaire

Le choix du modèle de contrôle d'accès a été expliqué dans le chapitre précèdent. Ce chapitre traite le côté pratique de notre travail, et l'aspect sécuritaire que nous avons employé pour protéger des données personnelles des patients.

Plusieurs solutions ont été proposées pour régler les problèmes de sécurité associés au dossier médical partageable (DMP) comme le contrôle d'accès, le chiffrement des données et autres.

4.1 Environnement de développement:

Pour réaliser notre application on a utilisé les outils suivants :

Matériel: Laptop - processeur i7, 8 GB RAM, Windows OS
Logiciel: Wamp, google chrome, phpmyadmin,
Langage: Php, Html, Css, Javascript, Sql,

Et le Framework Laravel.

4.1.1 php

Nous avons choisi le langage PHP et le Framework Laravel pour l'implémentation de notre système. PHP est un langage de scripts généraliste, Open Source, libre, impératif et orienté objet. Il est spécialement conçu pour le développement d'applications web. Il peut être intégré facilement au HTML.

4.1.2 Laravel

4.1.2.1 Definition

Laravel, créé par Taylor Otwel, initie une nouvelle façon de concevoir un Framework en utilisant ce qui existe de mieux pour chaque fonctionnalité. [27]

Laravel est un Framework web open-source écrit en PHP respectant le principe modèle-vue-contrôleur et entièrement développé en programmation orientée objet.

Laravel colle aux plus récentes avancées de PHP et surtout à son approche objet.

4.1.2.2 Architecture MVC

Laravel, comme une grande partie des autres Framework php, a une architecture dite MVC (Model – View – Controller). Voici une illustration simple pour vous faire comprendre rapidement la logique de cette architecture. [28]

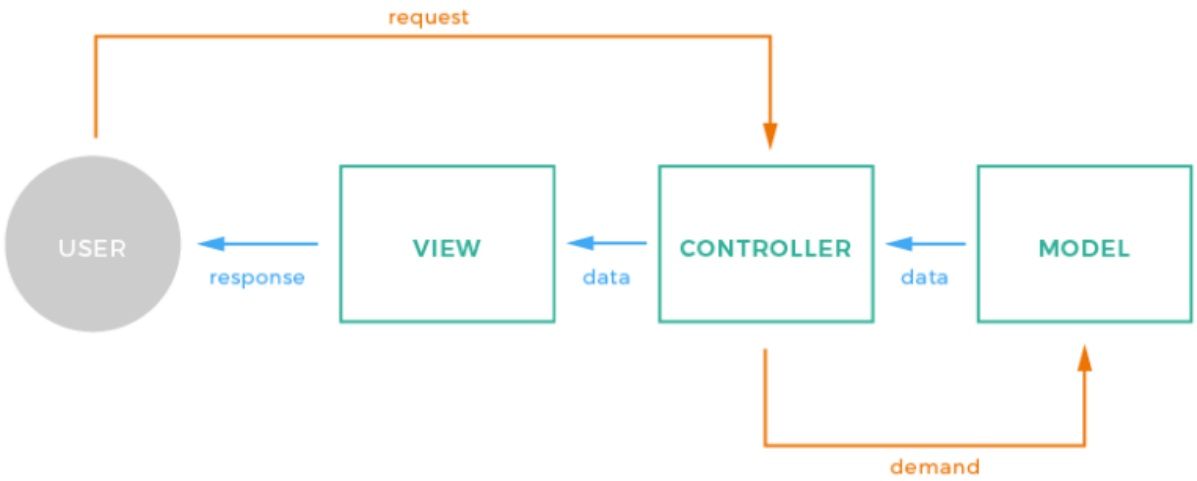


Figure 4-1: le modèle MVC

Chaque action de l'utilisateur passe par le contrôleur (controller) qui envoie des demandes de manipulation d'un objet au modèle. Le modèle (model) effectue les changements de l'objet et le renvoie au contrôleur qui à son tour le passe à la vue (view). Ainsi ces trois pôles ont des responsabilités différentes :

• Le **model** contient les données et leur logique.

• La **view** contient la présentation graphique à renvoyer à l'utilisateur.

• Le **controller** traite les actions utilisateur (via des requêtes), demande au modèle d'effectuer les changements, puis passe les données à la vue.

Le controller a donc une place centrale dans cette architecture. Il est le pont entre les interactions utilisateur et les traitements de données. Tout passe par lui afin de pouvoir tout contrôler.

4.1.2.3 Avantage de laravel

- Un Framework fait gagner du temps et donne l'assurance de disposer de composants bien codés et fiables.

- Laravel est un Framework novateur, complet, qui utilise les possibilités les plus récentes de PHP et qui est impeccablement codé et organisé.

- Laravel adopte le patron MVC mais ne l'impose pas, il est totalement orienté objet.

- La documentation de Laravel est complète et précise.

4.2 Analyse et conception

La réalisation de l'application doit être impérativement précédée d'une méthodologie d'analyse et de conception qui a pour objectif de permettre de formaliser les étapes préliminaires du développement afin de rendre ce développement plus fidèle aux besoins du client. La phase d'analyse permet de lister les résultats, en termes de fonctionnalités. La phase de conception permet de faciliter la réalisation.

4.2.1 Identification des besoins fonctionnels et non fonctionnels

Cette étape consiste à comprendre le contexte du système. Il s'agit de déterminer les fonctionnalités et les acteurs et d'identifier les cas d'utilisation initiaux. Nous

présentons dans ce qui suit tous les besoins fonctionnels classés par acteur ainsi que les besoins non fonctionnels communs à tous ces acteurs.

4.2.1.1 Besoins fonctionnels

- Médecin
  - Modifier ses informations personnelles
  - Accéder à la liste des patients
  - Ajouter/modifier un patient
  - voir la fiche des informations des patients
  - Ajouter/modifier une consultation
  - Accéder aux fichiers de consultations
  - La recherche
  - Gérer les rendez-vous
  - Déléguer ses permissions

- Résident
  - Modifier ses informations personnelles
  - Accéder à la liste des patients
  - Ajouter/modifier un patient
  - voir la fiche des informations des patients
  - Accéder aux fichiers de consultations
  - La recherche
  - Gérer les rendez-vous

- Orthoprothésiste
  - Modifier ses informations personnelles
  - Voir la fiche radiologique
  - Accéder aux dossiers de radiologie

- Kinésithérapeute
  - Modifier ses informations personnelles
  - Voir le type de rééducation
  - modifier le nombre de séances de la rééducation

- Administrateur de l’application

  - Approuver les utilisateurs

- Administration

  - voir les statistiques

4.2.1.2 Besoin non fonctionnel

- Simplicité et homogénéité du design.

