جامعة أبو بكر بلقايد- تلمسان

Université Abou Bakr Belkaïd de Tlemcen

Faculté de Technologie

Département de Génie Biomédical

MEMOIRE DE PROJET DE FIN D'ETUDES

Pour l'obtention du Diplôme de

MASTER en GENIE BIOMEDICAL

Spécialité : **Informatique Biomédicale**

Présenté par : DERBALE Asma et MEHENNI Ouassila

Sécurisation du dossier médical à base d'ontologie

Soutenu le 3 Juillet 2019 devant le Jury

M.	Bechar Hassane	*Docteur*	Université de Tlemcen	Président
M.	Abderrahim Med El Amine	*MCA*	Université de Tlemcen	Encadreur
Mme.	Belaidi Asma	*Docteur*	Université de Tlemcen	Co-encadreur
M.	Moussaoui Djillali	*MAA*	Université de Tlemcen	Examinateur

Année universitaire 2018-2019

Résumé

Le dossier médical informatisé est constitué d'informations administratives et médicales nominatives qui forment une base de données accessible par les nouvelles technologies, il a été conçu pour améliorer le suivi médical. Sa mise en place et sa confidentialité reste une question à laquelle il faut trouver une solution optimale pour une meilleure protection de données et respect de la vie privé.

Dans ce mémoire de master, nous allons proposer une modélisation du contrôle d'accès au dossier médical basée sur le modèle à base d'organisation Or-BAC et d'ontologie.

Pour la validation, nous avons implémenté ce modèle à l'aide des outils de gestion des ontologies. Le modèle ainsi développé a été intégré dans une application de gestion du dossier médical.

Abstract

The computerized medical file is made up of administrative and medical information, which forms a database accessible, by new technologies, it was designed to improve medical monitoring, and its implementation and its confidentiality remains a question to be found an optimal solution for better data protection and respect for privacy.

In this master thesis and based on the Or-BAC organization model and ontology, we will propose a modeling of the access control to the medical record.

For validation, we implemented this model by using ontology management tools. The model developed in this way has been integrated into a medical record management software.

ملخص

يتكون الملف الطبي الالكتروني من معلومات إدارية وطبية تشكل قاعدة بيانات يمكن الوصول إليها بواسطة التقنيات الحديثة، وقد تم تصميمها لتحسين المراقبة الطبية وتنفيذها. حيث تظل سريتها مسألة قائمة لذلك يجب ايجاد الحل الأمثل لها من اجل ضمان حماية البيانات بشكل أفضل واحترام خصوصية الفرد.

في هذه الرسالة، واستناداً إلى النموذج **Or-BAC** وعلم الأنطولوجيا، سنقترح نمذجة للتحكم في الوصول إلى الملف الطبي.

للتحقق من صحة النموذج المطور ، قمنا بتنفيذه عمليا باستخدام أدوات إدارة الأنطولوجيات . وفي الأخير تم دمج هذا النموذج في برنامج لإدارة الملفات الطبية.

Remerciement

À notre encadreur

Monsieur Abderrahim Med El Amine

Pour la confiance que vous nous avez accordée en nous proposant ce travail, pour votre implication, votre soutien et pour nous avoir fait l'honneur de présider cette thèse.

À notre co-encadreur

Mme. Belaidi Asma

Pour avoir accepté de diriger ce travail et pour les précieuses remarques que vous nous avez apportées pour l'améliorer.

À Monsieur le Président de jury

M. Bechar Hassane

On vous remercie chaleureusement de présider ce Jury. Votre présence nous ravit. Permettez-nous de vous exprimer notre profond respect, et nos remerciements.

À Monsieur le Pr. Moussaoui Djillali

Vous nous faites un grand honneur en acceptant d'examiner ce travail, on tient à vous exprimer nos sincères reconnaissances.

À ma mère

Nulle dédicace ne saurait t'exprimer toute ma gratitude et ma reconnaissance. **M**aman, la noble, la combattante, l'amante, la sève, la splendeur des splendeurs ; ma merveille, sans ton soutien, ton amour, tes prières je ne serai jamais arrivée là, ce qui tu m'as fait apprendre sera gravé à jamais dans mon âme.

À ChahraZed, Nor El Houda, Khadidja ET Abir

À mon cher Fayçal

Ma fierté et ma force, Vous m'avez soutenue dans tous mes projets et mes ambitions, unis et inséparables on a surmontait tous ensemble les moments sales et difficiles, tout mon amour.

À la mémoire de mon petit frère Abd Samed,

À mon binôme Ouassila ;

Ravie de t'avoir partagé le trajet.

Asma.

Table des matières

Liste des figures

INTRODUCTION GÉNÉRALE

L'apparition de l'informatique a conduit à plusieurs changements dans différents domaines, ceci s'applique aussi sur le domaine médical, l'utilisation des nouvelles technologies s'accélère de plus en plus, l'informatisation est devenue un phénomène primordial dans nos jours.

L'un des projets majeurs dans le domaine médical est la mise en place d'un dossier médical personnel informatisé, qui est un outil moderne et adéquat pour favoriser les coordinations des soins et faciliter le partage des informations entre les professionnels de santé.

Un des défis majeurs pour la réussite du Dossier Médical Personnel (**DMP**) est de créer la confiance des utilisateurs dans un outil emblématique de la dématérialisation des données de santé au service de l'amélioration de la qualité et de la coordination des soins. À ce titre, la sécurité est prise en compte dans toutes les phases du cycle de vie du système d'information de santé.

Les systèmes d'informations de santé sont des systèmes complexes, riches en fonctionnalités, qui deviennent de plus en plus exigeants en matière de sécurité, il est indispensable de définir au préalable une politique de sécurité qui soit à la fois robuste, efficace, flexible, assez générique et facile à vérifier.

La sécurité informatique est un monde qui regroupe un ensemble de compétences et de savoir-faire. Cela s'explique par le fait que la notion de sécurité informatique intègre les notions de confidentialité, d'intégrité, de disponibilité, de la non-répudiation, d'imputation et d'authentification. L'un des aspects de la sécurité informatique est le Contrôle d'Accès (**CA**) qui en est un de ces piliers.

Dans ce mémoire de master, nous avons développé un modèle de **CA** au **DMP**. Ce modèle de CA se base sur des ontologies comme source de vocabulaire et base de modélisation.

Ce mémoire de master s'articule autour de quatre chapitres. Chaque chapitre comporte une introduction, nos réflexions, et une conclusion synthétisant le chapitre.

Le premier chapitre aborde la présentation de **DMP** ; le deuxième chapitre se focalise sur la présentation de la sécurité informatique et les différents modèles de **CA** dans les systèmes d'informations ; le troisième chapitre traite la notion d'ontologies. Le quatrième chapitre est dédié à la modélisation et l'implémentation de notre modèle proposé pour le **CA** au **DMP**, ce modèle est basé sur une ontologie.

CHAPITRE I : LA SÉCURITÉ INFORMATIQUE

1. Introduction

Une réelle avancée technologique dans un monde où tout doit aller si vite, mais un véritable problème de fond en ce qui concerne la sécurité des données et la vie privée de chacun. On ne développe pas un nouveau média sans développer quelques effets de bord nuisibles.

La sécurité est un ensemble de stratégies, conçues et mises en place pour détecter, prévenir et lutter contre une attaque.

La sécurité informatique, ou plus globalement la sécurité des systèmes d'information, représente l'ensemble des moyens et des techniques mises en œuvre pour assurer l'intégrité et la non-diffusion involontaire des données transitant dans le système d'information.

Le système d'information définit l'ensemble des données et des ressources (matérielles, logicielles et humaines) permettant de stocker et de faire circuler les informations qu'il contient. Il représente également le réseau d'acteurs qui interviennent sur celui-ci, qui échangent les données, y accèdent, les utilisent.

« *Le système d'information représente un patrimoine essentiel de l'organisation, qu'il convient de protéger. La sécurité informatique consiste à garantir que les ressources matérielles ou logicielles d'une organisation sont uniquement utilisées dans le cadre prévu*. » **[1].**

2. La sécurité informatique

2.1. Les objectifs de la sécurité informatique

La sécurité informatique à plusieurs objectifs, bien sûr liés aux types de menaces [1] ainsi qu'aux types de ressources, etc. Néanmoins, les principaux points sont les suivants **[2]** :

- Empêcher la divulgation non-autorisée de données.
- Empêcher la modification non-autorisée de données.
- Empêcher l'utilisation non-autorisée de ressources réseau ou informatiques de façon générale.

[1] Les menaces : ce sont des adversaires déterminés capables de monter une attaque exploitant une vulnérabilité **[ISO 7498-2].**

2.2. Les champs d'application de la sécurité informatique

La sécurité informatique s'appliquent dans différents domaines ou champs d'applications, chacun faisant appel à des techniques différentes pour atteindre le ou les mêmes objectifs ; ces champs sont **[2]** :

- La sécurité physique.
- La sécurité personnelle.
- La sécurité procédurale (audit de sécurité, procédures informatiques...).
- La sécurité des émissions physiques (écrans, câbles d'alimentation, courbes de consommation de courant...).
- La sécurité des systèmes d'exploitation.
- La sécurité des communications.

2.3. Services principaux de la sécurité informatique

Pour remédier aux failles et pour contrer les attaques, la sécurité informatique se base sur un certain nombre de services qui permettent de mettre en place une réponse appropriée à chaque menace. À ce niveau, aucune technique n'est encore envisagée ; il ne s'agit que d'un niveau d'abstraction visant à obtenir une granularité minimale pour déployer une politique de sécurité de façon optimale (les aspects pratiques tels qu'analyses de risques, solutions technologiques et coûts viendront par la suite). Décrivons les principaux services de sécurité **[2]** :

a. **La disponibilité :** le système doit fonctionner sans faille durant les plages d'utilisation prévues et garantir l'accès aux services et ressources installées avec le temps de réponse attendu.

b. **L'intégrité** : les données doivent être celles que l'on attend, et ne doivent pas être altérées de façon fortuite, illicite ou malveillante. En clair, les éléments considérés doivent être exacts et complets.

c. **La confidentialité** : seules les personnes autorisées peuvent avoir accès aux informations qui leur sont destinées. Tout accès indésirable doit être empêché.

d. **L'authentification** : l'identification des utilisateurs est fondamentale pour gérer les accès aux espaces de travail pertinents et maintenir la confiance dans les relations d'échange.

e. **La non-répudiation** et **l'imputation** : aucun utilisateur ne doit pouvoir contester les opérations qu'il a réalisées dans le cadre de ses actions autorisées et aucun tiers ne doit pouvoir s'attribuer les actions d'un autre utilisateur.

2.4. Types d'attaques :

Les attaques [2] peuvent être classées en deux grandes catégories **[2]** :

---

[2] Les attaques (exploits) : elles représentent les moyens d'exploiter une vulnérabilité. Il peut y avoir plusieurs attaques pour une même vulnérabilité mais toutes les vulnérabilités ne sont pas exploitables **[ISO 7498-2].**

- Les attaques passives : consistent à écouter sans modifier les données ou le fonctionnement du réseau. Elles sont généralement indétectables, mais une prévention est possible.

- Les attaques actives : consistent à modifier des données ou des messages, à s'introduire dans des équipements réseau ou à perturber le bon fonctionnement de ce réseau. Noter qu'une attaque active peut être exécutée sans la capacité d'écoute. De plus, il n'y a généralement pas de prévention possible pour ces attaques, bien qu'elles soient détectables (permettant ainsi une réponse adéquate).

2.5. Les types de Sécurité

Pour sécuriser un système informatique, il est important de définir un modèle de sécurité qui exprime les besoins de sécurité du système d'informations. Il inclut : un règlement de sécurité [3] et un modèle d'administration spécifiant (qui a le droit de mettre à jour le règlement de sécurité), la nature du règlement de sécurité définit la nature du modèle de sécurité **[3]** :

2.5.1. Contrôle d'Accès (**CA**)

Le CA est la politique ou bien la procédure qui permet de protéger les accès aux ressources du système, elle permet les accès autorisés, les accès interdis et les accès non autorisés à ces ressources. Le CA donc renforce particulièrement la confidentialité et l'intégrité de l'information et a fortiori sa disponibilité.

Le **CA** selon **Lampson** est un mécanisme grâce auquel un système autorise ou interdit les actions demandées par des sujets (entités actives) sur des objets (entités passives). Plusieurs entités entrent alors en jeu **[4]** :

- Un ensemble de sujets (*S*) : un sujet est l'entité qui possède l'autorisation (droits d'accès) sur un objet : les procédures (qui manipulent des variables (objets)). Un sujet peut être manipulé par un autre sujet et vu comme un objet, par exemple : les procédures qui manipulent des variables sont aussi des objets auxquels accèdent d'autres sujets comme les utilisateurs.

- Un ensemble d'objets (*O*) : les objets représentent les ressources du système qui doivent être protégés : les fichiers, les répertoires, les programmes, les variables, etc.

- Un ensemble d'actions (*A*) : l'action est le type d'accès permet pour un sujet sur un objet. (Exemples : lecture, écriture, exécution d'un fichier, envoi de signaux ou de messages interprocessus, etc.)

[3] Un règlement de sécurité est un ensemble de : permissions, interdictions, obligations. Il définit ce qui est autorisé et ce qui ne l'est pas.

Les principaux avantages du modèle de **CA** sont : la simplicité et la souplesse et le principal défaut est la vulnérabilité [4] aux chevaux de Troie [5] Défaut aggravé par le fait que les systèmes informatiques sont maintenant tous interconnectés (Internet).

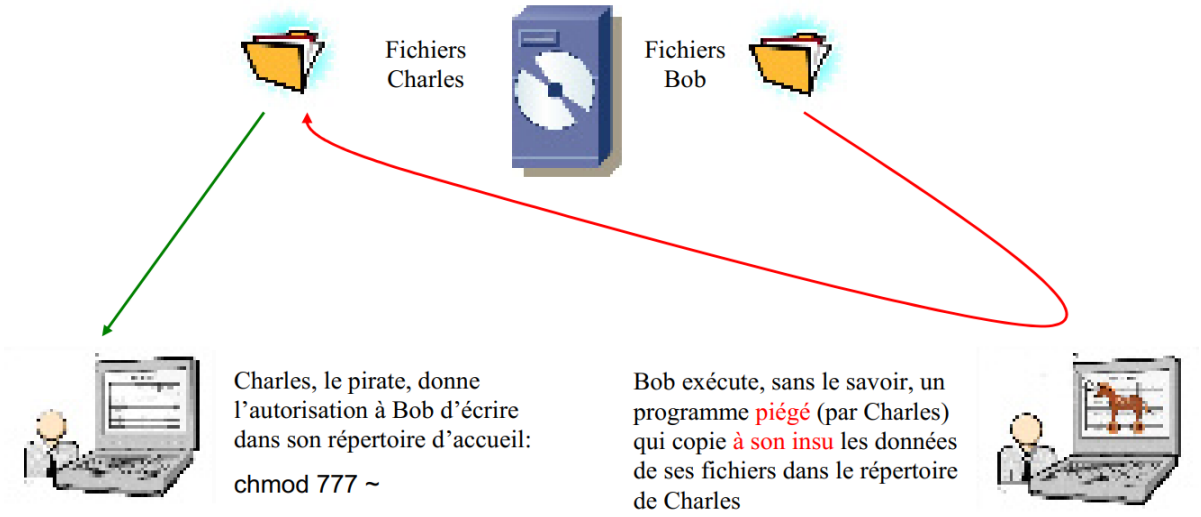

Figure 1: Vulnérabilité aux chevaux de Troie **[3].**

2.5.2. Contrôle des flux

Depuis 1975, le modèle de **CA** ne permet pas de prendre en compte les applications piégées par un cheval de Troie opérant par recopie de fichiers **[3].**

Le contrôle de flux (Flow Control) est l'ensemble de méthodes utilisées sur un réseau pour éviter les congestions ; il constitue une alternative au modèle de **CA** : on observe ce qui se passe pour réguler le trafic.

---

[4] **Les vulnérabilités** : ce sont les failles de sécurité dans un ou plusieurs systèmes. Tout système vu dans sa globalité présente des vulnérabilités, qui peuvent être exploitables ou non **[ISO 7498-2].**

[5] **Cheval de Troie** (trojan) : c'est un programme à apparence légitime qui exécute des routines nuisibles sans l'autorisation de l'utilisateur. La routine nuisible peut être : un programme effectuant directement son action ou une installation de virus de ver, d'espions, ou de portes dérobée.

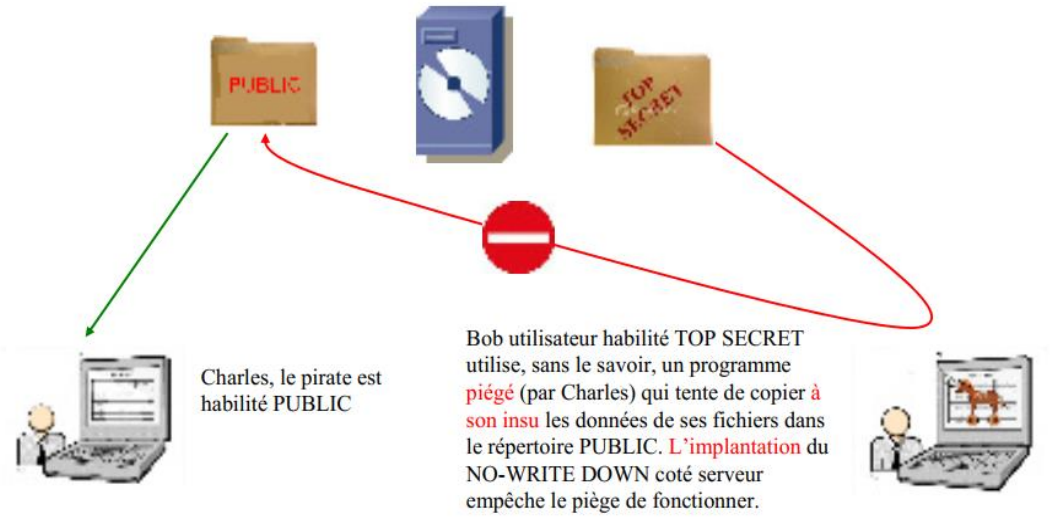

Figure 2 : Modèle de Contrôle de Flux **[3].**

Le **Firewall**[6] est l'outil principal de gestion de la politique de sécurité. Il gère et contrôle les flux de réseau tout en filtrant ses accès. Il se place à l'entrée du réseau et permet de garder des traces de chaque action. Sa position centrale en fait l'outil idéal pour y associer d'autres outils de sécurité. Sa capacité à coopérer avec d'autres outils est donc un critère de choix déterminant **[5].**

Le principal avantage du modèle de contrôle des flux est qu'il permet de lutter contre les chevaux de Troie opérant par recopie de fichiers.

Le principal désavantage de ce modèle est que le règlement est très rigide et le réserve à des applications militaires.

2.5.3. Contrôle d'usage

L'objectif du contrôle d'usage est de contrôler non seulement l'accès au document, mais également l'usage qui en est fait. Il vise principalement (mais pas seulement) à contrôler la recopie des fichiers.

Le modèle de contrôle d'usage dont la première version permet d'énoncer des règles de sécurité qu'il est difficile d'implanter avec des mécanismes classiques de CA :

- ✓ L'utilisateur de ce document ne pourra effectuer qu'une seule copie de sauvegarde.
- ✓ Le médecin aura l'obligation de mettre à jour le DM du patient avant de pouvoir imprimer l'ordonnance, etc.

[6] Le **Firewall** (**Pare-feu**) : un pare-feu est un logiciel dont l'objectif est de contrôler le trafic entre différentes zones de confiance, en filtrant les flux de données qui y transitent

En général, l'implantation d'un règlement de contrôle d'usage se fait en utilisant des techniques **DRM** [7] (**D**igital **R**ight **M**anagement).