- Rapidité d'exécution.

4.3 Déploiement de l'application:

4.3.1 Architecture de l'application:

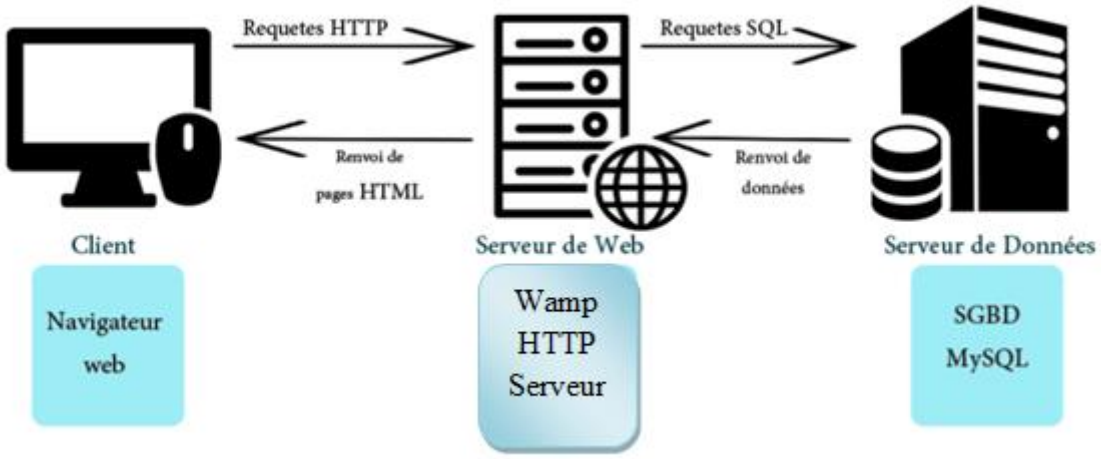


Figure 4-2: L'architecture de l'application

4.3.2 Présentation de l'application

Pour pouvoir accéder au DMP, les différents utilisateurs doivent se connecter s'ils ont déjà été inscrits sinon ils doivent s'inscrire.

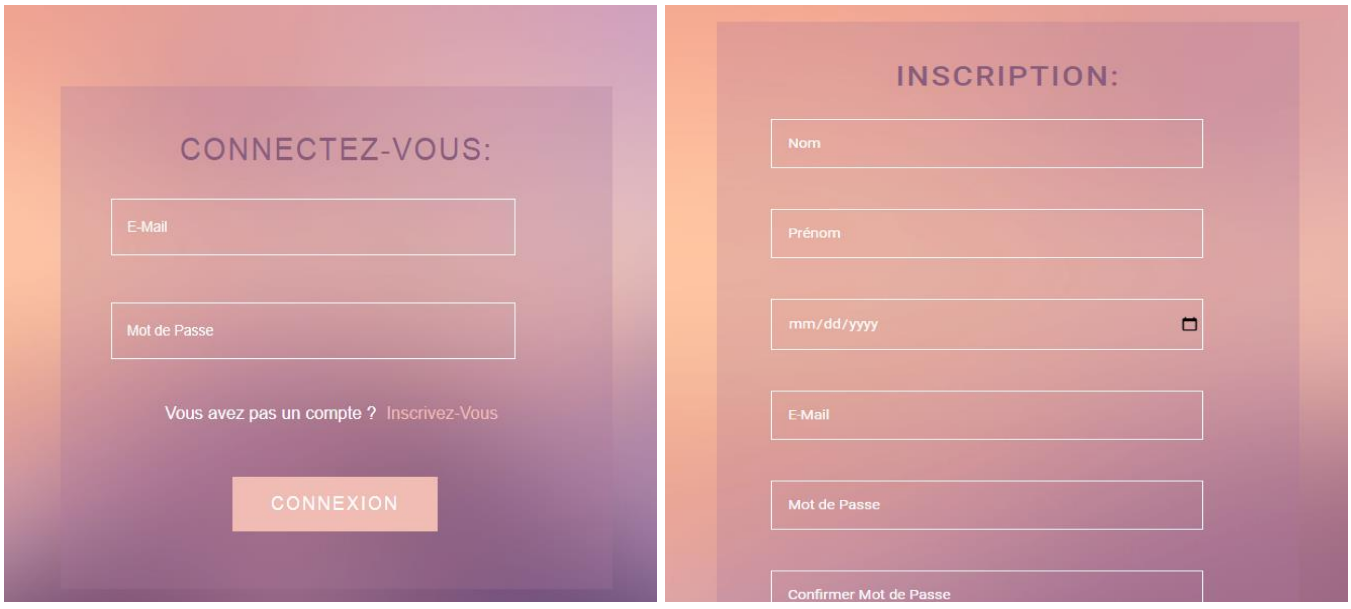


Figure 4-3: L'interface de connexion et d'inscription

Pour pouvoir s'inscrire, les utilisateurs doivent remplir leurs informations personnelles ainsi que scanner un code QR qui permet d'identifier leur spécialité qui nous sert de ROLE.

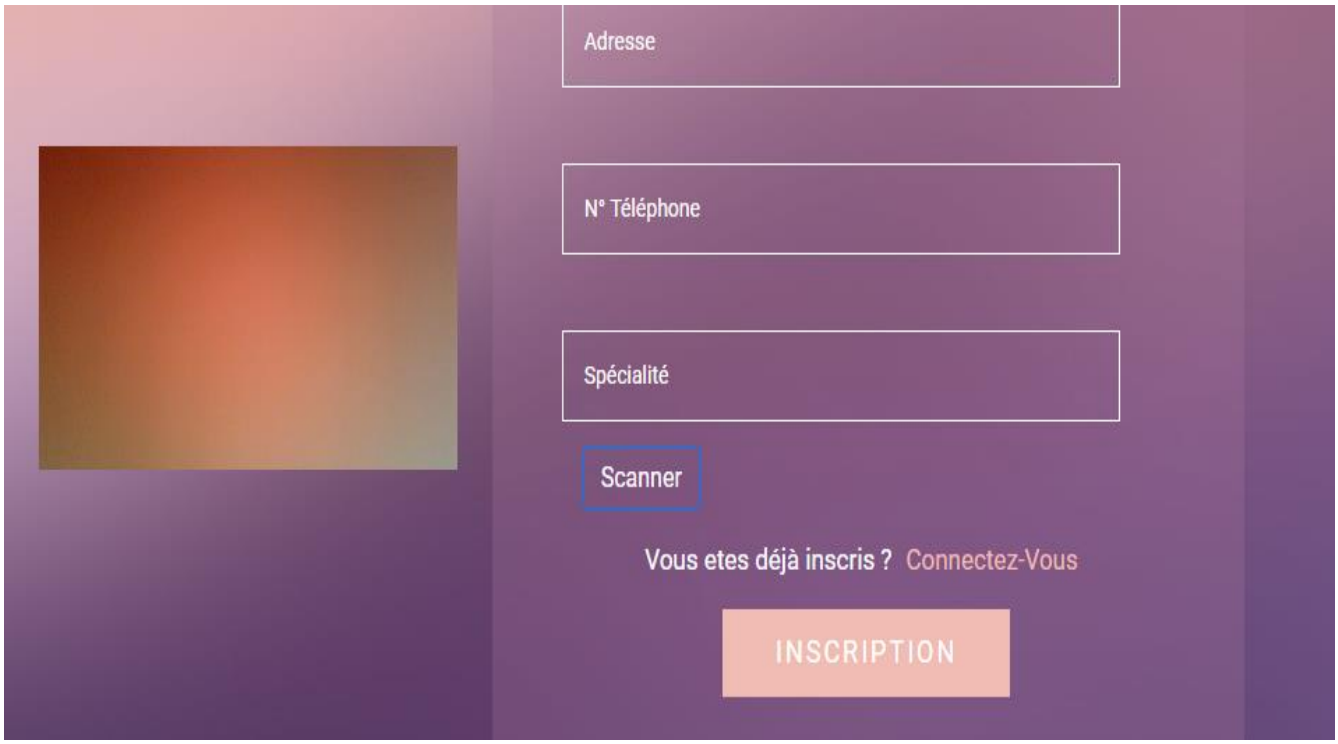
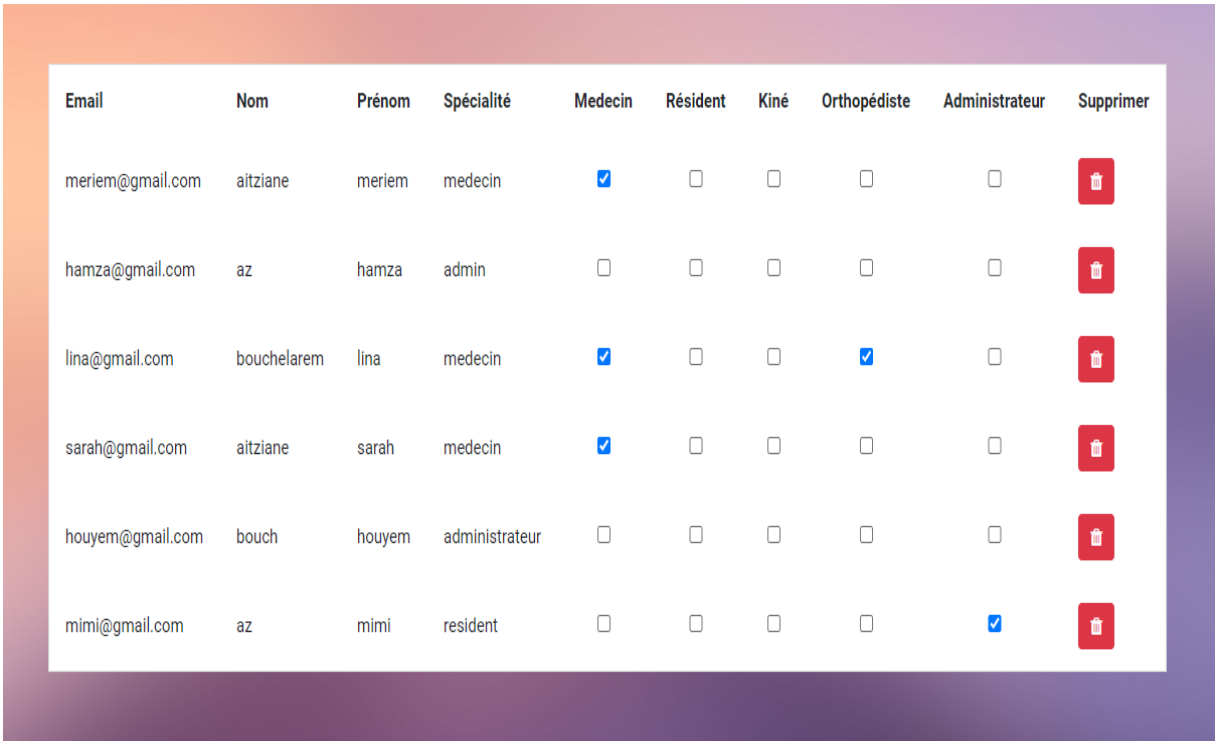


Figure 4-4: L'interface pour scanner le code QR

Après l'inscription, les utilisateurs auront accès uniquement à l'accueil de l'application. L'administrateur doit les approuvé pour qu'ils puissent se connecter au DMP.



Email	Nom	Prénom	Spécialité	Medecin	Résident	Kiné	Orthopédiste	Administrateur	Supprimer
meriem@gmail.com	aitziane	meriem	medecin	☑	☐	☐	☐	☐	🗑
hamza@gmail.com	az	hamza	admin	☐	☐	☐	☐	☐	🗑
lina@gmail.com	bouchelarem	lina	medecin	☑	☐	☐	☑	☐	🗑
sarah@gmail.com	aitziane	sarah	medecin	☑	☐	☐	☐	☐	🗑
houyem@gmail.com	bouch	houyem	administrateur	☐	☐	☐	☐	☐	🗑
mimi@gmail.com	az	mimi	resident	☐	☐	☐	☐	☑	🗑

Figure 4-5: L'interface pour approuver les utilisateurs

Après avoir été approuvé chaque utilisateur à un rôle précis donc des permissions bien précises et différentes.