Les applications des **DRM** sont de plusieurs ordres : Protection des droits d'auteurs et des intérêts commerciaux des distributeurs de contenus multimédia (films, musique). Cependant, de plus en plus, les DRM sont utilisées dans des applications dont l'objectif est de contrôler la distribution de contenus sensibles (Entreprise-DRM) **[3].**

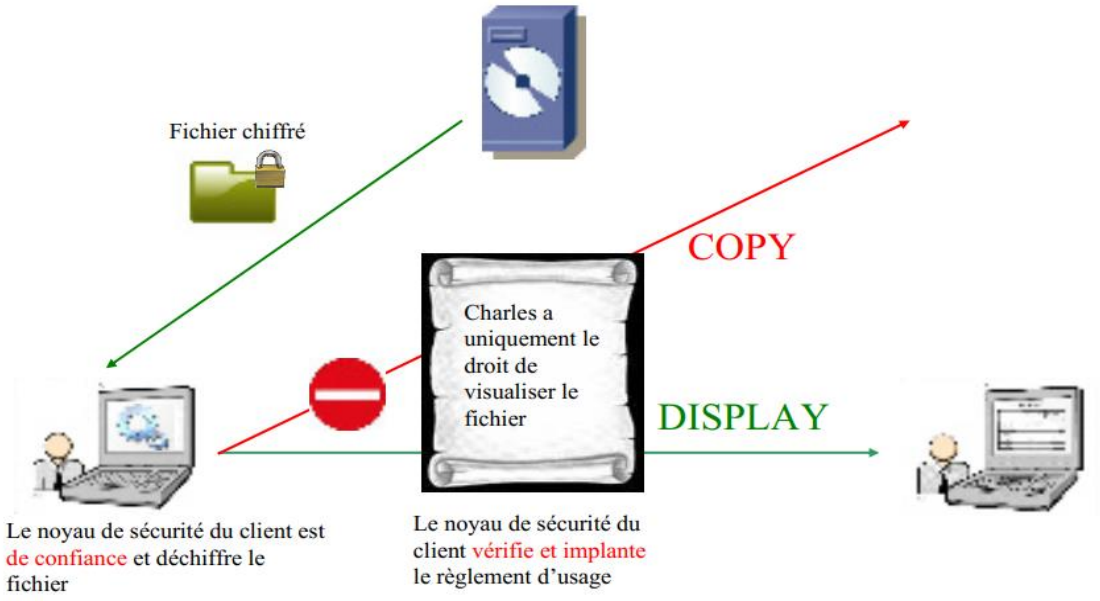

Figure 3: Modèle de Contrôle d'usage **[3].**

3. Modèles de **CA**

Comme évoqué précédemment, le **CA** revêt plusieurs aspects pour assurer la sécurité des ressources et des informations. Il repose sur l'utilisation de différentes notions telles que les rôles avec le modèle **RBAC** ou les périmètres avec des modèles tels qu'**Or-BAC,** etc.

3.1. Modèles de **CA** classiques

Les modèles de CA classiques définissent une relation directe entre les sujets et les objets. Ces modèles classiques sont développés pour résoudre des problèmes de sécurité traditionnels comme la confidentialité et l'intégrité. Mais, ils ont trouvé leurs limites : trop rigides, insuffisamment sûrs ou difficiles d'administration. À l'usage, une limite importante de ces modèles est apparue : la politique d'autorisation devient rapidement complexe à exprimer et administrer. Il est en effet nécessaire d'énumérer les autorisations pour chaque sujet, action ou objet **[6].**

---

[7] Les **DRM** se caractérisent par le fait que les contrôles de sécurité s'effectuent non pas du côté du serveur mais du côté du client

3.1.1. Modèle de **CA** Discrétionnaire (**DAC**)

La matrice de **CA** ou bien le **CA** discrétionnaire **DAC** est le modèle d'accès le plus traditionnel et le plus basic. Ce modèle est utilisé dans plusieurs types d'application comme : les systèmes d'exploitation, les serveurs web, les bases de données relationnelles, etc. Le système UNIX est l'un des exemples des systèmes qui utilisent le modèle de **CA** discrétionnaire pour protéger les accès aux fichiers système.

TCSEC [8] présente le **CA** discrétionnaire comme : *"un moyen de restriction d'accès aux objets basé sur l'identité des sujets et/ou groupes auxquels ils appartiennent. Les contrôles sont dits discrétionnaires dans le sens où le sujet est capable de transférer les permissions d'accès à d'autres sujets"* (La transmission des droits est exercée à la discrétion du sujet) **[7].**

Donc le principe du modèle de **CA** discrétionnaire est plus simple, dans ce modèle les politiques discrétionnaires accordent au sujet propriétaire d'objet, qui est généralement le créateur de cet objet tous les droits d'accès. Ce sujet propriétaire assume aussi toute la responsabilité pour décider quels autres sujets peuvent exerce des actions sur l'objet selon sa discrétion **[4].**

L'implantation de ce modèle a donné lieu à la constitution de matrices d'accès initialement introduite en 1971 par **Lampson** qui a été généralisée en 1976 par **Harison, Ruzzo et Ullman (HRU).** Dans ce dernier, l'état du système est défini par un triplé (S, O, M) où S représente l'ensemble des sujets (utilisateur, processus, etc.) pouvant exercer un ensemble d'actions. O représente l'ensemble des objets (fichier, table, classe, programme, etc.). Enfin, M représente la matrice d'accès, où les lignes correspondent aux sujets et les colonnes correspondent aux objets **[6].**

Sujets \ Objets	Fichier	Table
Utilisateur 1	Lire Ecrire Exécuter	Exécuter
Utilisateur 2	Lire Ecrire	Exécuter Lire

Figure 4: Exemple d'une matrice d'accès.

Il existe en pratique deux mécanismes pour implémenter la matrice d'accès **[4]** :

- ✓ La liste de contrôle d'accès (ou **ACL** pour **A**ccess **C**ontrol **L**ist) : la matrice est stockée par colonne. À chaque objet est associée une liste de règles indiquant pour chaque utilisateur les actions peuvent être exercées par ce dernier sur cet objet.

[8] Les TCSEC (**T**rusted **C**omputer **S**ystem **E**valuation **C**riteria) : sont un ensemble de critères énoncé par le département de la défense des États-Unis qui permettent d'évaluer la fiabilité de systèmes informatiques centralisés. **[Wikipédia]**

✓ La liste de capacité (ou capability liste) : la matrice est stockée par ligne. À chaque utilisateur correspond une liste, appelée liste de capacité, indiquant pour chaque objet les actions que l'utilisateur est en droit d'effectuer sur cet objet.

L'avantage majeur est l'utilisation d'une politique de gestion décentralisée [9]. Et les inconvénients de ce modèle sont :

- La mise à jour est difficile.
- Il ne permet pas de contrôler une information ou ce qui en est fait une fois qu'elle a été accédée par un utilisateur légitime.
- Le système vulnérable à des chevaux de Troie et l'expose à des fuites d'informations.
- La complexité de la modification des grandes matrices.
- L'impossibilité de modéliser des permissions dynamiques **[8].**

3.1.2. Modèle de CA Obligatoire (**MAC**)

Afin d'apporter une solution aux problèmes de fuites d'information des modèles de CA discrétionnaires, les modèles obligatoires (**M**andatory **A**ccess **C**ontrol) viennent fixer des règles incontournables destinées à forcer le respect de la politique de sécurité de l'organisation. Ainsi, le modèle multi-niveaux (voir figure 6) affecte aux sujets et aux objets des niveaux de sécurité qui sont non modifiables par les utilisateurs. Par conséquent, les droits de type posséder n'existent pas.

Le premier modèle, appelé modèle de **Bell et La Padula,** a été développé en 1976 pour le département de la défense américain et vise, plus particulièrement, à assurer la confidentialité des données dans le contexte de l'utilisation partagée de mainframes.

Le deuxième modèle, appelé modèle de **Biba** (en 1977) qui prend en compte les exigences commerciales s'intéresse plutôt à l'intégrité des informations **[6].**

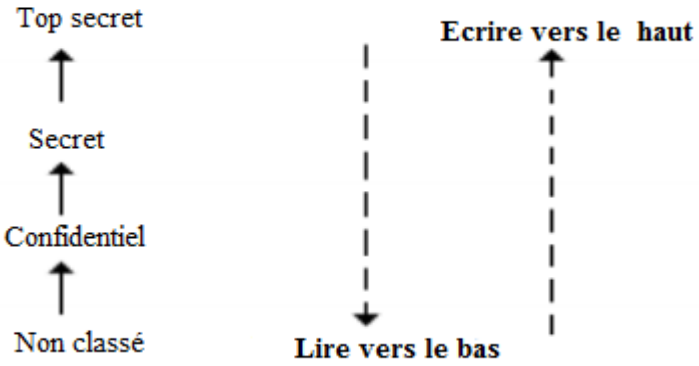

Figure 5: Sécurité multi-niveaux **[10].**

[9] La décentralisation, par le fait que la prise de décision et le pouvoir sont dispersés partout et au plus bas dans la hiérarchie de l'organisation, nécessite un contrôle administratif fort et met l'accent sur la délégation de la prise de décision et allège la charge des hauts dirigeants **[9].**

Le modèle de CA MAC est utilisé majoritairement pour des systèmes de sécurité militaire, qui permet de restreindre l'accès à des informations en fonction du niveau de sensibilité de celle-ci et de l'autorisation des utilisateurs à pouvoir accéder à un tel niveau d'information **[9].**

Le modèle **MAC** résout le problème de fuite d'information des modèles **DAC**. Il est quand même un modèle très rigide, car il ne permet pas de gérer les exceptions entre les différents niveaux de sécurité. Par exemple, un utilisateur de niveau de sécurité secret ne peut pas accéder, pour des raisons exceptionnelles, aux données de niveau de sécurité top secret **[6].**

3.2. Modèles de CA à base de rôle (**RBAC**)

Le modèle de CA basé sur les rôles **RBAC** a été proposé pour la première fois selon Amal HADDAD **[11]** en 1992 par **David Ferrailo** et **Richard Kuhn**, attachés au département de commerce des États-Unis.

RBAC est un modèle de CA où les permissions d'accès ne s'appliquent pas directement aux utilisateurs comme dans le modèle **DAC**. Des relations et des concepts intermédiaires sont introduits entre les utilisateurs et les permissions où les permissions sont accordées aux rôles d'un côté et d'un autre coté les utilisateurs sont affectés à un ou plusieurs rôles, les rôles des utilisateurs déterminent les accès permis et les accès interdits pour ces utilisateurs.

Le rôle est le concept central de la politique de sécurité dans le modèle **RBAC** et l'utilisation de ce concept permet une organisation souple et efficace des droits d'accès et il n'est pas nécessaire de mettre à jour l'ensemble des politiques de contrôle d'accès si un nouvel utilisateur est créé et il suffit juste d'assigner un rôle à cet utilisateur **[4].**

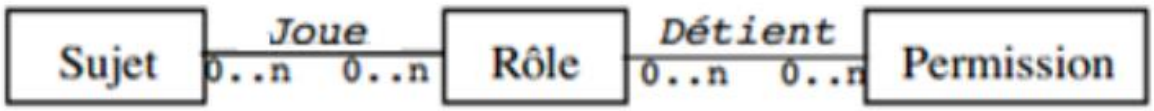

Figure 6: Attribution des permissions aux sujets à travers des rôles **[12].**

Le principal inconvénient de **RBAC** réside dans la difficulté de garantir la propriété de confidentialité. En effet, n'importe qu'elle utilisateur jouant le rôle médecin puisse accéder aux dossiers de tous les patients, y compris ceux qu'il ne les traite pas.

Ce modèle est toujours vulnérable aux attaques par cheval de Troie, il nécessite de mettre en place une procédure d'administration des rôles **[13].**

3.3. Modèles de CA dérivés de **RBAC**

Le modèle **RBAC** a été largement adopté par l'industrie et par la communauté de recherche. Il a déclenché un renouveau des modèles de CA et plusieurs propositions ont été faites pour ajouter de nouveaux concepts ou notions au modèle RBAC de base : par exemple le temps, la localisation, le contexte spatial, la position géographique de l'utilisateur, etc. Nous classons dans cette section les modèles qui couvrent la plupart de ces nouvelles notions ou concepts dérivés de RBAC **[6] :**

3.3.1. Modèles de CA prenant en compte la localisation

3.3.1.1. Modèle **Géo-RBAC**

Le modèle **Géo-RBAC** est proposé par **Bertino et al** en 2005**,** étend le modèle **RBAC** en définissant de nouveaux concepts spatiaux pour représenter la position des sujets et celles des objets. Ces nouveaux concepts sont utilisés pour limiter géographiquement l'utilisation des rôles. Le principe proposé dans **Géo-RBAC** est de comparer une position physique, supposée obtenue de façon fiable (par exemple la localisation GPS), à des positions logiques (Exemples : route, ville, région) auxquelles sont associées des rôles géographiques.

Il est composé comme **RBAC** de sous-modèles de base, hiérarchique, et contraint. Le modèle **Géo-RBAC** comprend tous les concepts de base de RBAC et ajoute des nouveaux concepts : la notion de rôle spatial, et de position réelle/logique.

Ce modèle est très précis pour répondre à la nécessité de prendre en compte la localisation géographique, dans la construction d'une règle de politique de CA **[6].**

3.3.1.2. Modèles de CA **LRBAC**

Proposé par **Zhang et al** en 2006**,** il étend le modèle **RBAC** pour que le CA puisse être établi en prenant en compte les informations de localisation. Un tel modèle a été proposé pour autoriser ou interdire l'accès lorsque les systèmes sont dans/ou hors d'une zone d'opération définie.

Ce modèle, proposé dans le cadre de la prolifération d'équipements mobiles, utilise la localisation logique des utilisateurs et/ou des systèmes comme paramètre contextuel. La localisation logique exprime les frontières ou les secteurs (i.e. départements, bureaux individuels, secteur public, etc.) dans l'organisation. Ainsi, les domaines de localisation logique définissent les limites de l'espace dans lequel les rôles peuvent être assumés par l'utilisateur **[6].**

3.3.2. Modèles de CA à base de contexte temporel

GTRBAC est proposé en 2005 par **Joshi et al.** Il étend le modèle **RBAC** afin d'exprimer un large éventail de contraintes temporelles. En particulier, le modèle permet d'exprimer le temps et des contraintes temporelles sur les rôles, l'affectation des rôles aux utilisateurs, et l'affectation des permissions aux rôles.

Ce modèle répond aux besoins précis d'applications avec une contrainte temporelle forte, comme les systèmes intégrant des workflows où la notion de temps est importante. Ces systèmes sont utilisés par des organisations désirant spécifier des règles d'autorisation qui permettent ou interdisent l'accès à des ressources pendant un intervalle de temps donné.

Ce modèle, intégrant le contexte temporel dans la modélisation des droits, est basé sur l'existence d'une horloge globale fiable, grâce à laquelle sont développées des contraintes d'accès basées sur l'horaire où les sujets agissent dans le système :

- ✓ l'activation et la désactivation périodique de rôle.
- ✓ les affectations de rôles aux utilisateurs et de permissions aux rôles.

- ✓ la durée pendant laquelle on peut endosser un rôle.

Tout comme le modèle **RBAC**, **GTRBAC** propose de structurer les informations sous forme de hiérarchie. De plus, ce modèle inclut l'étude de conflits entre les éléments : rôles, utilisateurs, et contraintes temporelles. Ainsi, ce modèle répond à un contexte précis impliquant l'utilisation de la notion de « temps » dans les politiques de CA au sein de l'organisation **[6].**

3.3.3. Principe général des modèles dérivés de **RBAC**

Les politiques de sécurité dérivées du modèle de CA RBAC permettent **[6] :**

- ✓ D'organiser les droits de la façon la plus proche possible de la structure des organisations, afin de permettre aux administrateurs de manipuler les droits d'une façon plus intuitive.
- ✓ De limiter le nombre d'affectations des permissions, pour éviter les erreurs en réduisant la taille des politiques.
- ✓ D'exprimer de nouvelles règles et contraintes, qui permettront de traduire facilement les politiques exprimées en langage naturel.
- ✓ De prendre en compte des notions autres que le rôle tel qu'il est introduit dans RBAC, pour spécifier des politiques de contrôle d'accès qui répondent à des besoins spécifiques.

3.4. Modèles de CA à base des tâches (**TBAC**)

En parallèle des travaux originaux sur **RBAC**, le modèle **TBAC** (**T**ask **B**ased **A**ccess **C**ontrol) a été proposé par **Thomas et Sandhu** en 1993**.** Il est conçu afin d'activer une permission par rapport aux tâches effectuées par l'utilisateur.

L'idée essentielle de ce modèle consiste à ajouter la notion de tâche dans des règles d'autorisation. Cela permet de définir les permissions qu'un sujet peut activer selon la tâche qui est en cours. Chaque étape d'autorisation correspond à certaines activités ou tâches dans le contexte plus large d'un workflow [10] de l'organisation. Le modèle **TBAC** fut le premier modèle à introduire le concept de tâche. **TBAC** offre une approche pour différencier l'affectation et l'activation des permissions par rapport à des tâches données aux utilisateurs au sein de l'organisation.

La notion de tâche permet de contrôler les activités exercées par les utilisateurs d'un système d'information au sein de l'organisation. **TBAC** peut parfaitement être adapté et intégrer la notion de rôle. C'est dans cet esprit que le modèle **TR-BAC** (**T**ask and **R**ôle **BAC [38]14)** a été défini. Dans ce cas, les droits sont activés en fonction d'un rôle et portent sur la réalisation des tâches.

---

[10] Le **Workflow** se traduit par le « *flux de travail* ». Il s'agit d'un processus qui permet d'automatiser la circulation des flux d'information dans une entreprise. De façon pratique, il permet généralement le suivi et l'identification des acteurs en précisant leur rôle et la manière de le remplir au mieux.

De plus, **TBAC** ou **TR-BAC** présente l'inconvénient de ne pas prendre en compte des contraintes sur les horaires ou périodes d'accès pendant lesquels les utilisateurs sont en charge de la réalisation de leurs activités. Le manque constaté est couvert par d'autres modèles formels de CA **[6].**

3.5. Modèles de CA à base d'équipes (**TMAC**)

La notion d'équipe a été proposée dans le modèle **TMAC** par Thomas et Sandhu en 1997 (**T**ea**M**based **A**ccess **C**ontrol). Les permissions sont associées aux rôles ainsi qu'aux équipes. La notion d'équipe a été introduite pour représenter des aspects transversaux des rôles qui ne sont pas directement exprimables dans les modèles **RBAC [15].** Dans TMAC, l'objectif est d'accorder à chaque utilisateur membre d'une équipe des permissions accordées aux autres membres de l'équipe qui sont actifs. On distingue deux types d'informations **[16]** :

- le contexte utilisateur : les utilisateurs qui font partie de l'équipe à tout moment.
- le contexte objet : l'ensemble des instances des objets dont l'équipe a besoin pour accomplir sa tâche.

Il faut noter qu'ici les relations de ce modèle sont dynamiques, car les permissions sont accordées par rapport au contexte des membres d'une équipe dans des sessions actives. Ce modèle prend seulement les requêtes actives dans une session. Ce modèle offre les avantages d'une administration simplifiée d'une modélisation **RBAC**, mais aussi, il fournit un contrôle plus fin sur l'activation d'autorisation d'utilisateurs individuels et des objets **[6].**

3.6. Modèle de CA basé sur les attributs (**ABAC**)

Le modèle ABAC a été développé par **Eric Yuan** et **Jin Tong** en 2005, 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. De part, sa définition, le modèle ABAC peut être le plus adapté pour les architectures fonctionnant dans un environnement ouvert « in the cloud » où différentes organisations peuvent assurer à la fois les accès aux informations et la protection de leurs ressources **[17].**

Le modèle d'accès basé sur les attributs **ABAC** est un modèle plus générale que celui du modèle **RBAC**. L'utilisation du modèle ABAC donne la capacité pour déterminer l'accès sans avoir besoin d'une liste des individus qui sont autorisés au sein de l'organisation où la décision d'accès se fait sur la base d'un ensemble des caractéristiques et des attributs associés soit avec l'entité qui demande l'accès à la ressource, l'environnement ou bien avec la ressource elle-même.