Figure 4-6: L'interface d'accueil

Figure 4-7: Les menus de l'accueil

Les médecins et résidents peuvent ajouter/modifier/rechercher un patient grâce à la liste des patients qui est mis à leur disposition

Figure 4-8: L'interface de la liste des patients

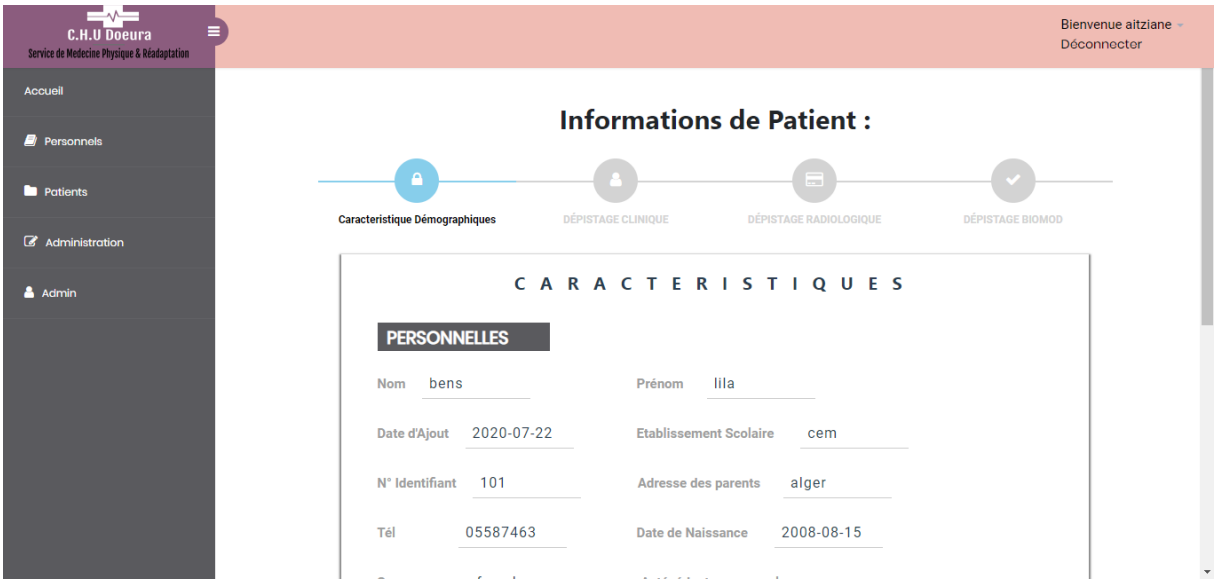


Figure 4-9: L'interface des informations des patients

Pour effectuer une consultation le médecin doit remplir une fiche de consultation qui se compose de plusieurs étapes.

Figure 4-10: L'interface de la fiche de consultation

Après la consultation, le médecin décide si le patient a besoin d'une rééducation.

L'orthoprothésiste consulte la liste et la fiche radiologique des patients qui ont besoin d'une rééducation uniquement.

Figure 4-11: L'interface d'orthoprothésiste

Et le kinésithérapeute consulte la liste des patients avec le type de rééducation et le nombre de séance nécessaire.

Figure 4-12: L'interface du kinésithérapeute

Les médecins peuvent gérer leur droit d'accès et le déléguer aux résidents en cas d'absence ou autre.

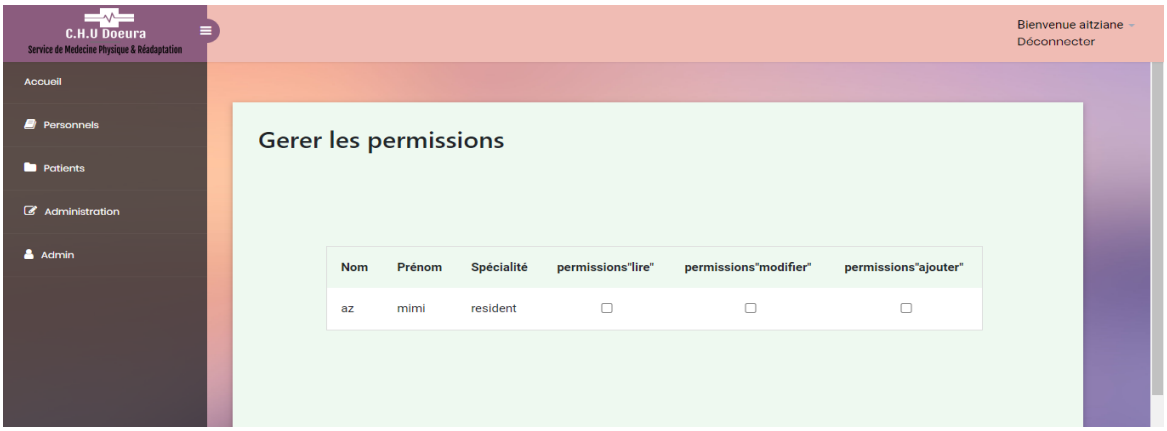


Figure 4-13: L'interface pour gérer les permissions

Les différents utilisateurs d'application peuvent consulter/modifier leurs informations personnelles

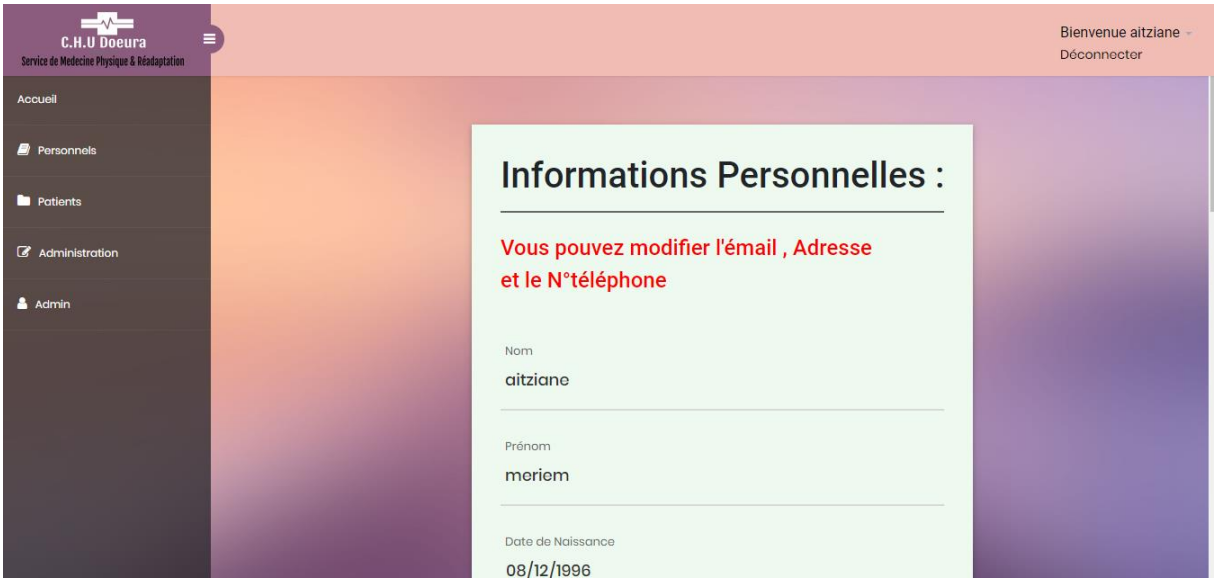


Figure 4-14: L'interface des informations personnelles

Si un utilisateur essaye d'accéder à une information à qui n'a pas la permission, un message d'erreur est affiché.

Figure 4-15: L'interface du message d'erreur

4.3.3 L'implémentation du RBAC

Pour implémenter le modèle RBAC, il existe plusieurs méthodes mais celle qu'on a utilisée dans notre application est la méthode la plus professionnelle, elle nous permet d'attribuer les rôles, les permissions et les autorisations, également on peut la contrôler parfaitement

L'implémentation se fait en suivant les étapes suivantes :

Parmi les différentes tables de la base de données, on a créé une table qui relie deux tables ROLE/USER, car chaque user peut avoir plusieurs rôles et chaque rôle peut être associé à plusieurs user, c'est pour cela qu'on est obligé d'avoir une relation many to many (plusieurs à plusieurs), et cette relation nous impose à utiliser une table intermédiaire rôle-user.

Le code pour relier les deux tables dans Laravel est dans la figure suivante :

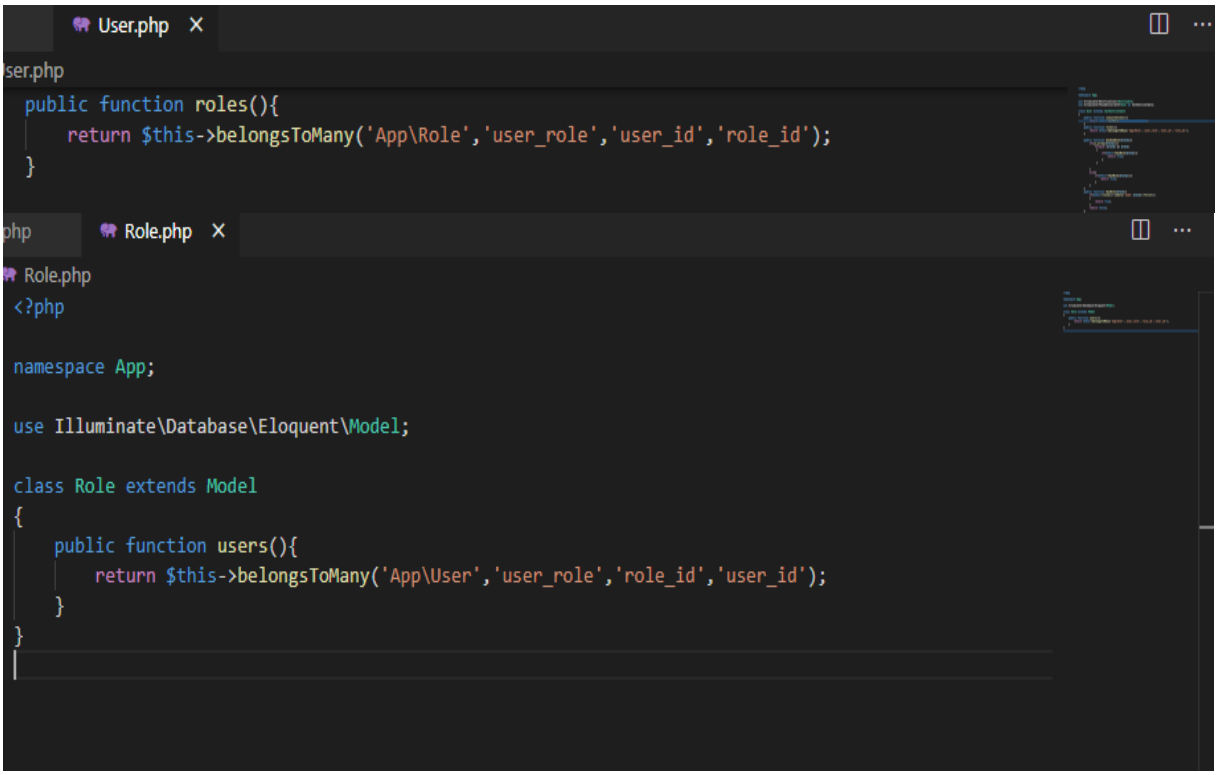


Figure 4-16: Le code pour relier les tables rôle/user

La deuxième étape, c'est l'étape la plus importante qui consiste a créé un nouveau middleware.

Le middleware est une fonction qui s'interpose entre l'appel de la route et l'exécution du code qui est appelé par cette route, il permet d'enrichir ou de vérifier une requête avant qu'elle arrive au contrôleur.

Plusieurs middlewares sont fournis de base avec Laravel comme ***auth*** pour autoriser l'accès à la route seulement aux requêtes liées à un utilisateur connecter.