Le modèle **ABAC** et à l'inverse des modèles **DAC** et **RBAC** ne peut pas être supporté par les systèmes d'exploitation, ce modèle est appliqué uniquement au niveau application **[4].**

3.7. Modèle de CA à base d'organisation (**Or-BAC**)

Le modèle de CA **Or-BAC** (**Or**ganization **B**ased **A**ccess **C**ontrol) est proposé en 2003 par **Abou El Kalam et al.** Il vise à résoudre certains problèmes rencontrés par les premiers modèles de CA des années 90 et à établir une politique de CA plus abstraite. Il s'intéresse, non seulement aux permissions, mais aussi aux interdictions, obligations et recommandations dans une politique de sécurité. Or-BAC prend le concept de rôle dans **RBAC**.

En plus de ce concept, il ajoute des nouveaux concepts pour structurer les sujets, les objets et les actions **[6].**

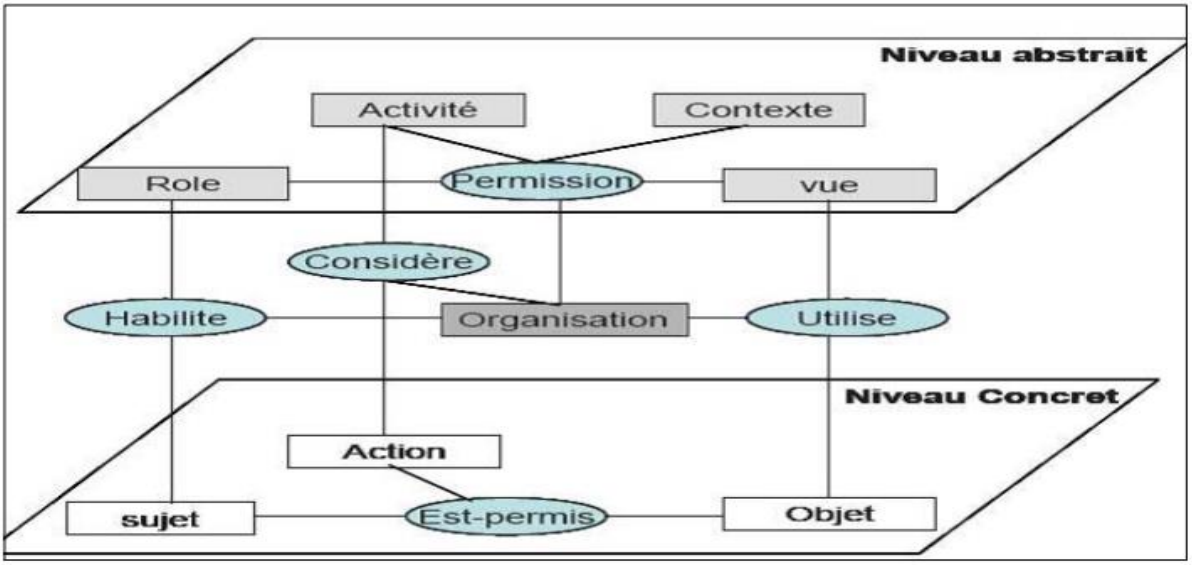

Figure 7: Modèle de CA Or-BAC **[6].**

Or-BAC considère les ensembles suivants : Organisation (ensemble des organisations), Sujet (ensemble des sujets), Action (ensemble des actions), Objet (ensemble des objets), Rôle (ensemble des rôles), Activité (ensemble des activités), Vue (ensemble des vues), et Contexte (ensemble de contexte).

Chaque entité peut avoir certains attributs. Ceci est représenté par des fonctions qui associent des entités avec la valeur de ces attributs. Par exemple si sujet s $\in$ Sujet, alors nom(s)=n et adresse(s)=m représentent les attributs *nom* et *adresse* utilisés pour désigner le nom et l'adresse du sujet s, où *n* est la valeur de *nom* et *m* est la valeur de l'*adresse* **[6].**

3.7.1. Organisations

L'entité centrale dans ce modèle est l'organisation. Dans le domaine médical, nous pouvons considérer les organisations suivantes : une clinique privée, le service des urgences de l'hôpital, l'unité des soins intensifs, etc.

Une organisation peut être vue comme un groupe structuré d'entités actives, c'est-à-dire de sujets jouant certains rôles. Notons qu'un groupe de sujets n'est pas nécessairement considéré comme une organisation.

Autrement dit, le fait que chaque sujet joue un rôle dans l'organisation correspond à un certain accord entre les sujets pour former une organisation **[18]**.

3.7.2. Sujets et rôles

L'entité sujet est utilisée différemment selon les modèles de sécurité. Dans le modèle **OR-BAC**, un sujet peut être soit une entité active, c'est-à-dire un utilisateur, soit une organisation.

Les rôles nous permettent de structurer les sujets et de faciliter la mise à jour de la politique de sécurité quand un nouvel utilisateur est ajouté.

Comme les sujets jouent des rôles dans des organisations, nous introduisons une relation entre ces entités :

La relation *Habilite*. Si ***org*** est une organisation, **S** est un sujet et ***R*** est un rôle, alors *Habilite (**org**, **S, R**)* signifie que ***org*** habilite le sujet ***S*** à jouer le rôle ***R***.

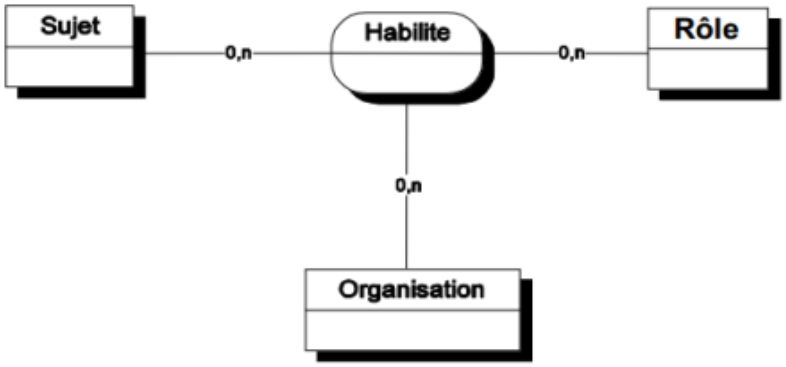

Figure 8: La relation Habilite **[18].**

Un sujet est soit un utilisateur, soit une organisation. Par exemple {Habilite (H1, Dr.Mohamed, cardiologue) : « l'hôpital H1 habilite Dr.Mohamed dans le rôle cardiologue »} ou {Habilite (H2, ICU31, unité_des_soins_intensifs) : « l'hôpital H2 habilite l'unité ICU31 dans le rôle d'unité des soins intensifs »} **[13].**

3.7.3. Objets el vues

L'entité Objet représente principalement les entités non actives comme les dossiers administratifs, les dossiers médicaux et les dossiers chirurgicaux des patients.

Dans la mesure où il est également nécessaire de structurer les objets et d'ajouter de nouveaux objets au système, nous l'appelons : entité Vue.

Une vue correspond, comme dans les bases de données relationnelles, à un ensemble d'objets qui satisfait une propriété commune. Par exemple, la vue « dossiers médicaux » correspond aux dossiers médicaux des patients.

Dans la mesure où les vues caractérisent la manière dont les objets sont utilisés dans l'organisation, nous avons besoin d'une relation qui lie ces trois entités : la relation Utilise (***org***, ***O***, ***V***) signifie que ***org*** utilise l'objet ***O*** dans la vue ***V*** **[13]**.

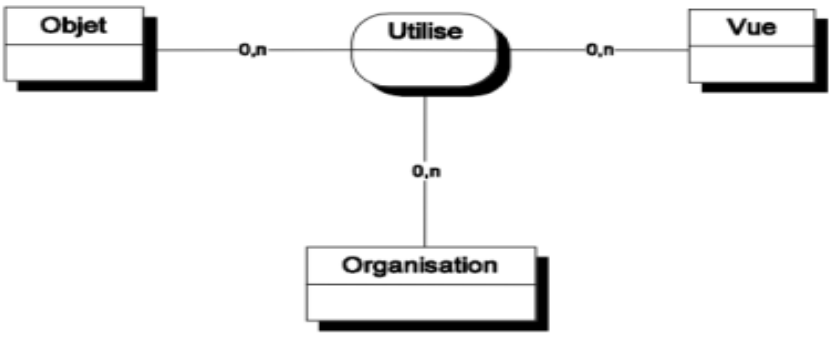

Figure 9: La relation Utilise **[18].**

3.7.4. Actions et activités :

L'entité Action englobe principalement les actions informatiques comme « lire, écrire, envoyer, etc. ».

Les activités correspondent à des actions qui ont un objectif commun, ils pourront être « consulter, modifier, transmettre, etc. » **[13].**

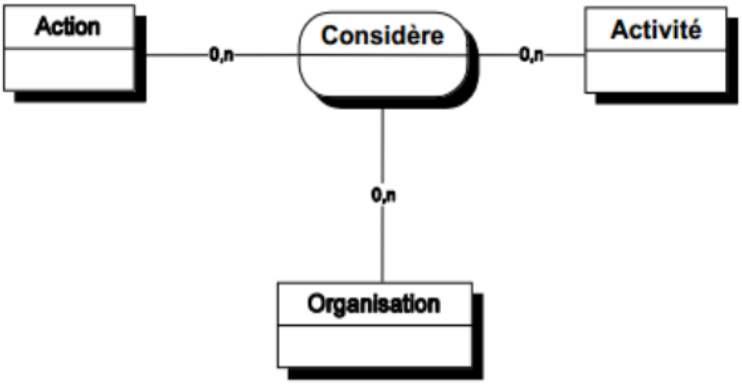

Figure 10: la relation Considère **[18].**

L'objectif est de pouvoir caractériser des organisations qui structurent différemment les mêmes activités. Si ***org*** est une organisation, ***α*** est une action et ***A*** est une activité, alors Considère (***org***, ***α***, ***A***) signifie que l'organisation ***org*** considère l'action ***α*** comme faisant partie de l'activité ***A***.

Si nous considérons l'activité « *consultation* ». Cette activité peut correspondre, dans l'organisation hôpital ***H1***, à l'action « *lire* » un fichier, mais peut tout aussi bien correspondre à l'action « *select* » sur une base de données dans l'hôpital ***H2*.**

- Considère (H1, lire, consultation) : « l'hôpital H1 considère lire comme une consultation »
- Et Considère (H2, select, consultation) : « l'hôpital H2 considère select comme une consultation ».

3.7.5. Contextes

Les modèles de CA classiques ne permettent de modéliser que des politiques de sécurité qui se restreignent à des permissions statiques. Ils n'offrent pas la possibilité d'exprimer des règles contextuelles. En effet, il est fréquent d'avoir des règles de sécurité spécifiques à un certain contexte.

Les contextes sont utilisés pour spécifier les circonstances concrètes dans lesquelles les organisations accordent aux sujets des permissions de réaliser des actions sur les objets telles que « urgence », « médecin traitant », etc.

Les contextes peuvent être vus comme des relations entre les sujets, les objets et les actions définis dans une certaine organisation. Par conséquent, ces quatre entités sont liées par une nouvelle relation appelée *Définit*. Telle que : *Définit* (***org***, ***S, α, O, C***) signifie qu'au sein de l'organisation ***org***, le contexte ***C*** est vraie entre le sujet ***S***, l'objet ***O*** et l'action ***α.***

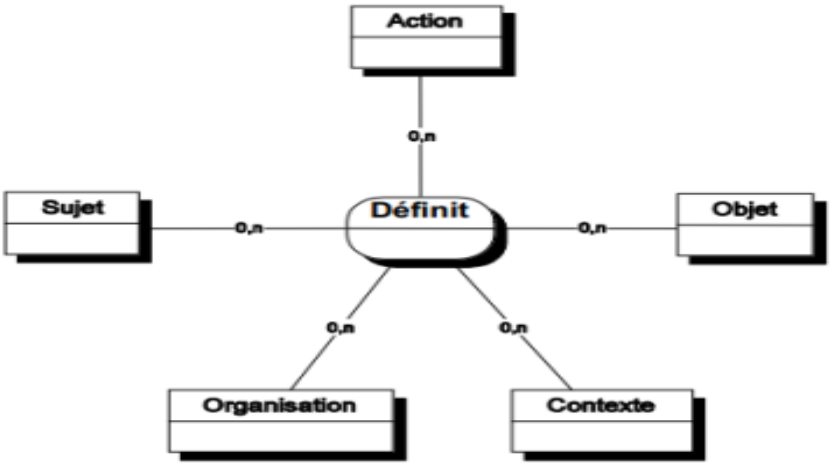

Figure 11: la relation Définit **[18].**

Par exemple :

(1) *Définit* (hôpital1, Mohamed, lire, F31.doc, urgence) et,
(2) *Définit* (hôpital2, Ali, lire, F32.tex, médecin-traitant).

Si le premier fait est vrai, alors *Mohamed* n'a pas besoin d'être le *médecin-traitant* du patient correspondant au dossier médical *F31.doc* pour consulter son dossier. En effet, il est raisonnable de considérer que dans un contexte *d'urgence*, les médecins ont un accès immédiat à tous les dossiers médicaux.

Si le second fait est vrai, alors *Ali* doit être le *médecin-traitant* du patient dont le dossier médical est *F32.tex* : dans un contexte normal comme « médecin traitant » **[13].**

3.8. Synthèse

En introduisant ces différentes entités, **Or-BAC** représente un modèle très générique qui reflète la structure des droits et relations au sein de l'organisation. Les entités « rôle », « activité », « vue »

rendent la politique de **CA** flexible dans le sens où une modification des entités concrètes « sujet, action, objet » n'invalide pas la politique elle-même. Le modèle **Or-BAC** prend ainsi la notion de contexte pour spécifier des permissions ou autorisations dynamiques **[6].**

4. Conclusion

La sécurité informatique est un monde qui regroupe un ensemble de compétences et de savoir-faire. Cela s'explique par le fait que la notion de sécurité informatique intègre les notions de confidentialité, d'intégrité, de disponibilité, de la non-répudiation, d'imputation et d'authentification. L'un des aspects de la sécurité informatique est le **C**ontrôle d'**A**ccès (**CA**) qui en est un de ces piliers.

Dans ce chapitre, nous avons présenté un bilan des divers modèles formels de **CA** existants. Ces modèles ont été conçus pour traiter le CA dans des situations bien différentes. Ils introduisent de multiples concepts pour spécifier les politiques de sécurité. Le but de ces divers modèles est d'offrir la palette la plus vaste possible d'expression de politiques de CA.

Chapitre II : Contrôle d'accès par les ontologies

1. Introduction

L'ontologie est abordée de plusieurs manières par plusieurs domaines très variés de la philosophie à l'informatique, en passant par la biologie. Les balbutiements de l'ontologie nous ont été présentés par la philosophie, il y a de cela plusieurs centaines d'années, par exemple dans l'ouvrage « Les catégories » d'**Aristote [19].** Il a été depuis exploré par plusieurs auteurs, tels que **Bertrand Russell** en 1905, **Rudolf Carnap Carnap** en 1997, et **Quine** en 1971.

Le concept a été plus tard introduit en informatique en 1980 par un des instigateurs de l'intelligence artificielle **McCarthy**, en référence à l'ontologie de **Quine [20].** Plus récemment, le **W3C** [1] poussé par son fondateur **Tim Berners-Lee**, avance le concept de l'ontologie comme couche sous-jacente au web sémantique, l'extension proposée du *« World Wide Web »*. On a aussi vu en 2001 la première proposition d'utiliser l'ontologie comme modèle de connaissance en sécurité informatique **[21].**

2. Notion d'ontologie

Le terme d'ontologie est cependant usité en philosophie depuis le XIXème siècle. Dans ce domaine, l'ontologie est une étude de l'être en tant qu'être, c'est-à-dire, une étude des propriétés générales de ce qui existe. C'est à l'occasion de l'émergence de l'**I**ngénierie des **C**onnaissances (**IC**) que les ontologies sont apparues en **I**ntelligence **A**rtificiel (**IA**), comme réponses aux problématiques de représentation et de manipulation des connaissances au sein des systèmes informatiques **[22].**

2.1. Définitions d'une ontologie

Le terme « ontologie » est employé dans des contextes très différents touchant la philosophie, la linguistique ou l'IA. De nombreuses définitions ont été offertes pour donner un éclaircissement sur ce terme, mais aucune de ces définitions ne s'est explicitement imposée. Les définitions de ce terme ne sont pas toujours consistantes et cela dépend des domaines spécifiques **[23].** Pour ne pas dévier de notre propos, nous avons recensé les définitions suivantes :

Les ontologies, à l'origine d'une branche de la philosophie qui s'intéresse à la nature et à l'organisation de la réalité, correspondent à ce qu'Aristote appelait la Philosophie première, c'est-à-

[1] **W3C :** Ou **W**orld **W**ide **W**eb **C**onsortium, est un organisme international qui développe des standards pour le Web afin que les gens puissent communiquer efficacement à travers Internet, autour de formats ouverts garantissant une meilleure interopérabilité (c'est-à-dire une meilleure compréhension des systèmes hétérogènes à travers des données et langages standardisés). Le Consortium existe depuis 1994 et est dirigé par l'inventeur du Web, Tim Berners-Lee **[24]**.

dire la partie de la métaphysique qui s'intéresse à l'être en tant qu'être, par opposition aux philosophies secondes qui s'intéressent à l'étude des manifestations de l'être **[25].**

En informatique, la littérature fournit plusieurs définitions du mot ontologie. Ces définitions, dans leur diversité, offrent des points de vue à la fois différents et complémentaires. Cependant, une définition qui fait autorité a été faite par **Greber** et s'énonce comme suit : « *Une ontologie est la spécification d'une conceptualisation. [...] Une conceptualisation est une vue abstraite et simplifiée du monde que l'on veut représenter* ». Ainsi, **Studer** en 1998 définit l'ontologie comme une « *spécification formelle et explicite d'une conceptualisation partagée »* :

- ✓ ***Formelle*** : l'ontologie doit être lisible par une machine, ce qui exclut le langage naturel.
- ✓ ***Explicite*** : la définition explicite des concepts utilisés et des contraintes de leurs utilisations.
- ✓ ***Conceptualisation*** : le modèle abstrait d'un phénomène du monde réel par identification des concepts clefs de ce phénomène.
- ✓ ***Partagée*** : l'ontologie n'est pas la propriété d'un individu, mais elle représente un consensus accepté par une communauté d'utilisateurs.

Pour nous, l'ontologie se définit comme étant un ensemble de termes hiérarchiquement structurés, conçu afin de décrire un domaine qui peut être utilisé comme un squelette de base pour les bases de connaissances.

Une ontologie est basée sur la logique descriptive, or, cette dernière est un langage de représentation de connaissance qui peut être utilisée pour représenter la connaissance terminologique d'un domaine d'application d'une manière formelle et structurée.

Notre objectif étant de faire une représentation du CA en informatique donc naturellement l'utilisation d'une ontologie est justifiée **[26]**.

2.2. Constituantes d'une ontologie

Une ontologie est composée d'un ensemble structuré de concepts d'un domaine bien déterminé. Elle est structurée comme un dictionnaire formel qui définit les concepts par leurs relations sémantiques et de subsomption. Ainsi, une ontologie est composée de **[26]** :

- ✓ Classes qui énumèrent l'ensemble des concepts d'un domaine.
- ✓ Attributs qui décrivent les caractéristiques et les propriétés d'une classe. On parle parfois de rôles.
- ✓ Facettes qui sont des restrictions sur les attributs.
- ✓ Instances qui constituent une base de connaissances. Ils sont les vrais individus ou données réels de l'ontologie.

2.3. Différentes sortes d'ontologies

Cette section n'a pas l'ambition de fournir une typologie approfondie des ontologies. Cependant, elle présente les types d'ontologies les plus généralement utilisés. Nous pouvons classer les ontologies selon plusieurs dimensions. Parmi celles-ci, nous en examinerons deux **[22]** :

- Objet de conceptualisation.
- Niveau de formalisme de représentation.

2.3.1. Objet de conceptualisation

Dans **[27],** les ontologies sont classifiées selon leur objet de conceptualisation (le but de leur utilisation) de la façon suivante **[22]** :

a) **Ontologie de haut niveau :** décrit des concepts très généraux comme l'espace, le temps, la matière, les objets, les événements, les actions, etc. Ces concepts ne dépendent pas d'un problème ou d'un domaine particulier, et doivent être, du moins en théorie, consensuels à de grandes communautés d'utilisateurs.

b) **Ontologie de domaine :** contrairement aux ontologies de haut niveau, les ontologies de domaine sont plus spécifiques. Elles synthétisent les connaissances spécifiques à un domaine particulier. Elles décrivent le vocabulaire ayant trait à un domaine générique (l'enseignement, la médecine, …), notamment en spécialisant les concepts d'une ontologie de haut niveau.

c) **Ontologie de tâches :** ce type d'ontologies est utilisé pour conceptualiser des tâches spécifiques dans les systèmes, telles que les tâches de diagnostic, de planification, de conception, de configuration, de tutorat. Sois tout ce qui concerne la résolution de problèmes. Ce type d'ontologies décrit le vocabulaire concernant une tâche générique (enseigner, diagnostiquer, …), notamment en spécialisant les concepts d'une ontologie de haut niveau.

d) **Ontologie d'application :** cette ontologie est la plus spécifique, elle contient des concepts dépendants d'un domaine et d'une tâche particuliers, qui sont généralement subsumés par des concepts de ces deux ontologies. Ces concepts correspondent souvent aux rôles joués par les entités du domaine lors de l'exécution d'une certaine activité.

2.3.2. Niveau de formalisme de représentation

Selon le niveau du formalisme de représentation, **[28]** propose une classification comprenant quatre catégories **[22]** :

a) **Informelles** : ontologies opérationnelles dans un langage naturel (sémantique ouverte).
b) **Semi-informelles** : utilisation d'un langage naturel structuré et limité.
c) **Semi-formelles** : langage artificiel défini formellement.
d) **Formelles** : utilisation d'un langage artificiel contenant une sémantique formelle, ainsi que des théorèmes et des preuves de propriétés telles la robustesse et l'exhaustivité.

2.4. Langages des ontologies

Pour la création et la manipulation des ontologies, il existe plusieurs langages de spécification spécialisés ; nous pouvons citer **[26]** :

- **OKBC** (Open Knowledge Base Connectivity - 1997) : API permettant d'accéder à des bases de connaissance.
- **KIF** (Knowledge Interchange Format - 1998) : langage destiné à faciliter des échanges de savoirs entre systèmes informatiques hétérogènes.
- **Loom** : langage de représentation des connaissances dont le but avoué est de « permettre la construction d'applications intelligentes ».
- **DAML-ONT** (DARPA Agent Markup Language Ontology – 2000) : fondé sur XML, résulte d'un effort du **DARPA** (Defense Advanced Research Projects Agency) pour l'expression de classes plus complexes que le permet RDF-S.
- **RDF/RDF-S** (Resource Description Framework) : RDF est un modèle de graphe destiné à décrire de façon formelle les ressources Web et leurs métadonnées, de façon à permettre le traitement automatique de telles descriptions. RDF-S fournit des éléments de bases pour la définition d'ontologies ou vocabulaires destinés à structurer des ressources RDF.

- **OWL** (Web Ontology Language) : est un langage de description d'ontologies conçu pour la publication et le partage d'ontologies sur le Web sémantique [2].

2.5. Langage OWL

Dans le cadre de notre projet, nous nous sommes particulièrement intéressés au langage OWL. Ce dernier est inspiré de DAML (US **D**ARPA **A**gent **M**arkup **L**anguage) projet Américain et OIL (**O**ntology **I**nference **L**ayer) projet Européen [3].

Le langage **OWL** fournit des mécanismes pour créer tous les composants d'une ontologie : classes, instances, propriétés et axiomes. **OWL** repose également sur la syntaxe des triplets RDF et réutilise certaines des constructions RDFS. Comme en RDFS, les classes peuvent avoir des sous-classes, fournissant ainsi un mécanisme pour le raisonnement et l'héritage des propriétés. Par contre, en OWL, on distingue **[29]** :

1) Les propriétés objet (***object property***) : les relations, qui relient des instances de classes à d'autres instances de classes. C'est l'équivalent des triplets **RDF** dont l'objet est une ressource.
2) Les propriétés type de données (***datatype property***) : les attributs, qui relient des instances de classes à des valeurs de types de données (nombres, chaînes de caractères, etc.). C'est l'équivalent des triplets **RDF** dont l'objet est une valeur littérale.

Les axiomes fournissent de l'information au sujet des classes et des propriétés, spécifiant par exemple l'équivalence entre deux classes. Donc **OWL** permet de définir des ontologies comme un jeu de définition de classes, de propriétés et de contraintes. Toute classe définie dans une ontologie **OWL** est une sous-classe de ***owl:Thing***.

OWL a été fractionné en trois langages distincts chacune étant une extension de la précédente **[29]** :

- **OWL Lite :** convient aux utilisateurs qui ont principalement besoin d'une hiérarchie de classification et de contraintes simples. Ce sous langage reprend tous les constructeurs de RDF (c'est-à-dire fournit des mécanismes permettant de définir un individu comme instance d'une classe, et de mettre des individus en relation), il utilise les mots-clés de RDFS (***rdfs:subClassOf, rdfs:Property, rdfs:subPropertyOf, rdfs:range, rdfs:domain***), avec la même sémantique, et il supporte les contraintes de cardinalité, mais ne permet d'utiliser que les valeurs 0 ou 1.

- **OWL LD** (OWL Description Logic) : convient aux utilisateurs qui veulent le maximum d'expressivité, ce sous langage reprend tous les constructeurs d'**OWL LITE**, il permet tout entier positif dans les contraintes de cardinalité, et le tire son nom de sa correspondance avec les logiques de descriptions.

- **OWL FULL** : ce sous langage reprend tous les constructeurs d'**OWL DL**, et tous les constructeurs de RDF Schéma. Il permet d'utiliser une classe en position d'individu dans les constructeurs.

---

[2] **Le Web sémantique** : ou toile sémantique, est une extension du Web standardisée par le **W3C**. Ces standards encouragent l'utilisation de formats de données et de protocoles d'échange normés sur le Web. Le Web sémantique fournit un modèle qui permet aux données d'être partagées et réutilisées entre plusieurs applications, entreprises et groupes d'utilisateurs **[Wikipédia]**.
[3] **DAML + OIL** est un langage de balisage sémantique pour les ressources Web. Il s'appuie sur les normes antérieures du W3C telles que RDF et RDF Schéma, et étend ces langages avec des primitives de modélisation plus riches.

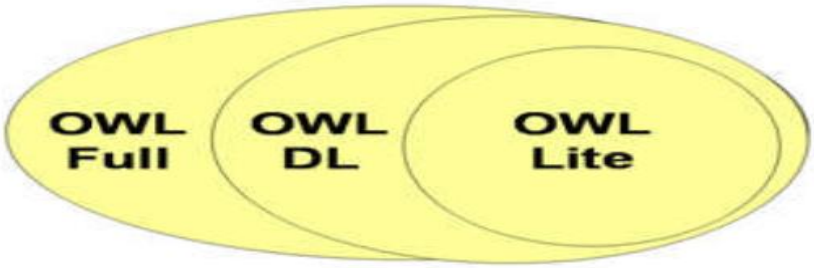

Figure 1: Les types de langage OWL

Il y a une stricte compatibilité ascendante de ces trois langages : toute ontologie **OWL Lite** valide est une ontologie **OWL DL** valide, et toute ontologie **OWL DL** valide est une ontologie **OWL Full** valide. Ainsi, toute conclusion d'une ontologie **OWL Lite** est une conclusion valide d'**OWL DL**, et toute conclusion **OWL DL** est une conclusion valide d'**OWL Full [29].**

2.6. Éditeurs d'ontologie

Il existe plusieurs outils pour éditer et visualiser les ontologies, nous pouvons citer **[26]** :

- **SWOOP** : qui est développé par l'université du Maryland et qui supporte le standard RDF et OWL.
- **OntoEdit** : qui est un éditeur qui intègre l'aspect collaboratif de création d'une ontologie.
- **HOZO** : développé au Japon est un éditeur graphique d'ontologie de haut niveau et permet de gérer des ontologies volumineuses.
- **Protégé** : qui est l'outil de référence dans la création et le développement des ontologies.

Protégé est une plateforme qui permet de créer, de gérer et d'implémenter des ontologies. Elle est très modulaire et peut intégrer plusieurs plug-ins pour la représentation graphique des ontologies. Il a été créé à l'université Stanford et est très populaire dans le domaine du Web sémantique et dans monde de la recherche scientifique.

De plus, **Protégé** est un logiciel conçu en java et il existe une API programmable pour définir et traiter les ontologies dans d'autres projets java.

Ainsi, pour notre projet, nous utiliserons **Protégé** pour créer notre ontologie et grâce au plug-in graphique, nous allons extraire plusieurs représentations graphiques de notre ontologie.

2.7. Critères d'ontologies

D'après **Gruber**, cinq critères permettent de mettre en évidence des aspects importants d'une ontologie **[30]** :

1) **La clarté** : la définition d'un concept doit faire passer le sens voulu du terme, de manière aussi objective que possible (indépendante du contexte). Une définition doit de plus être complète (c'est-à-dire dé nie par des conditions à la fois nécessaires et suffisantes) et documentée en langage naturel.

2) **La cohérence** : rien qui ne puisse être inféré de l'ontologie ne doit entrer en contradiction avec les définitions des concepts (y compris celles qui sont exprimées en langage naturel).

3) **L'extensibilité** : les extensions qui pourront être ajoutées à l'ontologie doivent être anticipées. Il doit être possible d'ajouter de nouveaux concepts sans avoir à toucher aux fondations de l'ontologie.

4) **Une déformation d'encodage minimale :** une déformation d'encodage a lieu lorsque la spécification influe sur la conceptualisation (un concept donné peut être plus simple à définir d'une certaine façon pour un langage d'ontologie donné, bien que cette définition ne corresponde pas exactement au sens initial.). Ces déformations doivent être évitées autant que possible.

5) **Un engagement ontologique minimal :** le but d'une ontologie est de définir un vocabulaire pour décrire un domaine, si possible de manière complète ; ni plus, ni moins. Contrairement aux bases de connaissances par exemple, on n'attend pas d'une ontologie qu'elle soit en mesure de fournir systématiquement une réponse à une question arbitraire sur le domaine. Une ontologie est la théorie la plus faible couvrant un domaine ; elle ne définit que les termes nécessaires pour partager la connaissance liée à ce domaine.

3. Un squelette de méthodologie pour construire des ontologies

3.1. Évaluation des besoins

Le but visé par la construction d'une ontologie se décline en 3 aspects :

L'objectif opérationnel : il est indispensable de bien préciser l'objectif opérationnel de l'ontologie, en particulier à travers des scénarios d'usage.

Le domaine de connaissances : il doit être délimité aussi précisément que possible.

Les utilisateurs : ils doivent être identifiés autant que faire se peut, ce qui permet de choisir en accord avec l'objectif opérationnel, le degré de formalisme de l'ontologie, et sa granularité.

Une fois le but défini, le processus de construction de l'ontologie peut démarrer, en commençant par la phase de conceptualisation **[22]**.

3.2. Conceptualisation

Cette étape permet d'aboutir à un modèle informel, donc sémantiquement ambiguë et généralement exprimé en langage naturel. Elle consiste, à partir des données brutes, à dégager les concepts et les relations entre ces concepts permettant de décrire de manière informelle les entités cognitives du domaine.

L'objectif est d'aboutir à un modèle conceptuel, ce modèle consiste en un ensemble de termes désignant les entités du domaine de connaissances (concepts, relations, propriétés des concepts et des relations, etc.), assortis d'informations exprimant leur sémantique. La découverte des connaissances d'un domaine peut s'appuyer à la fois sur l'analyse de documents et sur l'interview d'experts du domaine. Ces activités doivent être raffinées au fur et à mesure que la conceptualisation émerge **[22]**.

3.3. Ontologisation

L'ontologisation consiste en une formalisation partielle, sans perte d'information, du modèle conceptuel obtenu dans l'étape précédente. Ce qui permet de faciliter sa représentation ultérieure dans un langage complètement formel et opérationnel.

Elle effectue une transcription des connaissances dans un certain formalisme de connaissances, ce formalisme devant être aussi générique que possible, mais sémantiquement clair **[22]**.

3.4. Opérationnalisation

Cette étape consiste à formaliser complètement l'ontologie obtenue dans un langage de représentation de connaissances formel (i.e. possédant une syntaxe et une sémantique) et opérationnel (i.e. doté de services inférentielles permettant de mettre en œuvre des raisonnements), par exemple, le modèle des Graphes Conceptuels ou la Logique de Descriptions.

On obtient alors une représentation formelle des connaissances du domaine. Ainsi, le caractère formel de l'ontologie permet à une machine, via cette ontologie, de manipuler des connaissances du domaine. La machine doit donc pouvoir utiliser des mécanismes opérant sur les représentations de l'ontologie **[22].**

4. Différents besoins d'ontologies

Les ontologies sont utilisées dans plusieurs domaines, les plus répandus sont :

- ✓ Communication.
- ✓ Interopérabilité entre les systèmes.
- ✓ Ingénierie des systèmes.

La figure ci-dessous montre les domaines d'utilisations des ontologies **[22]** :

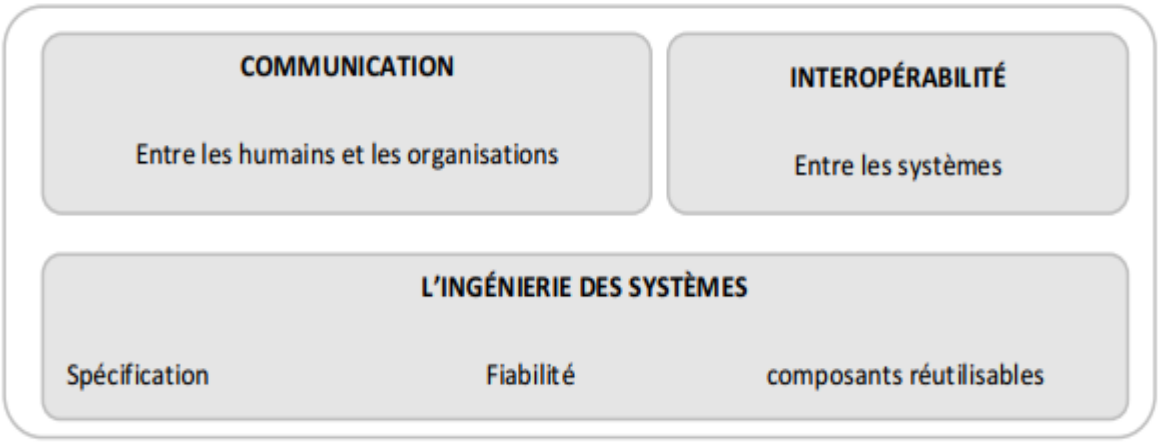

Figure 2 : Domaines d'utilisation des Ontologies.

5. Les ontologies et le CA

Dans ce qui suit nous allons présenter quelques recherches et travaux qui ont utilisé les ontologies dans le CA.

5.1. Gestion sémantique des droits d'accès : AMO

Le Web 2.0 a entrainé une émergence des applications Web dans le monde de l'entreprise. Cette révolution a permis le développement de plusieurs plates-formes pour la collaboration, le télétravail et les réseaux sociaux. Ainsi, les wikis, les blogues, les forums et d'autres outils de partage de contenu sont devenus incontournables pour une entreprise numérique. La particularité de ces systèmes est qu'ils sont faits pour être conçus et déployés par des personnes qui ne sont pas dans le domaine de la conception d'applications web. Car, pour les créer, on utilise d'autres applications Web de gestion de

contenues qui sont connues sous le nom de CMS [4]. Comme tous systèmes informatiques, la problématique de la gestion des droits d'accès est à considérer pour assurer la sécurité de ces outils.

C'est dans ce cadre que **[31]** a défini une ontologie pour la gestion sémantique des droits d'accès au contenu avec l'utilisation d'une ontologie nommée **AMO** (**A**ccess **M**anagement **O**ntologiy).

L'idée qui est à la base de **AMO** est de fournir un mécanisme de gestion des droits d'accès dans les systèmes de gestion de contenu qui reposent sur des serveurs web sémantiques. Ce mécanisme est réalisé grâce à une ontologie qui décrit des classes et des propriétés permettant d'annoter les objets (pages web, article, images, etc.) sur lesquels le contrôle d'accès sera réalisé **[31].**

5.2. Validation automatique des droits d'accès par les ontologies

La sécurité informatique notamment le CA est un aspect critique de nos jours pour des entreprises et d'autres organisations. S'il n'est pas bien géré, des failles majeures et dangereuses peuvent causer d'énorme dégât. De plus, l'émergence de la cybercriminalité a fait que dans plusieurs pays, les législateurs ont créé une série de lois contraignant les entreprises à faire une gestion rigoureuse dans la sécurité des données sensibles et de faire des audits réguliers de leur système informatique.

C'est dans ce cadre que **[28]** a entrepris de développer un outil de validation automatique des droits d'accès qui se base principalement sur l'utilisation de l'ontologie comme base de traitement et d'analyse, et cela dans une infrastructure informatique hétérogène.

5.3. CA basé sur les rôles à l'aide d'une ontologie de référence dans les nuages

Dans l'informatique en nuage, la sécurité est un problème important en raison de la taille croissante des utilisateurs. Les approches actuelles en matière de contrôle d'accès sur les nuages ne répondent pas correctement aux exigences multi-locataires car elles sont principalement basées sur des ID utilisateur individuels à différents niveaux de granularité.

Cependant, le nombre d'utilisateurs peut être énorme et entraîner une surcharge importante dans la gestion de la sécurité. Le contrôle d'accès basé sur les rôles (**RBAC**) est attrayant, car le nombre de rôles est nettement inférieur et les utilisateurs peuvent être classés en fonction de leurs rôles.

C'est dans ce cadre que **[32]** propose un modèle RBAC utilisant une ontologie de rôle pour une architecture multi-locataires (MTA) dans des nuages. L'ontologie est utilisée pour construire la hiérarchie des rôles pour un domaine spécifique. Des algorithmes d'opérations de transformation d'ontologies sont fournis pour comparer la similarité de différentes ontologies.

5.4. Modèle de CA basé sur ontologie pour le raisonnement du politique de sécurité dans le cloud computing

Il existe de nombreux problèmes de sécurité dans les environnements de services du cloud computing, notamment la virtualisation, le traitement distribué des données volumineuses, la facilité de maintenance, la gestion du trafic, la sécurité des applications, le contrôle d'accès, l'authentification et la cryptographie. En particulier, l'accès aux données à l'aide de diverses ressources nécessite un

[4] **CMS** : **C**ontent **M**anagement **S**ystem, en français on parle de système de gestion de contenu : **SGC.**

modèle d'authentification et de contrôle d'accès pour une gestion et un contrôle intégrés dans les environnements de cloud computing.

Les services de cloud computing sont différenciés en fonction des politiques de sécurité en raison des différences de droits d'accès autorisés entre les fournisseurs de services et les utilisateurs. Les modèles **RBAC** et **C-RBAC** (RBAC contextuel) ne suggèrent pas de solutions efficaces et pratiques pour les gestionnaires et les utilisateurs basées sur des méthodes de contrôle d'accès dynamiques. Suggérant la nécessité d'un nouveau modèle de contrôle d'accès dynamique capable de remédier aux limites des caractéristiques de l'informatique en nuage.

C'est dans ce cadre que **[33]** propose **Onto-ACM** (modèle de CA basé sur une ontologie), un modèle d'analyse sémantique pouvant traiter de la différence de CA autorisé entre les fournisseurs de services et les utilisateurs. Le modèle proposé est un modèle d'accès intelligent sensible au contexte permettant d'appliquer de manière proactive le niveau d'accès aux ressources sur la base du raisonnement ontologique et de la méthode d'analyse sémantique.