Pour créer un nouveau middleware ***checkRole*** :

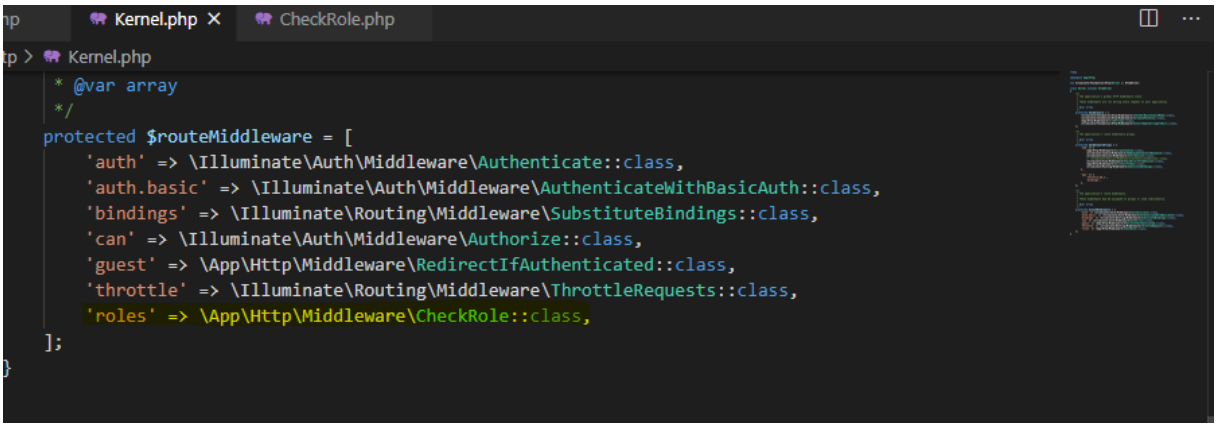


Figure 4-17: Le code pour créer un middleware

Le middleware ***checkRole*** vérifie quel rôle est associé a quel user.

Il vérifie les permission des users, si les permissions sont valables alors le ***user*** peut continuer, par contre si les autorisations ne respectent pas les conditions on affiche un message d'erreur.

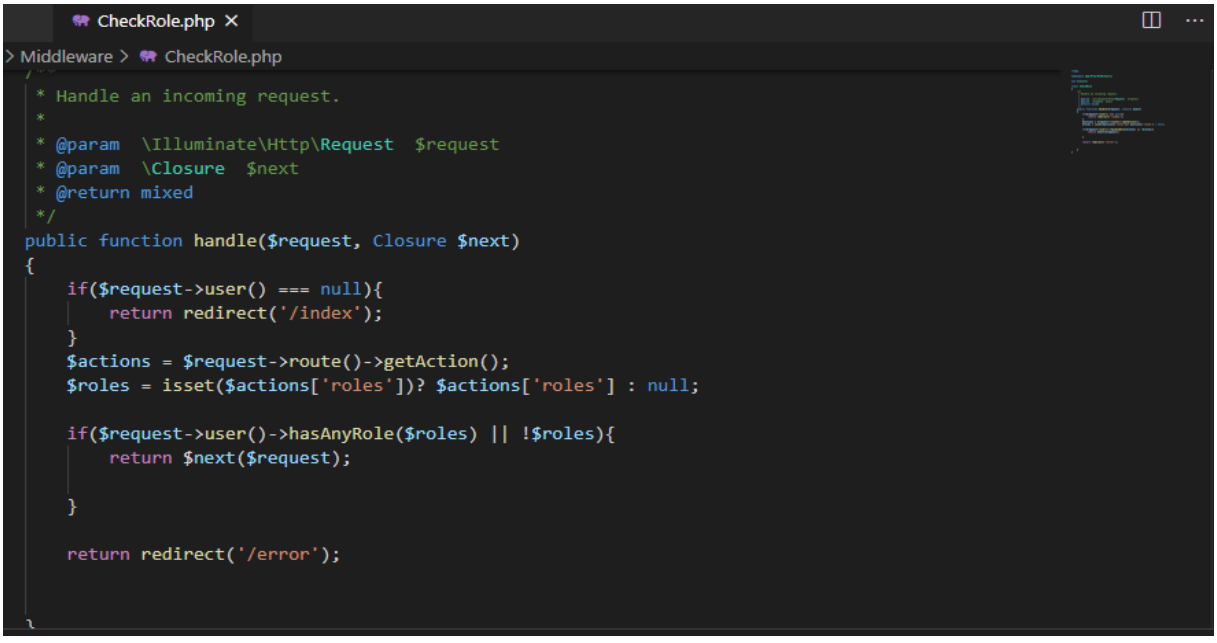


Figure 4-18: Le middleware checkRole

L’étape suivante consiste à utiliser la fonction ***hasAnyRole*** pour identifier le rôle de l’utilisateur.

User.php

```php
    }

    public function hasAnyRole($roles){
        if(is_array($roles)){
            foreach ($roles as $role)
            {
                if($this->hasRole($role)){
                    return true;
                }
            }

        }
        else{
            if($this->hasRole($roles)){
                return true;
            }
        }
    }
    public function hasRole($role){
        if($this->roles()->where('name',$role)->first())
        {
            return true;
        }
        return false;
    }
```

Figure 4-19: La fonction hasAnyRole

La dernière étape c'est l'utilisation du nouveau middleware qu'on a créé

Figure 4-20: L'utilisation du middleware

Après avoir mis en place les rôles, nous avons accordé des permissions à ces rôles

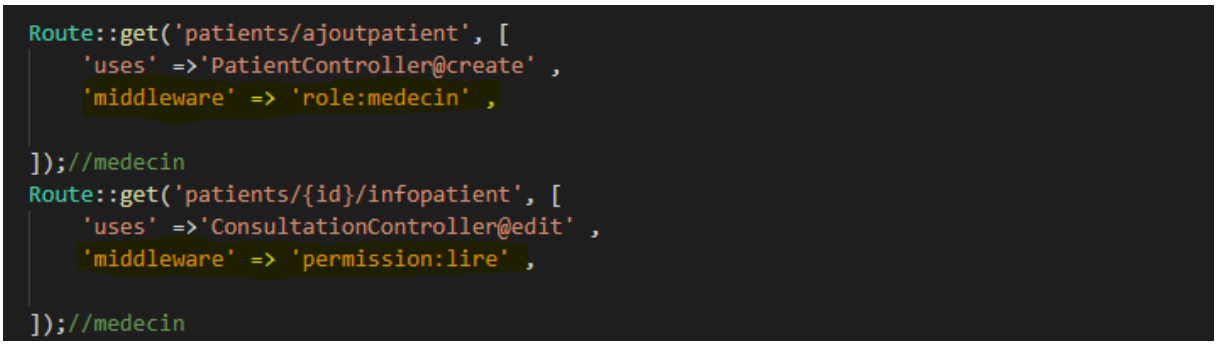


Figure 4-21: Exemple de l'accord d'une permission à un rôle

4.4 L'aspect sécuritaire

4.4.1 QR CODE

Le code QR est un type de code-barres en deux dimensions constitué de modules noirs disposés dans un carré à fond blanc. L'agencement de ces points définit l'information que contient le code.