5.5. Modèle de CA basé sur ontologie **OBAC** pour les services web

Des études montrent qu'il est important de réduire l'écart entre les services de sécurité et le Web sémantique. C'est dans ce cadre que **[34]** présente un modèle de CA basé sur l'ontologie(**OBAC**) pour prendre en charge le service Web sémantique.

Pour cela, des ontologies de sécurité sont développées pour spécifier les concepts et les termes impliqués dans ce modèle. Le modèle de CA proposé par **[34]** est expressif et général avec ces caractéristiques importantes :

(i) L'utilisation de l'ontologie permet de raisonner pour la prise de décision de CA et permet aux leurs informations d'être recherchées, interrogées et découvertes automatiquement.

(ii) Le modèle proposé présente un degré d'interopérabilité plus élevé par rapport aux autres approches du mécanisme de CA. Cela est dû à la nature des ontologies qui fournissent une interopérabilité sémantique.

(iii) Le modèle proposé est sensible au contexte. L'ontologie de contrainte représente différents types de contrainte de contexte.

(iv) Ce modèle est conçu sur la base des langages Web sémantiques largement acceptés, le langage d'ontologie Web (OWL) et le langage d'ontologie Web pour le service (OWL-S), de sorte que sa mise en œuvre peut être facilement réalisée en utilisant des outils déjà existants conçus pour fonctionner avec ces langues.

6. Conclusion

Dans ce chapitre, nous avons rappelé la notion des ontologies, leurs différents types et composants, et quelques outils de manipulation. Ainsi, nous avons expliqué les éléments qui ont motivé le choix de développer un outil de validation en utilisant les ontologies.

CHAPITRE III :

MODÉLISATION ET IMPLÉMENTATION DU CA POUR LE DM

1. Introduction

Dans ce chapitre, nous allons présenter la partie modélisation et implémentation que nous avons accompli, et qui consistait à l'édition d'un prototype qui permet de faire la validation automatique des droits d'accès ; Suivi par son exploitation dans une application de **DM**.

2. Dossier médical

Depuis le début des années 2000, la gestion des informations liée à la prise en charge d'un patient a été profondément modifiée. Autrefois conservée sous la forme d'un **D**ossier **M**édical (**DM**) papier, les données du patient ont été rassemblés sous la forme d'un **DM I**nformatisé (**DMI**) par la numérisation progressive des hôpitaux. Son développement et sa bonne maîtrise constituent aujourd'hui un sujet capital au sein d'un système de santé.

Le **DM** est un ensemble des informations concernant la santé du patient détenues par le professionnel de santé, qui sont formalisées et ont contribué à l'élaboration et au suivi du diagnostic et du traitement ou d'une action de prévention, ou ont fait l'objet d'échanges écrits entre professionnels de santé **[35].**

Depuis juin 2016, le ***DM Personnel*** est devenu ***DM Partagé (DMP)***. Il s'agit du même service, qui a été amélioré afin de mieux répondre aux besoins des patients et des professionnels de santé **[36]**.

Le **DMP** est un **DMI** qui appartient à la personne soignée (c'est le patient qui choisit les professionnels de santé qui seront autorisés à l'utiliser.), il est sécurisé (il garantit un très haut niveau de sécurité et de confidentialité des données personnelles.) et partagé entre les professionnels de santé avec l'accord préalable du patient, il permettra aux professionnels de consulter :

- ✓ L'historique clinique et médicamenteux d'un patient indépendamment du lieu et du moment.
- ✓ Les données démographiques du patient : adresse, date de naissance, numéro d'immatriculation et numéro d'identification du patient, etc.
- ✓ Il rassemble les informations médicales relatives à un patient, nécessaires à la coordination des soins : prescriptions, synthèses médicales, comptes rendus d'hospitalisation, résultats d'analyses, mentions d'allergies, etc. **[37]**

2.1. L'objectif du DMP

Le DMP a les objectifs suivants **[38]** :

- Assurer la continuité des soins.
- Simplifier la vie du patient dans ses démarches de soins.
- Améliorer le suivi du parcours de soins coordonné.
- Coordonner les soins entre médecine libérale et secteur hospitalier.
- Permettre l'accès aux données essentielles dans le contexte de l'urgence.
- Limiter les prescriptions redondantes.
- Lutter contre la iatrogénie médicamenteuse [1]
- Partager les résultats pour mieux gérer les prescriptions d'examens complémentaires.
- Disposer d'un outil de communication professionnelle.

2.2. La création du DMP

La création du DMP se fait à la demande du patient par un médecin ou une structure de soins, lors d'une consultation médicale ou lors d'une admission au sein d'un Centre Hospitalier **[39].**

En pratique, tout professionnel de santé peut créer un DMP : médecin généraliste et spécialiste, radiologue, infirmier, pharmacien, etc.

Le médecin, ou la structure de soin doit normalement disposer d'un logiciel compatible. Sinon, il est possible de se connecter directement par Internet sur le dossier. C'est également par Internet que le patient se connecte, prend connaissance, puis gère son dossier, y compris les droits d'accès des professionnels de santé **[37].**

Le dossier est la propriété du patient avant tout, il est obligatoire d'informer le patient sur le fonctionnement du DMP, ce que cela implique et sur leurs droits. Puis, une fois informé, il donne son consentement oral. Ce dernier est recueilli en cochant une case dans l'écran informatique. Pas de document papier à signer ni à conserver. Le système informatique garde la trace du consentement **[37].**

Tout est porté dans le DMP, y compris le lieu de création et l'identité de la personne qui l'a créé.

Le patient doit disposer d'une carte vitale et d'un **I**dentifiant **N**ational de **S**anté (INS) [2], fourni à la création du dossier. Le médecin, ou les autres personnels soignants, doivent disposer d'une carte de professionnel de santé et de l'INS du patient si le dossier existe déjà. La sécurité d'accès est assurée par la carte vitale et par la carte professionnelle de santé. Ensuite, insérer la carte vitale du patient dans le lecteur afin de créer le DMP. La sécurité d'accès au DMP repose sur le couple « identifiant (INS) – mot de passe », via une liaison Internet protégée (HTTPS) **[39].**

Le système va vérifier que le patient n'a pas déjà un DMP. Ensuite, le patient doit cocher les actions qu'il autorise sur son DMP (le nom et les données des personnelles autorisées).

---

[1] La iatrogénie médicamenteuse : désigne les effets indésirables provoqués par les médicaments. Elle regroupe des symptômes très divers depuis la simple fatigue jusqu'à l'hémorragie digestive, ou la fracture de la hanche. La prise de médicaments s'est aujourd'hui banalisée et ces risques sont trop souvent sous-estimés.

[2] **I**dentifiant **N**ational de **S**anté (**INS**) : est un identifiant attribué à tout bénéficiaire de l'assurance maladie. Il est utilisé par les professionnels de santé pour attribuer des informations de santé à la personne qui en est titulaire.

Le DMP alors est créé, la chargée d'accueil va remettre au patient son « document des secrets » qui atteste de cette création et liste les codes qui seront nécessaires au patient pour consulter son DMP à tout moment même chez lui **[40].**

Le patient a la possibilité de décider à tout moment de fermer son DMP : les données sont alors conservées durant dix ans ; et durant cette période, il peut demander qu'il soit réactivé par un professionnel de santé avec les données qu'il contient **[37]**. Il peut également demander la destruction totale ou partielle de son DMP. La destruction est irréversible **[40].**

2.3. Les éléments du DMP

Le DMP est composé de plusieurs informations différentes **[37] :**

- Le dossier socio-administratif : nom complet actualisé ; sexe ; date de naissance ; numéro du dossier ; adresse ; téléphone ; profession ; numéro de sécurité sociale ; personne à contacter.

- Rencontre : nom du médecin ; date de la rencontre ; type de contact (directe, par mail, par téléphone, etc.) ; décisions.

- Historique médicale actualisée et facteurs de santé : antécédents personnels ; antécédents familiaux ; facteurs de risque ; vaccinations et autres actions de préventions et dépistage.

- Informations Recueillies dès le 1er contact et durant le séjour :

  - La lettre du médecin qui est à l'origine de la consultation ou de l'admission.
  - Les motifs d'hospitalisation.
  - La recherche d'antécédents et de facteurs de risque.
  - Les conclusions de l'évaluation clinique initiale.
  - La nature des soins dispensés et les prescriptions établies lors de la consultation externe ou du passage aux urgences.
  - Les informations relatives à la prise en charge en cours d'hospitalisation : état clinique, soins reçus, examens para cliniques, notamment d'imagerie.
  - Les informations sur la démarche médicale adoptée dans certaines conditions.
  - Le dossier d'anesthésie.
  - Le compte-rendu opératoire ou d'accouchement.
  - La mention des actes transfusionnels pratiqués sur le patient et le cas échéant, copie de la fiche d'incident transfusionnel.
  - Les éléments relatifs à la prescription médicale, à son exécution et aux examens complémentaires.

- Les Informations formalisées établis à la fin du séjour comportant notamment :

  - Le compte-rendu d'hospitalisation et la lettre rédigée à l'occasion de la sortie.
  - La prescription de sortie et des doubles d'ordonnances de sortie.
  - Les modalités de sortie (domicile, autres structures).
  - La fiche de liaison infirmière.

2.4. Droits du patient sur son dossier médical

Toute personne a droit à la protection de sa santé et aux soins qu'exige son état de santé, à toutes les étapes de la vie. Le code de la santé publique impose des droits à la confidentialité et l'accès a aux patients **[41]** :

- Droit au respect de sa vie privée et du secret des informations la concernant : « *Toute personne prise en charge par un professionnel, un établissement, un réseau de santé ou tout autre organisme participant à la prévention et aux soins a droit au respect de sa vie privée et du secret des informations la concernant*. **» [42].**

- Toute personne a accès à l'ensemble des informations concernant sa santé : « *Tout patient a plus que 14 ans a le droit d'accès à son dossier sauf si le médecin traitant ou designer juge que cela risque de causer un préjudice grave à sa santé* » **[43].**

- Dossier d'un patient décédé : l'accès au dossier médical d'un patient décédé est strictement encadré car le droit au secret professionnel survit au décès du patient. Nous retrouvons des dispositions permettant cet accès principalement dans la *Loi sur les services de santé et services sociaux,* dans la *Loi sur la protection des renseignements personnels dans le secteur privé* et dans le *Code de déontologie des médecins.* Ce n'est que lorsqu'il sera autorisé par la loi qu'un tiers pourra avoir accès à certains renseignements du dossier médical d'une personne décédée.

Le conjoint, les ascendants (père et mère) et les descendants (enfants) directs du patient décédé âgé de plus de 14 ans ont le droit de connaître les renseignements relatifs à la cause du décès, à moins que le patient n'ait consigné par écrit à son dossier son refus d'accorder ce droit d'accès. Nonobstant, ce refus possible du patient, toute personne liée par le sang à ce dernier a le droit de recevoir la communication des renseignements contenus dans le dossier, dans la mesure où cette communication est nécessaire pour vérifier l'existence d'une maladie génétique ou d'une maladie à caractère familial **[44].**

- Conformément à l'article 34 de la loi informatique et libertés modifiée, une société s'engage à prendre toutes précautions utiles afin de préserver la sécurité des informations et notamment d'empêcher qu'elles ne soient déformées, endommagées ou communiquées à des personnes non autorisées **[45].**

2.5. La Sécurité des dossiers patients

Un des défis majeurs pour la réussite du DMP est de créer la confiance des utilisateurs dans un outil emblématique de la dématérialisation des données de santé au service de l'amélioration de la qualité et de la coordination des soins. À ce titre, la sécurité est prise en compte dans toutes les phases du cycle de vie du système.

Les orientations retenues pour sécuriser les services du DMP sont fortement conditionnées par le respect des droits du patient qui choisit les professionnels de santé autorisés à consulter son dossier.

Les mesures de sécurité mises en œuvre ne doivent ni représenter une gêne pour la prise en charge des patients par les professionnels de santé ni entraîner de perte de temps voire d'éventuelle (perte de

chance). Il y a donc un arbitrage nécessaire à effectuer entre « facilité d'accès au DMP », dans un objectif de gain de chance et «sécurisation» de l'accès aux données de santé personnelles **[46].**

La sécurité du DMP repose sur :

• La mise en œuvre de contrôles a priori : tous les utilisateurs sont authentifiés de manière forte pour accéder au dossier médical, le contrôle d'accès aux informations qui est appliqué laisse la possibilité à un professionnel de santé d'accéder sous son entière responsabilité aux données de santé des patients qu'il prend en charge dans la limite de l'autorisation d'accès donnée par le patient et des documents autorisés pour sa profession.

• Le contrôle a posteriori des actions des utilisateurs : ce contrôle est fondé sur une traçabilité et une responsabilité totale des actions effectuées par l'ensemble des utilisateurs, et toute personne a une mauvaise utilisation sera pénalisés.

L'entrée en service du DMP favorise le partage des données de santé, et entraîne une évolution significative de la nature des risques relatifs à la sécurité de l'information de point de vue d'évolution des menaces et des vulnérabilités potentielles portant sur les données.

Les établissements de santé doivent donc toujours protéger les données personnelles de santé de leurs patients au sein de leur *Système d'Information Hospitalier*.

Les gestionnaires des dossiers médicaux contrôlent l'accès aux dossiers des patients et préservent la confidentialité et l'intégrité des données personnelles contenues dans ces dossiers. Il trace les accès et enregistre toutes les actions d'un patient sur son DMP. Toutefois, lorsqu'un utilisateur accède à des données dans un système en ligne, ces données sont aussi temporairement présentes dans la machine utilisée. Si cette machine n'est pas protégée, il peut faire l'objet d'une attaque et héberger un code malveillant capable d'exploiter ces données. Dans ce cas l'accès au système à partir d'un terminal protégé contre les attaques Internet et les codes malveillants est une précaution essentielle de la sécurité **[46].**

3. Modélisation de notre politique de sécurité

Le modèle le plus utilisé dans le domaine médical est le modèle Or-BAC ; car il offre la possibilité d'exprimer des règles contextuelles relatives aux permissions, interdictions, obligations et aux recommandations. Ce type de règle est particulièrement utile pour exprimer des politiques de sécurité dans le domaine médical ; en plus, il répond à la plupart des besoins de sécurité.

Dans ce qui suit, nous allons décrire les éléments de ce modèle pour une structure de santé Algérienne (CHU).

3.1. Organisation

L'entité centrale (CHU) dans le cas de la modélisation de la politique de sécurité liée au dossier patient est l'organisation au sens Or-BAC réunissant un ensemble de professionnels de santé et de patients. Sa structure est donnée par le schéma de hiérarchie d'organisations suivant **[8]** :

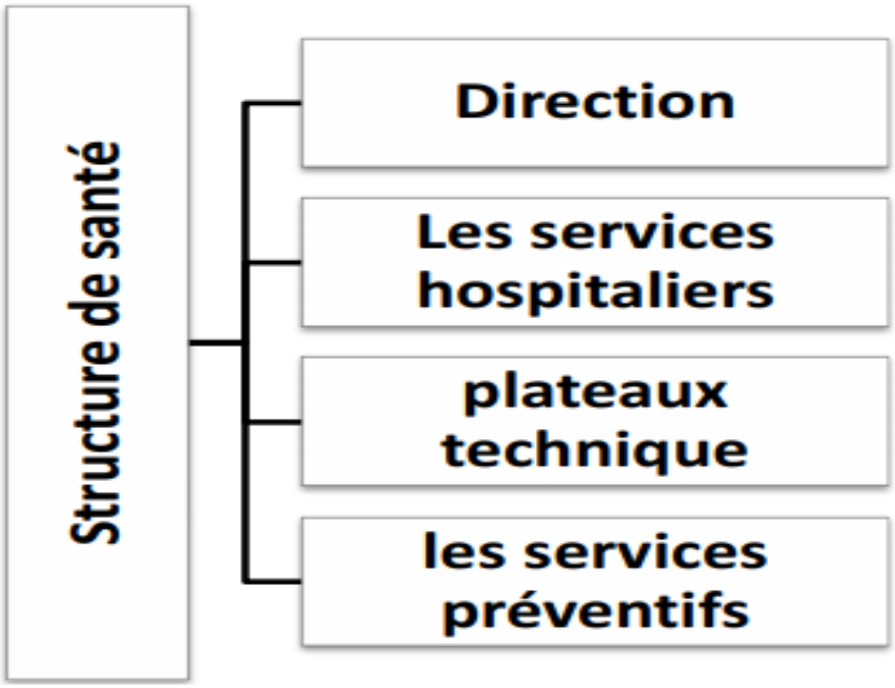

Figure 1: Hiérarchie d'organisation d'une structure de santé **[8].**

3.2. Sujets et rôles

Dans notre politique de sécurité Or-BAC, l'organisation (CHU) affect un rôle à un sujet.

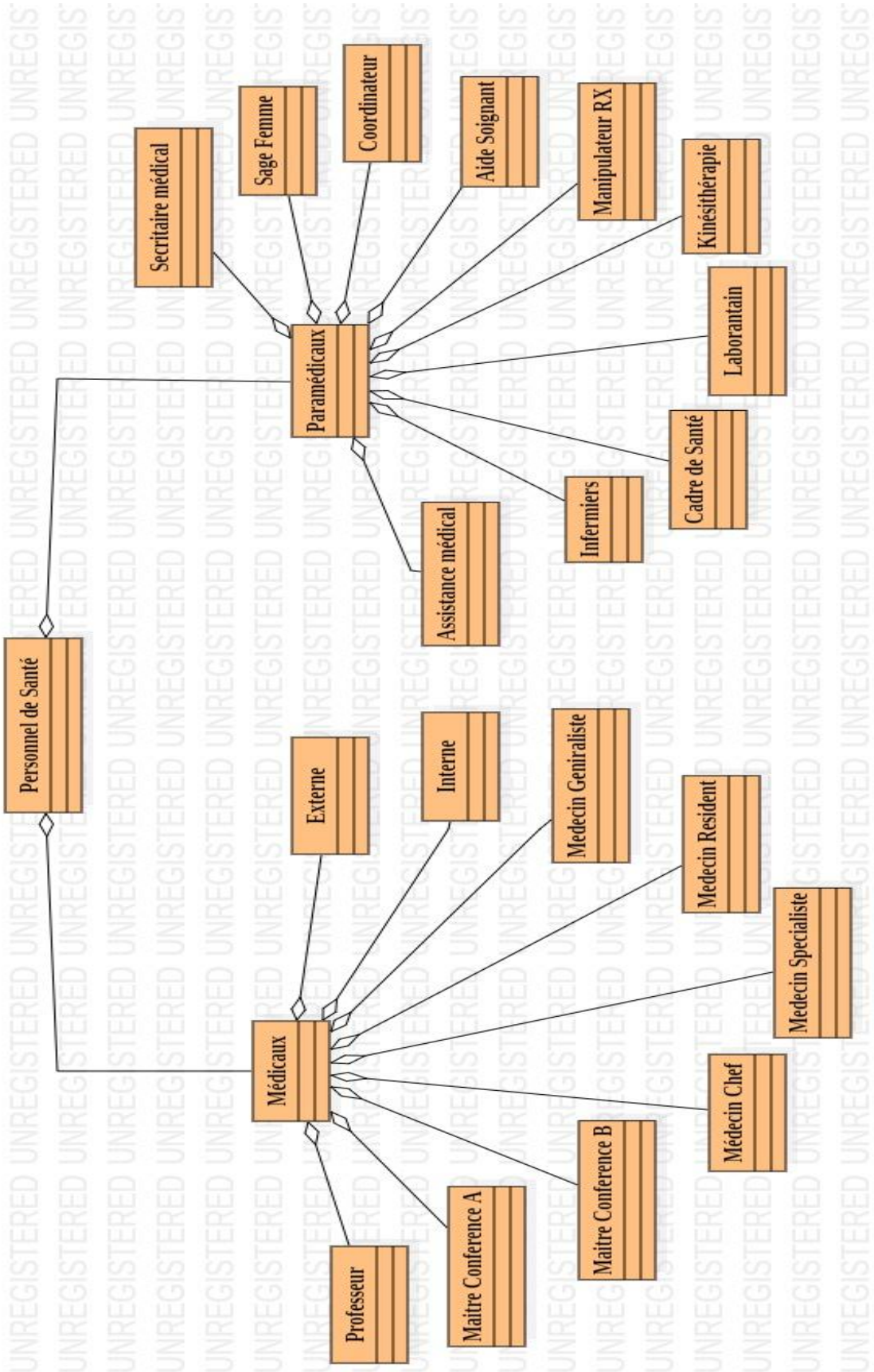

Figure 2: Hiérarchie de personnel de santé **[8].**

3.3. Objets et vues

Le dossier médical comporte de nombreux documents. Dans Or-BAC, les documents sont modélisés sous forme d'objets qui sont regroupés dans des vues.

Cette abstraction des objets en vues permet de diminuer le nombre de règles à définir dans la politique de sécurité à l'image de l'apport de la structuration des sujets en rôles.

En effet, pour chaque document du dossier médical, il existe des contraintes. Pour chaque patient hospitalisé dans un établissement de santé public ou privé.

Ce dossier contient les vues suivantes **[8]** :

- Identification (nom, prénom, date de naissance,).
- Rencontre (nom médecin, prénom médecin, date de rencontre, le type de prise en charge prévu, les prescriptions effectue, motifs d'hospitalisation, lettre d'admission).
- Informations techniques (numéro de sécurité sociale, personnes à contacter).
- Interrogatoire (antécédents, historiques des consultations).
- Résultats d'examens biologiques.
- Les données de soins (pathologies en cours, traitements prescrits et administres).
- Imagerie (date d'imagerie, type d'imagerie, compte rendu d'imagerie).
- Le dossier d'anesthésie.
- Le compte rendu opératoire ou d'accouchement.
- Lettre de sortie (soins reçu, compte rendu, date, type).
- Les correspondances échangées entre professionnels de santé.
- Don d'organes (le consentement).
- Personnes de confiance (nom, prénom, numéro de téléphone).

3.4. Action et activités

Les activités correspondent à des actions qui ont un objectif commun, dans notre modèle nous avons identifié cinq activités : Modifié, Ajouter, Supprimé, Transférer, Consulter **[8]**.

3.5. Contextes

Dans notre modèle nous avons identifié plusieurs contextes d'attribution des droits d'accès à ce type de document qui peuvent être cumulés selon les besoins de sécurité **[8]** :

- **Urgence** : ce contexte est activé dans le cas d'urgence.

- **Temporel** : ce sont des contextes qui régissent la validité des privilèges en mesurant leurs durées en intervalle de temps ou en se référant à une date précise, ce qui suppose que le système d'information dispose d'un dispositif mesurant le temps (généralement une horloge système) et que la consultation de ce dispositif soit possible.

- **Spatial** : certaines règles de CA sont déterminées en connaissant au préalable le lieu (localisation, espace) du sujet, il s'agit donc d'un contexte spatial qui peut être physique dépendant d'une position géographique (siège, succursale, bureau, région, etc.), ou logique (Appartenance à un réseau, Cellule GSM, etc.). Dans notre cas nous avons identifié deux contextes : intérieur de l'organisation ou hors organisation.

4. Construction de notre Ontologie

4.1. Liste des concepts intervenant dans le CA

Dans le domaine de **CA**, il est important de mentionner qu'un autre axe de recherche se base sur des ontologies comme source de vocabulaire et base de modélisation convenable au traitement automatique et au formalisme.

L'objectif de l'utilisation d'une ontologie étant de donner un caractère générique à un outil de validation de droit d'accès et de faire abstraction du modèle de **CA** sous-jacent.

Les concepts représentés dans notre ontologie utilisent les concepts de modèle de CA à base d'organisation **Or-BAC**.

Le modèle de **CA Or-BAC** vise à résoudre certains problèmes rencontrés par les premiers modèles de CA des années 90 et à établir une politique de sécurité plus abstraite.

Il s'intéresse, non seulement aux permissions, mais aussi aux interdictions, obligations et recommandations dans une politique de sécurité. **Or-BAC** prend le concept de rôle dans **RBAC**. En plus de ce concept, il ajoute des nouveaux concepts pour structurer les sujets, les objets et les actions.

Le concept central de ce modèle est la notion d'organisation comme son nom l'indique. Une organisation peut être un groupe structuré de sujets jouant des rôles déterminés, par exemple : un hôpital, une clinique médicale, un service d'urgence, etc.

L'organisation représente l'ensemble des rôles, des activités, et des vues qui représentent les abstractions respectives des utilisateurs, des opérations et des objets par rapport à une organisation

donnée. Par exemple, un utilisateur est lié à un ensemble de rôles pour une organisation donnée. Il peut être affecté à d'autres rôles pour une autre organisation.

La liste des concepts de notre ontologie peut alors être dans un premier temps regroupée en deux niveaux essentiels :

- Élément concret : Sujet ; Objet ; Action.
- Élément Abstrait : Contexte ; Rôle ; Vues ; Activités ; Règles.

4.2. Relation entre les différents concepts du CA

Les relations entre les différents concepts de notre ontologie se définissent comme suit :

- Une *Organisation* est composée de : *E. Concret* et *E. Abstrait.*
- E. Concret est composé de : *Sujet*, *Objet* et *Action*.
- E. Abstrait est composé de : *Contexte*, *Rôle*, *Vues*, *Activités* et *Règles*.
- *Organisation* habilite un *Sujet* S à jouer un *Rôle* r.
- *Organisation* utilise l'*Objet* O dans la *Vue* V.
- *Organisation* considère l'*Action* α comme faisant partie de l'*Activité* A.
- *Contexte* C est vrai entre le *Sujet* S, l'*Objet* O et l'*Action* α ; au sein d'*Organisation*
- *Rôle* peut avoir un/plusieurs *Règles* (permission, obligation, recommandations, interdiction).

Alors les propriétés que nous disposons sont :

- *estComposeDe* : qui exprime les éléments qui composent un concept.
- *hasRegle* : affecte un ou plusieurs règles à un rôle (permission, obligation, recommandation, interdiction).
- *actionEstConsidereComme :* préciser l'action (ajouter, supprimer, modifier, etc.)
- *contextEstVraisDans :* préciser le contexte (Spatial, Temporel ou Urgence).
- *objetEstUtiliséDansLaVue :* préciser la vue utilisée (identification, rencontre, historique, etc.)
- *sujetEstJoueLeRole :* affect un rôle à un sujet.

La simplicité de nos concepts et de leurs relations résume les droits d'accès en :

- un Sujet a la permission(ou interdiction /obligation/recommandation) de faire une Action sur un Object.

La figure suivante est un diagramme de classe qui représente la structure de notre politique de sécurité :

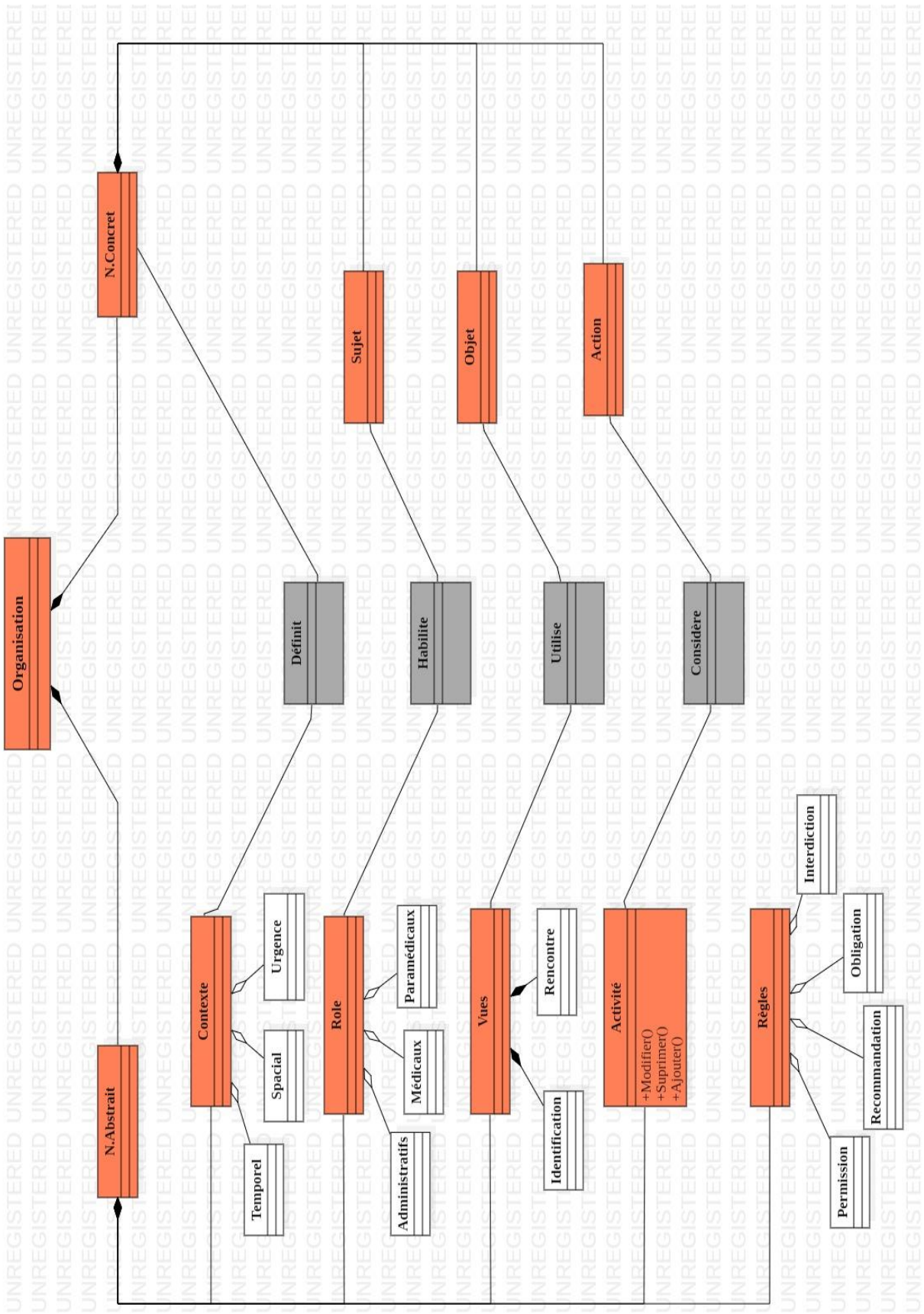

Figure 3: Modélisation UML de notre politique de CA.

4.3. Choix de l'éditeur de l'ontologie :

Parmi les éditeurs des ontologies existant nous avons choisis d'utiliser protégé (version 3.4.8). Protégé est une plateforme qui permet de créer, de gérer et d'implémenter des ontologies. Elle est très modulaire et peut intégrer plusieurs plug-ins pour la représentation graphique des ontologies. Il a été créé à l'université Stanford et est très populaire dans le domaine du Web sémantique et dans le monde de la recherche scientifique **[26]**.

4.4. Représentation graphique de l'ontologie

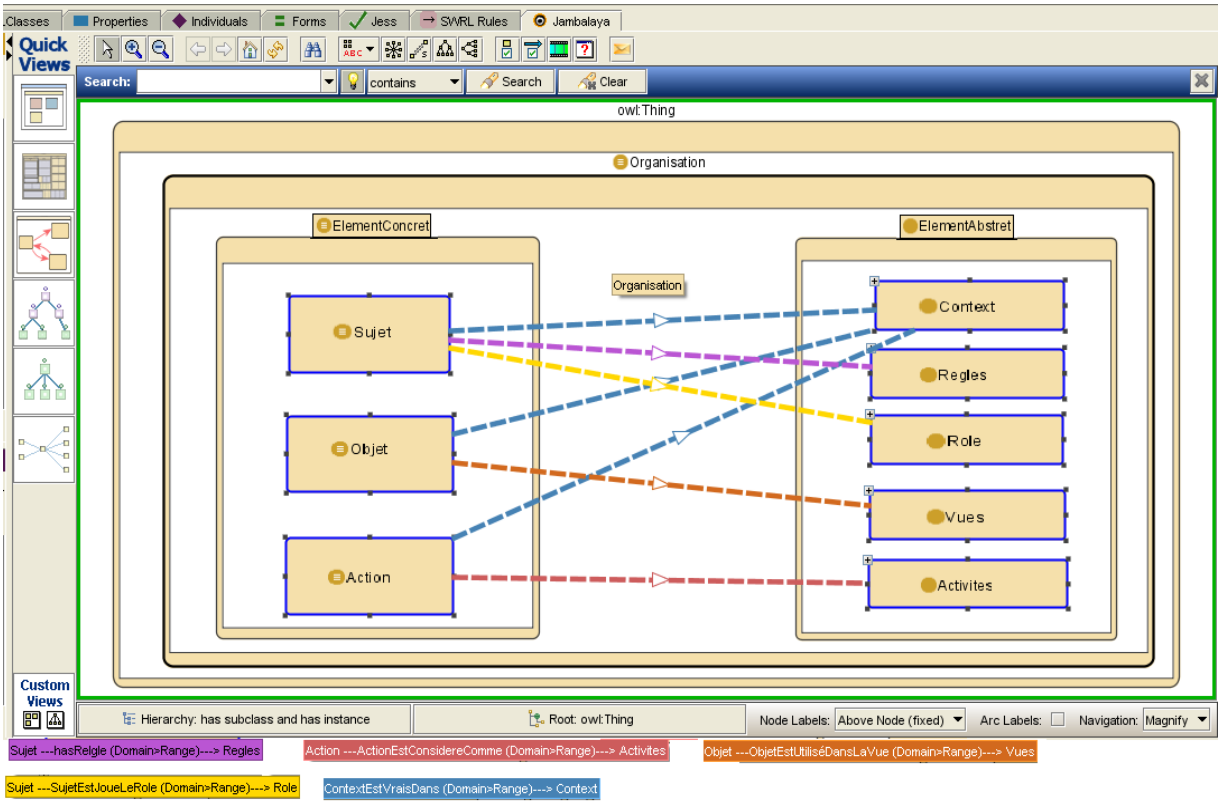

Figure 4: Représentation Graphique de l'ontologie.

4.5. Vérification de la cohérence de l'ontologie

Le grand intérêt de l'utilisation de Protégé est la possibilité de vérifier si l'ontologie créée ne contient pas des définitions contradictoires.

Les ontologies peuvent être traitées par un raisonneur. Un des services les plus importants que le raisonneur peut fournir est de tester la subsumption [3]. À partir de ce service, le raisonneur peut construire une hiérarchie de l'ontologie inférée. Un autre service standard offert par le raisonneur est de tester la consistance de l'ontologie.

Pour la vérification de notre ontologie, nous avons utilisé Pellet de Protégé (version 1.5.2).

Jusqu'à là, nous avons décrit les concepts essentiels de notre ontologie qui basé sur le modèle Or-BAC. L'étape suivante est de créer les règles de droits d'accès.

[3] Raisonnement par lequel on met une idée sous une autre plus générale.

4.6. SWRL

SWRL, acronyme pour « **S**emantic **W**eb **R**ule **L**anguage », permet d'exprimer des règles logiques sur une ontologie sous la forme d'une clause « *antécédent* → *conséquence* », c'est-à-dire que **Si** l'antécédent est exact, **Alors** la conséquence doit aussi l'être **[34]**.

OWL permet de raisonner sur une ontologie afin de vérifier sa consistance logique. OWL étendu par un Langage de Règles **SWRL** permet de représenter l'aspect dynamique du fonctionnement de l'environnement.

SWRL est un langage qui enrichit la sémantique d'une ontologie définie en OWL. C'est la combinaison du langage **OWL DL** et le langage **Rule ML** (**R**ule **M**arkup **L**anguage). SWRL permet contrairement à OWL, de manipuler des instances par des variables (? x,? y,?z). Il ne permet pas de créer des concepts ni des relations, il permet simplement d'ajouter des relations suivant les valeurs des variables et la satisfaction de la règle **[35]**.

Dans notre politique de sécurité, la relation Permission par exemple correspond à une relation entre les organisations, les rôles, les vues, les activités et les contextes. Les relations Interdiction, Obligation et Recommandation sont définies de la même manière.

Permission (**org**, **r**, **a**, **v**, **c**) signifie que l'organisation **org** accorde au rôle **r** la permission de réaliser l'action **a** sur la vue **v** dans le contexte **c**.

Par exemple, nous pouvons affirmer que :

- Au niveau de CHU : **Si** un *Médecin généraliste* demande l'accès au DMP d'un patient pour *Consulter* l'*imagerie* en cas d'*Urgence* **Alors** le système autorise l'accès.

En utilisant la syntaxe de SWRL, on obtient :

SujetEstJoueLeRole(?x, MedecinGeneraliste1) ∧ ActionEstConsidereComme(?x, Consulter1) ∧ ObjetEstUtiliséDansLaVue(?x, Imagerie1) ∧ ContextEstVraisDans(?x, Urgence1) → hasRelge(?x,Permission)

Dans SWRL, les variables sont précédées d'un point d'interrogation. Ici, elles sont les **?Sujet**, les **?Objet** et les **?Action**. La conséquence de cette règle est qu'il sera ajouté à tous les éléments **?Sujets** répondant à l'antécédent de la règle la propriété « **hasRegle** » avec comme valeur **Permission**, de manière à ce que la conséquence soit elle aussi positive.

La combinaison d'un langage de règles avec une ontologie offre plusieurs points positifs :

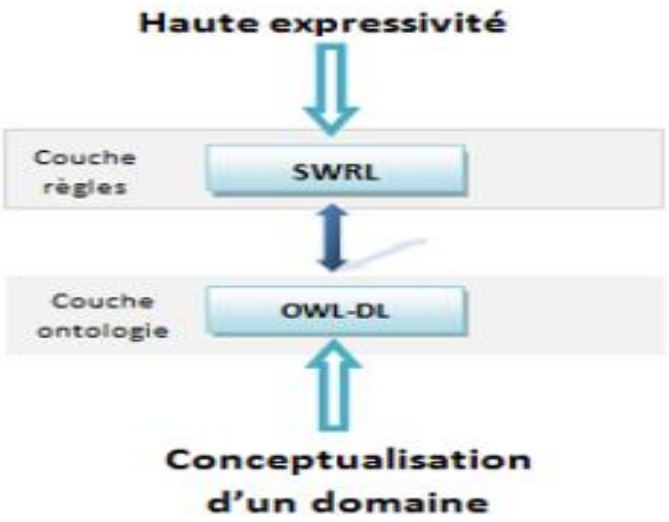

Figure 5: Intérêt de combinaison règles et ontologie.

4.7. SWRL Jess Tab

Jess est un moteur de règles réalisé, sous **Sun** avec le langage Java par **Ernest Friedman-Hill** à « **Sandia National Laboratories in Livermore, CA »**. L'utilisation de **Jess** permet de produire des programmes capables de raisonner, utilisant les connaissances exprimées sous forme de règles déclaratives. **Jess** est considéré comme un outil rapide et disponible et il peut être intégré dans n'importe qu'elle application java **[47]**.

5. Intégration de la politique d'accès dans une application

- Dans le but de tester notre modèle de CA nous avons développé une application nommée **DMP-Doc**.

- **DMP-Doc** est une application de gestion de patient, créée pour aider les personnels de santé à gérer les données des patients. Elle embarque plusieurs fonctions intéressantes : identification de patient, les rencontres, les informations techniques, les données de soins, résultats d'examens biologiques, etc.

- Notre application a été développée avec l'environnement de développement **WinDEV.**

- **WinDEV** est un atelier de génie logiciel (AGL) édité par la société française PC SOFT et conçu pour développer des applications, principalement orientées données pour Windows et également pour **Linux**, **.NET** et **Java**. Il propose son propre langage : le **WLangage**.

- Nous avons développé notre application en parallèle avec notre politique de sécurité.

- La figure suivante est un diagramme de séquences qui résume le comportement du notre système en général. Il modélise le scénario de ce comportement, et définit les communications entre les entités du système.