Dans notre application, nous avons utilisé des codes QR pour définir les rôles des utilisateurs.

Le DMP est un dossier très sensible, qui nécessite un très haut niveau de sécurité.

Pour s'inscrire les utilisateurs doivent enregistrer leurs informations personnelles et leurs professions qui sont dans notre cas les RÔLES, ensuite l'administrateur doit les accepter pour qu'ils puissent s'authentifier.

L'erreur est humaine, si par exemple une infermière s'inscrit par erreur comme étant un médecin et l'administrateur l'accepte par manque de concentration. L'infermière aura accès à des informations qu'elle n'est pas supposée voir.

Notre travail tourne principalement autours des rôles donc pour renforcer la sécurité et pour éviter toute erreur que ce soit une erreur de frappe ou des pensées malsaines, de la part des utilisateurs ou de l'administrateur, on a met en œuvre un système pour protéger le DMP.

A l'inscription, L'utilisateur ne va pas mettre son rôle lui-même, mais il doit scanner le code QR de son badge qui représente son rôle.

Grace au code QR le rôle est pris automatiquement, et l'administrateur doit vérifier si l'utilisateur est un membre du personnelle du service pour l'accepter.

La figure suivante représente le badge d'un membre du personnel.

Figure 4-22: Badge avec le QR code

4.4.2 Le hashage

Laravel possède la façade Hash qui permet de faire du hashage. C'est ce qui est utilisé pour l'encryption du mot de passe dans Auth/RegisterController :

Laravel peut utiliser 3 types d'encryption :

- bcrypt
- argon
- argon2

Dans notre cas, on a travaillé avec bcrypt.

bcrypt est une fonction de hachage créée par Niels Provos et David Mazières. Elle est basée sur l'algorithme de chiffrement Blowfish et a été présentée lors de USENIX en 19991. En plus de l'utilisation d'un sel pour se protéger des attaques par table arc-en-ciel (rainbow table), bcrypt est une fonction adaptative, c'est-à-dire que l'on peut augmenter le nombre d'itérations pour la rendre plus lente. Ainsi elle continue à être résistante aux attaques par force brute malgré l'augmentation de la puissance de calcul. [29]

Blowfish est un algorithme de chiffrement par bloc.

4.4.3 Le cryptage des données

Toute personne prise en charge par un professionnel ou un établissement de santé a droit au respect de sa vie privée et au secret des informations la concernant. Les professionnels de santé, ainsi que ceux intervenant dans le système de santé, sont soumis au secret médical.

Le chiffrement des informations stockées est une mesure technique pour la protection, cela signifie que l'information sur la santé ne peut être lue que par les personnes qui utilisent un système qui peut les décrypter avec une clé.

Nous utilisons le décodage en base 64 pour commencer l'opération. nous allons utiliser des pseudo octets ssl aléatoires ouverts pour rendre cette chaîne aussi compliquée que possible. Ensuite, nous allons utiliser openssl encrypt. Ensuite, nous utilisons aes-256-cbc qui n'est pas crackable sans la clé. Enfin, nous

retournons la chaîne cryptée en base 64 et comme ça nous avons une chaîne cryptée.

Et pour déchiffrer les données, nous décodons en utilisant la base 64. Notez que nous avons également notre clé dedans. Ensuite, nous utilisons la fonction list en PHP pour interpréter notre tableau. Ensuite, nous utilisons openssl decrypt pour décrypter notre chaîne avec notre clé.

Figure 4-23: la base de données cryptée

4.4.4 Les injections SQL

Une injection SQL est une attaque qui consiste à ajouter à une requête inoffensive un complément qui peut être dangereux pour l'application

L'injection sql est un groupe de méthodes d'exploitation de faille de sécurité d'une application interagissant avec une base de données.

L'un des avantages les plus importants du choix de Laravel pour le développement de notre application Web réside dans ses capacités à fournir une sécurité de haut niveau. L'application ne présente aucun risque d'injections SQL involontaires et cachées grâce à Eloquent l'ORM de Laravel. Un ORM (Object-Relational Mapping) est un logiciel permettant la conversion des données relationnelles d'une base de données en objets afin de pouvoir les manipuler dans notre application en POO. [30]

Par contre si vous faites des requêtes avec par exemple DB::raw() ou whereRaw, autrement dit si vous contournez Eloquent, alors vous devez vous-même vous prémunir contre les attaques SQL.

4.4.5 CSRF

Cross-site request forgery est un type de vulnérabilité des services d'authentification web.

Grâce au système d'authentification de Laravel cette faille est gérée automatiquement par Laravel.

4.5 Conclusion:

Dans la partie réalisation, on a présenté les différents outils et langage utilisés dans l'implémentation de notre application. Par la suite, on a présenté les méthodes de sécurité utilisées.

L'application offre toutes les fonctions nécessaires au bon fonctionnement d'un DMP.

Nous pensons avoir atteint les objectifs initiaux, mais pouvons encore en améliorer quelques aspects esthétiques et fonctionnels pour le rendre plus attractif et plus marchand.

Conclusion Générale

Ce mémoire avait pour ambition de protéger les données personnelles médicales informatisées de service de rééducation fonctionnelle de l'hôpital de Douera. La clé de la protection de ces données est de s'assurer que seules les professionnels de santé ayant droit peuvent y accéder, et pour cela on a adapter un modèle de contrôle d'accès le plus adéquat afin d'éviter que les données manipulées ne soient utilisées de façon inappropriée.

Dans ce mémoire nous avons présenté dans le chapitre 1, la sécurité des systèmes d'information et le système d'information hospitalier ainsi que les principaux modèles de contrôle d'accès classiques.

Ensuite, dans le chapitre 2 nous avons présenté les principes de sécurité et de protection des données personnelles relatifs au domaine de la santé et particulièrement au dossier médical partageable.

Et finalement dans chapitres 3 et 4 on a terminé par une présentation de notre architecture de politique de sécurité qui repose sur le model RBAC ainsi que les différents environnements de développement que nous avons utilisé pour réaliser notre projet, et aussi l'aspect sécuritaire qu'on a ajouté pour renforcer la sécurité du DMP.

Enfin, notre projet contient un système de protection qui consiste à sécuriser les données personnelles médicales d'une façon unique afin de mettre l'utilisateur dans un environnement de confiance.

- Bibliographie :

- Références documentaires :

[1] : THION, Romuald. STRUCTURATION RELATIONNELLE DES POLITIQUES DE CONTRÔLE D'ACCÈS REPRÉSENTATION, RAISONNEMENT ET VÉRIFICATION LOGIQUES. 2008. Thèse de doctorat. Institut National des Sciences Appliquées de Lyon.

[2] : ITSEC, Critères d'évaluation de la sécurité des systèmes informatiques, v1.2, 163p., ISBN 92-826-3005-6, Office des publications officielles des Communautés Européennes, Luxembourg, 1991.

[3] : KALAM, Anas Abou El, BAIDA, R. E., BALBIANI, Philippe, et al. Organization based access control. In : Policies for Distributed Systems and Networks, 2003. Proceedings. POLICY 2003. IEEE 4th International Workshop on. IEEE, 2003. p. 120-131.

[4] : A. Jøsang, J. Fabre, B. Hay, J. Dalziel, S. Pope. Trust Requirements in Identity Management. Australasian Information Security Workshop 2005 volume 44, pages 99- 108, 2005.

[5] : ISO/IEC 24760-1:2011(E). ISO/IEC, 20 pages, 2011.

[6] : A. Balat, R. Bergeron, A. Butel, M. Cottreau, F. Depierre, G. Khouberman, L. Mourer, W. Poloczanski. Gestion des identités. CLUSIF, 63 pages, 2007.

[7] : ABOBA, Bernard, ARKKO, Jari, et HARRINGTON, David. Introduction to accounting management. RFC 2975, October, 2000.

[8] : MEKKANE ,Salem. Un modèle de contrôle d'accès pour la protection des données personnelles dans le dossier médical partageable.2015. Thème de magister. Université A-MIRA-BEJAIA.

[9] : LAMPSON, Butler W. Protection. ACM SIGOPS Operating Systems Review, 1974, vol. 8, no 1, p. 18-24.

[10] : HARRISON, Michael A., RUZZO, Walter L., et ULLMAN, Jeffrey D. Protection in operating systems. Communications of the ACM, 1976, vol. 19, no 8, p. 461-471.

[11] : François KOLER : Informatique médicale, CHRU Nancy, instigateur du premier DESS information médicale.

[12] : Eric TOUSSAINT : historien belge, président du Comité pour l'abolition de la dette du Tiers Monde, membre du Conseil international du Fond Social Mondial.

[13] : HAS : Evaluation des pratiques professionnelles dans les établissements de santé. Dossier du patient : réglementation et recommandations, Service évaluation des pratiques, juin 2003.

[14] : LE DOSSIER DE SANTÉ ÉLECTRONIQUE: le contrôle des données personnelles de santé dans un contexte d'informatisation des dossiers médicaux, Commissariat à la vie privée du Canada. 2010.

[15] : VÉRIFICATEUR GÉNÉRAL DU QUÉBEC. Rapport du Vérificateur général du Québec à l'Assemblée nationale du Québec pour l'année 2009-2010, chapitre 6 (Vigie relative au projet Dossier de santé du Québec), mai 2009, aux pages 6 et 7.

[16] : Walter HANHART. Le dossier médical informatisé. Institut de droit de la santé.

[17] : WARDEN v. HAYDEN., 387 U.S. 294 United States Supreme Court (1967).

[18] : American Health Information Management Association. Auditing copy and paste. J Am Health Inf Management Assoc. 2009;80(1):26-29. Web Site:http://www.ahima.org/, consulted 2013.

[19] : Alan Westin's Legacy of Privacy and Freedom, Web site: https://www.privacyassociation.org/privacy_perspectives/post/alan_westins_legacy_of_privacy_and_freedom.

[20] : WANG, Yifei, SMITH, Sean W., et GETTINGER, Andrew. Access control hygiene and the empathy gap in medical IT. In : Proceedings of the USENIX Workshop on Health Security and Privacy. 2012.

[21] : D. Ferraiolo, J. Cugini et R. Kuhn, «Role-based access control (RBAC): Features and motivations», In Proceedings of the Annual Computer Security Applications Conference, IEEE Press, Los Alamitos, CA, 1995.

[22] : HASSEN KHALIFA. Détection des anomalies entre les contraintes dans les politiques de contrôle d'accès. Université du Québec en outaouais.

[23] : D. Ferraiolo, J. Cugini et R. Kuhn, «Role-based access control (RBAC): Features and motivations», In Proceedings of the Annual Computer Security Applications Conference, IEEE Press, Los Alamitos, CA, 1995.

[24] : F.D. Ferraiolo, R. Sandhu, S. Gavrila, D.R. Kuhn, R.Chandramouli, Proposed NIST standard for role-based access control, ACM Transaction on Information and System Security, Vol. 4, No. 3, Page 224-274, 2001.

[25] : R. Sandhu, E. Coyne, H. Feinstein et C. Youman, «Role-based access control models», IEEE Computer, vol. 29, n°12, pp. 38-47, 1996.

[26]: ABAKAR, Mahamat Ahmat. . Étude et mise en œuvre d'une architecture pour l'authentification et la gestion de documents numériques certifiés. Application dans le contexte des services en ligne pour le grand public. 2012. Thèse de Doctorat. Université Jean Monnet de Saint- Étienne.

- Références Internet :

[27] : *<< Framework Laravel>>* [En ligne] https://openclassrooms.com/fr/courses/3613341-decouvrez-le-framework-php-laravel/3616233-presentation-generale

[28] : *<<architecture mvc de Laravel >>* [En ligne] https://walkerspider.com/cours/laravel/architecture-mvc

[29] : *<<La sécurité Laravel >>* [En ligne] https://laravel.sillo.org/cours-laravel-6-la-securite/

[30] : *<< Laravel >>* [En ligne] https://walkerspider.com/cours/laravel