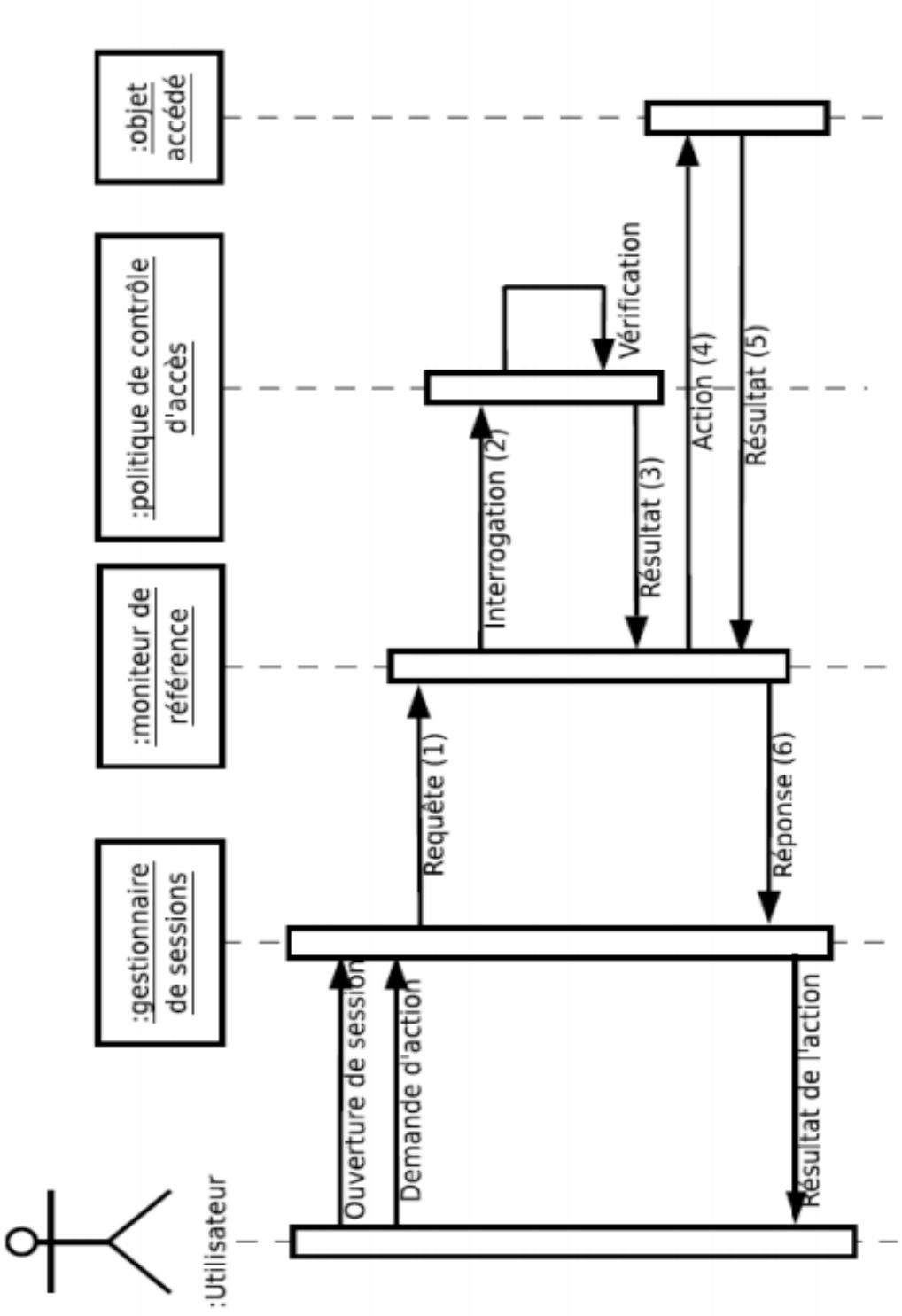

Figure 6: Diagramme de séquences.

- Les fonctionnalités et interfaces principales de **DMP-Doc** sont exprimés en détailles dans (**Annexe B**)

6. Conclusion

L'implantation de notre outil de contrôle d'accès se base principalement sur l'utilisation de l'ontologie comme base de traitement et d'analyse. Ainsi, dans ce chapitre, nous avons présenté le **DMP,** l'ontologie du CA et les différents éléments qui entrent en jeu dans le processus de validation.

Ensuite, nous avons intégré cette ontologie dans une application (nommée **DMP-Doc)** pour la gestion du DMP.

CONCLUSION GÉNÉRALE

La sécurité informatique notamment le contrôle d'accès est un aspect critique de nos jours pour les organisations. S'il n'est pas bien géré, des failles majeures et dangereuses peuvent causer d'énorme dégât.

Plusieurs systèmes informatiques implémentent le contrôle d'accès en se basant sur des modèles comme le MAC, DAC, RBAC entre autres. Un modèle de contrôle d'accès permet de définir une stratégie de définition de règles pour l'attribution des droits d'accès. Ainsi, chaque système a sa propre stratégie donc son propre modèle de contrôle d'accès.

C'est dans ce cadre que nous avons développé un modèle de contrôle d'accès **CA** qui se base principalement sur l'utilisation de l'ontologie comme base de traitement et d'analyse. Ainsi, nous avons présenté l'ontologie du **CA** et les différents éléments qui entrent en jeu dans le processus de validation.

Ensuite, nous avons intégré cet outil dans une application (nommée **DMP-Doc)** pour la gestion du DMP.

De ce fait, comme perspective, nous pensons qu'il y a beaucoup de choses restent à réaliser et plusieurs recherches peuvent être distinguées :

- Introduire la notion d'ontologie avec d'autres modèles de CA.
- Travailler en plus sur l'application DMP-Doc pour l'améliorer et lui rendre plus pratique.

Annexe (A) : Exemple des règles du contrôle d'accès.

Interdiction (Chu, généraliste, Modifier, Identification, Temporel & Spatial)

Interdiction (Chu, généraliste, Modifier, Identification, urgence)

Interdiction (Chu, généraliste, Ajouter, Informations techniques, urgence)

Permission (Chu, généraliste, Consulter, Informations techniques, urgence)

Permission (Chu, généraliste, Consulter, Les données de soins, urgence)

Permission (Chu, généraliste, Consulter, imagerie, urgence)

Interdiction (Chu, généraliste, Ajouter, imagerie, urgence)

Permission (Chu, généraliste, Consulter, Le dossier d'anesthésie, urgence)

Interdiction (Chu, généraliste, Ajouter, Le compte rendu opératoire ou d'accouchement, urgence)

Permission (Chu, généraliste, Consulter, Le compte rendu opératoire ou d'accouchement, urgence)

Permission (Chu, généraliste, consulter, lettre de sortie, urgence)

Permission (Chu, généraliste, consulter, Les correspondances échangées entre professionnels de santé, urgence)

Permission (Chu, généraliste, ajouter, Les correspondances échangées entre professionnels de santé, urgence)

Permission (Chu, généraliste, consulter, Personnes de confiance, urgence)

Interdiction (Chu, professeur, modifier, Identification, urgence)

Interdiction (Chu, professeur, supprimer, Identification, urgence)

Interdiction (Chu, professeur, Ajouter, Informations techniques, urgence)

Interdiction (Chu, professeur, Consulter, Informations techniques, urgence)

Permission (Chu, professeur, Consulter, Résultats d'examens biologiques, urgence)

Permission (Chu, professeur, Consulter, Les données de soins, urgence)

Interdiction (Chu, professeur, ajouter, imagerie, urgence)

Permission (Chu, professeur, consulter, imagerie, urgence)

Interdiction (Chu, professeur, Ajouter, Le dossier d'anesthésie, urgence)

Permission (Chu, professeur, Consulter, Le dossier d'anesthésie, urgence)

Permission (Chu, professeur, Ajouter, Le compte rendu opératoire ou d'accouchement, urgence)

Permission (Chu, professeur, Consulter, Le compte rendu opératoire ou d'accouchement, urgence)

Permission (Chu, professeur, consulter, lettre de sortie, urgence)

Permission (Chu, professeur, ajouter, Les correspondances échangées entre professionnels de santé, urgence)

Permission (Chu, professeur, consulter, Les correspondances échangées entre professionnels de santé, urgence)

Interdiction (Chu, professeur, Ajouter, Personnes de confiance, urgence)

Permission (Chu, professeur, Consulter, Personnes de confiance, urgence)

Interdiction (Chu, généraliste, Modifier, Informations techniques, urgence & Temporel & Spatial)

Interdiction (Chu, généraliste, Modifier, Interrogatoire, Temporel & Spatial)

Interdiction (Chu, généraliste, Modifier, Interrogatoire, urgence)

Interdiction (Chu, généraliste, Modifier, Résultats d'examens biologiques, Temporel & Spatial)

Interdiction (Chu, généraliste, Modifier, Résultats d'examens biologiques, urgence)

Interdiction (Chu, généraliste, Modifier, Imagerie, Temporel & Spatial)

Interdiction (Chu, généraliste, Modifier, Imagerie, urgence)

Interdiction (Chu, généraliste, Modifier, Le dossier d'anesthésie, urgence)

Interdiction (Chu, généraliste, Modifier, Le dossier d'anesthésie, Temporel & Spatial)

Interdiction (Chu, généraliste, Modifier, Personnes de confiance, urgence)

Interdiction (Chu, généraliste, Modifier, Personnes de confiance, Temporel & Spatial)

Interdiction (Chu, généraliste, Supprimer, Identification, urgence)

Interdiction (Chu, généraliste, Supprimer, Identification, Temporel & Spatial)

Interdiction (Chu, généraliste, Supprimer, Rencontre, urgence)

Interdiction (Chu, généraliste, Supprimer, Rencontre, Temporel & Spatial)

Interdiction (Chu, généraliste, Supprimer, Historique, Temporel & Spatial)

Interdiction (Chu, généraliste, Supprimer, Historique, urgence)

Interdiction (Chu, généraliste, Supprimer, Résultats d'examens biologiques, urgence)

Interdiction (Chu, généraliste, Supprimer, Résultats d'examens biologiques, Temporel & Spatial)

Interdiction (Chu, généraliste, Supprimer, Imagerie, Temporel & Spatial)

Interdiction (Chu, généraliste, Supprimer, Imagerie, urgence)

Interdiction (Chu, généraliste, Supprimer, Le dossier d'anesthésie, Temporel & Spatial)

Interdiction (Chu, généraliste, Supprimer, Le dossier d'anesthésie, urgence)

Interdiction (Chu, généraliste, Supprimer, Le compte rendu opératoire ou d'accouchement, urgence)

Interdiction (Chu, généraliste, Supprimer, Le compte rendu opératoire ou d'accouchement, Temporel & Spatial)

Interdiction (Chu, généraliste, Supprimer, Personnes de confiance, urgence)

Interdiction (Chu, généraliste, Supprimer, Personnes de confiance, Temporel & Spatial)

Interdiction (Chu, généraliste, Transférer, Informations techniques, Temporel & Spatial)

Interdiction (Chu, généraliste, Transférer, Informations techniques, urgence)

Interdiction (Chu, généraliste, ajouter, Personnes de confiance, urgence)

Interdiction (Chu, généraliste, ajouter, Personnes de confiance, Temporel & Spatial)

Interdiction (Chu, généraliste, ajouter, Le dossier d'anesthésie, Temporel & Spatial)

Interdiction (Chu, généraliste, ajouter, Le dossier d'anesthésie, urgence)

Interdiction (Chu, Secrétaire médicale, Modifier, Rencontre, Temporel & Spatial)

Interdiction (Chu, Secrétaire médicale, Modifier, Rencontre, urgence)

Interdiction (Chu, Secrétaire médicale, Modifier, Historique, Temporel & Spatial)

Interdiction (Chu, Secrétaire médicale, Modifier, Historique, urgence)

Interdiction (Chu, Secrétaire médicale, Modifier, Résultats d'examens biologiques, Temporel & Spatial)

Interdiction (Chu, Secrétaire médicale, Modifier, Résultats d'examens biologiques, urgence)

Interdiction (Chu, Secrétaire médicale, Modifier, Les données de soins, Temporel & Spatial)

Interdiction (Chu, Secrétaire médicale, Modifier, Les données de soins, urgence)

Interdiction (Chu, Secrétaire médicale, Modifier, Imagerie, Temporel & Spatial)

Interdiction (Chu, Secrétaire médicale, Modifier, Imagerie, urgence)

Interdiction (Chu, Secrétaire médicale, Modifier, Le dossier d'anesthésie, Temporel & Spatial)

Interdiction (Chu, Secrétaire médicale, Modifier, Le dossier d'anesthésie, urgence)

Interdiction (Chu, Secrétaire médicale, Modifier, Le compte rendu opératoire ou d'accouchement, Temporel & Spatial)

Interdiction (Chu, Secrétaire médicale, Modifier, Le compte rendu opératoire ou d'accouchement, urgence)

Interdiction (Chu, Secrétaire médicale, Modifier, Lettre de sortie, Temporel & Spatial)

Interdiction (Chu, Secrétaire médicale, Modifier, Lettre de sortie, urgence)

Interdiction (Chu, Secrétaire médicale, Modifier, Les correspondances échangées entre professionnels de santé, Temporel & Spatial)

Interdiction (Chu, Secrétaire médicale, Modifier, Les correspondances échangées entre professionnels de santé, urgence)

Interdiction (Chu, Secrétaire médicale, Modifier, Don d'organes, Temporel & Spatial)

Interdiction (Chu, Secrétaire médicale, Modifier, Don d'organes, urgence)

Interdiction (Chu, Secrétaire médicale, Modifier, Personnes de confiance, Temporel & Spatial)

Interdiction (Chu, Secrétaire médicale, Modifier, Personnes de confiance, urgence)

Interdiction (Chu, Secrétaire médicale, Supprimer, Identification, Temporel & Spatial)

Interdiction (Chu, Secrétaire médicale, Supprimer, Identification, urgence)

Interdiction (Chu, Secrétaire médicale, Supprimer, Rencontre, Temporel & Spatial)

Interdiction (Chu, Secrétaire médicale, Supprimer, Rencontre, urgence)

Interdiction (Chu, Secrétaire médicale, Supprimer, Historique, Temporel & Spatial)

Interdiction (Chu, Secrétaire médicale, Supprimer, Historique, urgence)

Interdiction (Chu, Secrétaire médicale, Supprimer, Interrogatoire, Temporel & Spatial)

Interdiction (Chu, Secrétaire médicale, Supprimer, Interrogatoire, urgence)

Interdiction (Chu, Secrétaire médicale, Supprimer, Résultats d'examens biologiques, Temporel & Spatial)

Interdiction (Chu, Secrétaire médicale, Supprimer, Résultats d'examens biologiques, urgence)

Interdiction (Chu, Secrétaire médicale, Supprimer, Les données de soins, Temporel & Spatial)

Interdiction (Chu, Secrétaire médicale, Supprimer, Les données de soins, urgence)

Interdiction (Chu, Secrétaire médicale, Supprimer, Imagerie, Temporel & Spatial)

Interdiction (Chu, Secrétaire médicale, Supprimer, Imagerie, urgence)

Interdiction (Chu, Secrétaire médicale, Supprimer, Le dossier d'anesthésie, Temporel & Spatial)

Interdiction (Chu, Secrétaire médicale, Supprimer, Le dossier d'anesthésie, urgence)

Interdiction (Chu, Secrétaire médicale, Supprimer, Le compte rendu opératoire ou d'accouchement, Temporel & Spatial)

Interdiction (Chu, Secrétaire médicale, Supprimer, Le compte rendu opératoire ou d'accouchement, urgence)

Interdiction (Chu, Secrétaire médicale, Supprimer, Lettre de sortie, Temporel & Spatial)

Interdiction (Chu, Secrétaire médicale, Supprimer, Lettre de sortie, urgence)

Interdiction (Chu, Secrétaire médicale, Supprimer, Les correspondances échangées entre professionnels de santé, Temporel & Spatial)

Interdiction (Chu, Secrétaire médicale, Supprimer, Les correspondances échangées entre professionnels de santé, urgence)

Interdiction (Chu, Secrétaire médicale, Supprimer, Don d'organes, Temporel & Spatial)

Interdiction (Chu, Secrétaire médicale, Supprimer, Don d'organes, urgence)

Interdiction (Chu, Secrétaire médicale, Supprimer, Personnes de confiance, Temporel & Spatial)

Interdiction (Chu, Secrétaire médicale, Supprimer, Personnes de confiance, urgence)

Interdiction (Chu, Secrétaire médicale, Transférer, Rencontre, Temporel & Spatial)

Interdiction (Chu, Secrétaire médicale, Transférer, Rencontre, urgence)

Interdiction (Chu, Secrétaire médicale, Transférer, Interrogatoire, Temporel & Spatial)

Interdiction (Chu, Secrétaire médicale, Transférer, Interrogatoire, urgence)

Interdiction (Chu, Secrétaire médicale, Transférer, Résultats d’examens biologiques, Temporel & Spatial)

Interdiction (Chu, Secrétaire médicale, Transférer, Résultats d’examens biologiques, urgence)

Interdiction (Chu, Secrétaire médicale, Transférer, Les données de soins, Temporel & Spatial)

Interdiction (Chu, Secrétaire médicale, Transférer, Les données de soins, urgence)

Interdiction (Chu, Secrétaire médicale, Transférer, Le dossier d'anesthésie, Temporel & Spatial)

Interdiction (Chu, Secrétaire médicale, Transférer, Le dossier d'anesthésie, urgence)

Interdiction (Chu, Secrétaire médicale, Transférer, Le compte rendu opératoire ou d’accouchement, Temporel & Spatial)

Interdiction (Chu, Secrétaire médicale, Transférer, Le compte rendu opératoire ou d’accouchement, urgence)

Interdiction (Chu, Secrétaire médicale, Transférer, Don d’organes, Temporel & Spatial)

Interdiction (Chu, Secrétaire médicale, Transférer, Don d’organes, urgence)

Interdiction (Chu, Secrétaire médicale, Transférer, Historique, Temporel & Spatial)

Interdiction (Chu, Secrétaire médicale, Transférer, Historique, urgence)

Interdiction (Chu, Secrétaire médicale, Transférer, Personnes de confiance, Temporel & Spatial)

Interdiction (Chu, Secrétaire médicale, Transférer, Personnes de confiance, urgence)

Interdiction (Chu, Secrétaire médicale, ajouter, Rencontre, Temporel & Spatial)

Interdiction (Chu, Secrétaire médicale, ajouter, Rencontre, urgence)

Interdiction (Chu, Secrétaire médicale, ajouter, Interrogatoire, Temporel & Spatial)

Interdiction (Chu, Secrétaire médicale, Ajouter, Interrogatoire, urgence)

Interdiction (Chu, Secrétaire médicale, Ajouter, Résultats d’examens biologiques, Temporel & Spatial)

Interdiction (Chu, Secrétaire médicale, Ajouter, Résultats d’examens biologiques, urgence)

Interdiction (Chu, Secrétaire médicale, Ajouter, Les données de soins, Temporel & Spatial)

Interdiction (Chu, Secrétaire médicale, Ajouter, Les données de soins, urgence)

Interdiction (Chu, Secrétaire médicale, Ajouter, Imagerie, Temporel & Spatial)

Interdiction (Chu, Secrétaire médicale, Ajouter, Imagerie, urgence)

Interdiction (Chu, Secrétaire médicale, Ajouter, Le dossier d'anesthésie, Temporel & Spatial)

Interdiction (Chu, Secrétaire médicale, Ajouter, Le dossier d'anesthésie, urgence)

Interdiction (Chu, Secrétaire médicale, Ajouter, Le compte rendu opératoire ou d’accouchement, Temporel & Spatial)

Interdiction (Chu, Secrétaire médicale, Ajouter, Le compte rendu opératoire ou d’accouchement, urgence)

Interdiction (Chu, Secrétaire médicale, Ajouter, Lettre de sortie, Temporel & Spatial)

Interdiction (Chu, Secrétaire médicale, Ajouter, Lettre de sortie, urgence)

Interdiction (Chu, Secrétaire médicale, Ajouter, Les correspondances échangées entre professionnels de santé, Temporel & Spatial)

Interdiction (Chu, Secrétaire médicale, Ajouter, Les correspondances échangées entre professionnels de santé, urgence)

Interdiction (Chu, Secrétaire médicale, Ajouter, Historique, Temporel & Spatial)

Interdiction (Chu, Secrétaire médicale, Ajouter, Historique, urgence)

Interdiction (CHU, Secrétaire médicale, consulter, Identification, Spatial)

Interdiction (Chu, Secrétaire médicale, consulter, Rencontre, Temporel & Spatial)

Interdiction (Chu, Secrétaire médicale, consulter, Rencontre, urgence)

Interdiction (Chu, Secrétaire médicale, consulter, Informations techniques, Temporel & Spatial)

Interdiction (Chu, Secrétaire médicale, consulter, Interrogatoire, Temporel & Spatial)

Interdiction (Chu, Secrétaire médicale, consulter, Interrogatoire, urgence)

Interdiction (Chu, Secrétaire médicale, consulter, Résultats d'examens biologiques, Temporel & Spatial)

Interdiction (Chu, Secrétaire médicale, consulter, Résultats d'examens biologiques, urgence)

Interdiction (Chu, Secrétaire médicale, consulter, Les données de soins, Temporel & Spatial)

Interdiction (Chu, Secrétaire médicale, consulter, Les données de soins, urgence)

Interdiction (Chu, Secrétaire médicale, consulter, Imagerie, Temporel & Spatial)

Interdiction (Chu, Secrétaire médicale, consulter, Imagerie, urgence)

Interdiction (Chu, Secrétaire médicale, consulter, Le dossier d'anesthésie, Temporel & Spatial)

Interdiction (Chu, Secrétaire médicale, consulter, Le dossier d'anesthésie, urgence)

Interdiction (Chu, Secrétaire médicale, consulter, Le compte rendu opératoire ou d'accouchement, Temporel & Spatial)

Interdiction (Chu, Secrétaire médicale, consulter, Le compte rendu opératoire ou d'accouchement, urgence)

Interdiction (Chu, Secrétaire médicale, consulter, Lettre de sortie, Temporel & Spatial)

Interdiction (Chu, Secrétaire médicale, consulter, Lettre de sortie, urgence)

Interdiction (Chu, Secrétaire médicale, consulter, Historique, Temporel & Spatial)

Interdiction (Chu, Secrétaire médicale, consulter, Historique, urgence)

Interdiction (Chu, Secrétaire médicale, consulter, Personnes de confiance, Temporel & Spatial)

Interdiction (Chu, Secrétaire médicale, consulter, Personnes de confiance, urgence)

Interdiction (CHU, Pharmacien, consulter, Identification, Spatial)

Interdiction (CHU, Pharmacien, consulter, Les données de soins, Spatial)

Interdiction (Chu, Pharmacien, consulter, Historique, Temporel & Spatial)

Interdiction (Chu, Pharmacien, consulter, Historique, urgence)

Interdiction (Chu, Pharmacien, consulter, Personnes de confiance, Temporel & Spatial)

Interdiction (Chu, Pharmacien, consulter, Personnes de confiance, urgence)

Interdiction (Chu, Pharmacien, consulter, Rencontre, Temporel & Spatial)

Interdiction (Chu, Pharmacien, consulter, Rencontre, urgence)

Interdiction (CHU, Pharmacien, consulter, Informations techniques, urgence)

Interdiction (Chu, Pharmacien, consulter, Informations techniques, Temporel & Spatial)

Interdiction (Chu, Pharmacien, consulter, Interrogatoire, Temporel & Spatial)

Interdiction (Chu, Pharmacien, consulter, Interrogatoire, urgence)

Interdiction (Chu, Pharmacien, consulter, Résultats d'examens biologiques, Temporel & Spatial)

Interdiction (Chu, Pharmacien, consulter, Résultats d'examens biologiques, urgence)

Interdiction (Chu, Pharmacien, consulter, Imagerie, Temporel & Spatial)

Interdiction (Chu, Pharmacien, consulter, Imagerie, urgence)

Interdiction (Chu, Pharmacien, consulter, Le dossier d'anesthésie, Temporel & Spatial)

Interdiction (Chu, Pharmacien, consulter, Le dossier d'anesthésie, urgence)

Interdiction (Chu, Pharmacien, consulter, Le compte rendu opératoire ou d'accouchement, Temporel & Spatial)

Interdiction (Chu, Pharmacien, consulter, Le compte rendu opératoire ou d'accouchement, urgence)

Interdiction (Chu, Pharmacien, consulter, Lettre de sortie, Temporel & Spatial)

Interdiction (Chu, Pharmacien, consulter, Lettre de sortie, urgence)

Interdiction (CHU, Pharmacien, Modifier, Identification, urgence)

Interdiction (CHU, Pharmacien, Modifier, Identification, temporel)

Interdiction (CHU, Pharmacien, consulter, Identification, Spatial)

Interdiction (CHU, Pharmacien, Modifier, Les données de soins, urgence)

Interdiction (CHU, Pharmacien, Modifier, Les données de soins, temporel)

Interdiction (CHU, Pharmacien, Modifier, Les données de soins, Spatial)

Interdiction (Chu, Pharmacien, Modifier, Historique, Temporel & Spatial)

Interdiction (Chu, Pharmacien, Modifier, Historique, urgence)

Interdiction (Chu, Pharmacien, Modifier, Personnes de confiance, Temporel & Spatial)

Interdiction (Chu, Pharmacien, Modifier, Personnes de confiance, urgence)

Interdiction (Chu, Pharmacien, Modifier, Rencontre, Temporel & Spatial)

Interdiction (Chu, Pharmacien, Modifier, Rencontre, urgence)

Interdiction (CHU, Pharmacien, Modifier, Informations techniques, urgence)

Interdiction (Chu, Pharmacien, Modifier, Informations techniques, Temporel & Spatial)

Interdiction (Chu, Pharmacien, Modifier, Interrogatoire, Temporel & Spatial)

Interdiction (Chu, Pharmacien, Modifier, Interrogatoire, urgence)

Interdiction (Chu, Pharmacien, Modifier, Résultats d'examens biologiques, Temporel & Spatial)

Interdiction (Chu, Pharmacien, Modifier, Résultats d'examens biologiques, urgence)

Interdiction (Chu, Pharmacien, Modifier, Imagerie, Temporel & Spatial)

Interdiction (Chu, Pharmacien, Modifier, Imagerie, urgence)

Interdiction (Chu, Pharmacien, Modifier, Le dossier d'anesthésie, Temporel & Spatial)

Interdiction (Chu, Pharmacien, Modifier, Le dossier d'anesthésie, urgence)

Interdiction (Chu, Pharmacien, Modifier, Le compte rendu opératoire ou d'accouchement, Temporel & Spatial)

Interdiction (Chu, Pharmacien, Modifier, Le compte rendu opératoire ou d'accouchement, urgence)

Interdiction (Chu, Pharmacien, Modifier, Lettre de sortie, Temporel & Spatial)

Interdiction (Chu, Pharmacien, Modifier, Lettre de sortie, urgence)

Interdiction (Chu, Kinésithérapie, consulter, Rencontre, Temporel & Spatial)

Interdiction (Chu, Kinésithérapie, consulter, Rencontre, urgence)

Interdiction (Chu, Kinésithérapie, consulter, Informations techniques, urgence)

Interdiction (Chu, Kinésithérapie, consulter, Informations techniques, Temporel & Spatial)

Interdiction (Chu, Kinésithérapie, consulter, Personnes de confiance, Temporel & Spatial)

Interdiction (Chu, Kinésithérapie, consulter, Personnes de confiance, urgence)

Interdiction (Chu, Kinésithérapie, consulter, Les correspondances échangées entre professionnels de santé, Temporel & Spatial)

Interdiction (Chu, Kinésithérapie, consulter, Les correspondances échangées entre professionnels de santé, urgence)

Interdiction (Chu, Kinésithérapie, consulter, Historique, Temporel & Spatial)

Interdiction (Chu, Kinésithérapie, consulter, Historique, urgence)

Interdiction (Chu, Kinésithérapie, consulter, Don d'organes, urgence)

Interdiction (Chu, Kinésithérapie, consulter, Don d'organes, Temporel & Spatial)

Interdiction (Chu, Kinésithérapie, consulter, Personnes de confiance, Temporel & Spatial)

Interdiction (Chu, Kinésithérapie, consulter, Personnes de confiance, urgence)

Interdiction (Chu, Kinésithérapie, consulter, Résultats d'examens biologiques, urgence)

Interdiction (Chu, Kinésithérapie, consulter, Résultats d'examens biologiques, Temporel & Spatial)

Interdiction (CHU, Infirmiers, consulter, Identification, Spatial)

Interdiction (CHU, Infirmiers, consulter, Rencontre, Spatial & Temporel)

Interdiction (CHU, Infirmiers, consulter, Informations techniques, urgence)

Interdiction (CHU, Infirmiers, consulter, Informations techniques, Temporel & Spatial)

Interdiction (CHU, Infirmiers, consulter, Interrogatoire, Temporel & Spatial)

Interdiction (CHU, Infirmiers, consulter, Interrogatoire, urgence)

Interdiction (CHU, Infirmiers, consulter, Résultats d'examens biologiques, Temporel & Spatial)

Interdiction (CHU, Infirmiers, consulter, Résultats d'examens biologiques, urgence)

Interdiction (CHU, Infirmiers, consulter, Imagerie, urgence)

Interdiction (CHU, Infirmiers, consulter, Imagerie, Temporel & Spatial)

Interdiction (CHU, Infirmiers, consulter, Le dossier d'anesthésie, Temporel & Spatial)

Interdiction (CHU, Infirmiers, consulter, Le dossier d'anesthésie, urgence)

Interdiction (CHU, Infirmiers, consulter, Historique, Temporel & Spatial)

Interdiction (CHU, Infirmiers, consulter, Historique, urgence)

Interdiction (CHU, Infirmiers, consulter, Le compte rendu opératoire ou d'accouchement, urgence)

Interdiction (CHU, Infirmiers, consulter, Le compte rendu opératoire ou d'accouchement, Temporel & Spatial)

Interdiction (CHU, Infirmiers, consulter, Lettre de sortie, Temporel & Spatial)

Interdiction (CHU, Infirmiers, consulter, Lettre de sortie, urgence)

Interdiction (CHU, Infirmiers, consulter, Les correspondances échangées entre professionnels de santé, Temporel & Spatial)

Interdiction (CHU, Infirmiers, consulter, Les correspondances échangées entre professionnels de santé, urgence)

Interdiction (CHU, Infirmiers, consulter, Don d'organes, Temporel & Spatial)

Interdiction (CHU, Infirmiers, consulter, Don d'organes, urgence)

Interdiction (CHU, Infirmiers, consulter, Personnes de confiance, urgence)

Interdiction (CHU, Infirmiers, consulter, Personnes de confiance, Temporel & Spatial)

Permission (Chu, Professeur, Modifier, Rencontre, Temporel)

Permission (Chu, Professeur, Modifier, Rencontre, Spatial)

Permission (Chu, Médecin Chef, Modifier, Rencontre, Temporel & Spatial)

Permission (Chu, spécialiste, Modifier, Rencontre, Temporel & Spatial)

Permission (Chu, résidents, Modifier, Rencontre, Temporel & Spatial)

Permission (Chu, généraliste, Modifier, Rencontre, Temporel & Spatial)

Permission (Chu, Professeur, Modifier, Rencontre, urgence)

Permission (Chu, Médecin Chef, Modifier, Rencontre, urgence)

Permission (Chu, spécialiste, Modifier, Rencontre, urgence)

Permission (Chu, généraliste, Modifier, Rencontre, urgence)

Permission (Chu, Secrétaire médicale, Modifier, Identification, Temporel & Spatial)

Permission (Chu, Secrétaire médicale, Modifier, Identification, urgence)

Permission (Chu, Secrétaire médicale, Modifier, Informations techniques, Temporel & Spatial)

Permission (Chu, Secrétaire médicale, Modifier, Informations techniques, urgence)

Permission (Chu, Professeur, Modifier, Lettre de sortie, Temporel & Spatial)

Permission (Chu, M.C.A, Modifier, Lettre de sortie, Temporel & Spatial)

Permission (Chu, M.C.B, Modifier, Lettre de sortie, Temporel & Spatial)

Permission (Chu, Médecin Chef, Modifier, Lettre de sortie, Temporel & Spatial)

Permission (Chu, spécialiste, Modifier, Lettre de sortie, Temporel & Spatial)

Permission (Chu, généraliste, Modifier, Lettre de sortie, Temporel & Spatial)

Permission (Chu, Professeur, Modifier, Lettre de sortie, urgence)

Permission (Chu, Médecin Chef, Modifier, Lettre de sortie, urgence)

Permission (Chu, spécialiste, Modifier, Lettre de sortie, urgence)

Permission (Chu, généraliste, Modifier, Lettre de sortie, urgence)

Permission (Chu, Professeur, Supprimer, Personnes de confiance, Temporel & Spatial)

Permission (Chu, Médecin Chef, Supprimer, Personnes de confiance, Temporel & Spatial)

Permission (Chu, spécialiste, Supprimer, Personnes de confiance, Temporel & Spatial)

Permission (Chu, généraliste, Supprimer, Personnes de confiance, Temporel & Spatial)

Permission (Chu, Professeur, Supprimer, Personnes de confiance, urgence)

Permission (Chu, Médecin Chef, Supprimer, Personnes de confiance, urgence)

Permission (Chu, spécialiste, Supprimer, Personnes de confiance, urgence)

Permission (Chu, généraliste, Supprimer, Personnes de confiance, urgence)

Permission (Chu, Secrétaire médicale, Supprimer, Informations techniques, Temporel & Spatial)

Permission (Chu, Secrétaire médicale, Supprimer, Informations techniques, urgence)

Permission (Chu, Professeur, Transférer, Identification, Temporel & Spatial)

Permission (Chu, Médecin Chef, Transférer, Identification, Temporel & Spatial)

Permission (Chu, spécialiste, Transférer, Identification, Temporel & Spatial)

Permission (Chu, généraliste, Transférer, Identification, Temporel & Spatial)

Permission (Chu, Secrétaire médicale, Transférer, Identification, Temporel & Spatial)

Permission (Chu, Professeur, Transférer, Identification, urgence)

Permission (Chu, Médecin Chef, Transférer, Identification, urgence)

Permission (Chu, spécialiste, Transférer, Identification, urgence)

Permission (Chu, généraliste, Transférer, Identification, urgence)

Permission (Chu, Secrétaire médicale, Transférer, Identification, urgence)

Permission (Chu, Professeur, Transférer, Rencontre, urgence)

Permission (Chu, Médecin Chef, Transférer, Rencontre, urgence)

Permission (Chu, spécialiste, Transférer, Rencontre, urgence)

Permission (Chu, généraliste, Transférer, Rencontre, urgence)

Permission (Chu, Professeur, Transférer, Rencontre, Temporel & Spatial)

Permission (Chu, Médecin Chef, Transférer, Rencontre, Temporel & Spatial)

Permission (Chu, spécialiste, Transférer, Rencontre, Temporel & Spatial)

Permission (Chu, généraliste, Transférer, Rencontre, Temporel & Spatial)

Permission (Chu, Secrétaire médicale, Transférer, Informations techniques, urgence)

Permission (Chu, Secrétaire médicale, Transférer, Informations techniques, Temporel & Spatial)

Permission (Chu, Professeur, Transférer, Historique, Temporel & Spatial)

Permission (Chu, Médecin Chef, Transférer, Historique, Temporel & Spatial)

Permission (Chu, spécialiste, Transférer, Historique, Temporel & Spatial)

Permission (Chu, généraliste, Transférer, Historique, Temporel & Spatial)

Permission (Chu, Professeur, Transférer, Historique, urgence)

Permission (Chu, Médecin Chef, Transférer, Historique, urgence)

Permission (Chu, spécialiste, Transférer, Historique, urgence)

Permission (Chu, généraliste, Transférer, Historique, urgence)

Permission (Chu, Sage-Femme, Transférer, Historique, Temporel & Spatial)

Permission (Chu, Sage-Femme, Transférer, Historique, urgence)

Permission (Chu, Professeur, Transférer, Interrogatoire, Temporel & Spatial)

Permission (Chu, Médecin Chef, Transférer, Interrogatoire, Temporel & Spatial)

Permission (Chu, spécialiste, Transférer, Interrogatoire, Temporel & Spatial)

Permission (Chu, généraliste, Transférer, Interrogatoire, Temporel & Spatial)

Permission (Chu, Professeur, Transférer, Interrogatoire, urgence)

Permission (Chu, Médecin Chef, Transférer, Interrogatoire, urgence)

Permission (Chu, spécialiste, Transférer, Interrogatoire, urgence)

Permission (Chu, généraliste, Transférer, Interrogatoire, urgence)

Permission (Chu, Sage-Femme, Transférer, Interrogatoire, Temporel & Spatial)

Permission (Chu, Sage-Femme, Transférer, Interrogatoire, urgence)

Permission (Chu, psychologue, Transférer, Interrogatoire, Temporel & Spatial)

Permission (Chu, psychologue, Transférer, Interrogatoire, urgence)

Permission (Chu, Professeur, Transférer, Lettre de sortie, Temporel & Spatial)

Permission (Chu, Médecin Chef, Transférer, Lettre de sortie, Temporel & Spatial)

Permission (Chu, spécialiste, Transférer, Lettre de sortie, Temporel & Spatial)

Permission (Chu, généraliste, Transférer, Lettre de sortie, Temporel & Spatial)

Permission (Chu, Professeur, Transférer, Lettre de sortie, urgence)

Permission (Chu, Médecin Chef, Transférer, Lettre de sortie, urgence)

Permission (Chu, spécialiste, Transférer, Lettre de sortie, urgence)

Permission (Chu, généraliste, Transférer, Lettre de sortie, urgence)

Permission (Chu, Secrétaire médicale, Transférer, Lettre de sortie, Temporel & Spatial)

Permission (Chu, Secrétaire médicale, Transférer, Lettre de sortie, urgence)

Permission (Chu, Professeur, Transférer, Les correspondances échangées entre professionnels de santé, Temporel & Spatial)

Permission (Chu, Médecin Chef, Transférer, Les correspondances échangées entre professionnels de santé, Temporel & Spatial)

Permission (Chu, spécialiste, Transférer, Les correspondances échangées entre professionnels de santé, Temporel & Spatial)

Permission (Chu, généraliste, Transférer, Les correspondances échangées entre professionnels de santé, Temporel & Spatial)

Permission (Chu, Professeur, Transférer, Les correspondances échangées entre professionnels de santé, urgence)

Permission (Chu, Médecin Chef, Transférer, Les correspondances échangées entre professionnels de santé, urgence)

Permission (Chu, spécialiste, Transférer, Les correspondances échangées entre professionnels de santé, urgence)

Permission (Chu, généraliste, Transférer, Les correspondances échangées entre professionnels de santé, urgence)

Permission (Chu, Sage-Femme, Transférer, Les correspondances échangées entre professionnels de santé, Temporel & Spatial)

Permission (Chu, Sage-Femme, Transférer, Les correspondances échangées entre professionnels de santé, urgence)

Permission (Chu, Secrétaire médicale, Transférer, Les correspondances échangées entre professionnels de santé, Temporel & Spatial)

Permission (Chu, Secrétaire médicale, Transférer, Les correspondances échangées entre professionnels de santé, urgence)

Permission (Chu, Professeur, Transférer, Le compte rendu opératoire ou d'accouchement, Temporel & Spatial)

Permission (Chu, Médecin Chef, Transférer, Le compte rendu opératoire ou d'accouchement, Temporel & Spatial)

Permission (Chu, spécialiste, Transférer, Le compte rendu opératoire ou d'accouchement, Temporel & Spatial)

Permission (Chu, résidents, Transférer, Le compte rendu opératoire ou d'accouchement, Temporel & Spatial)

Permission (Chu, généraliste, Transférer, Le compte rendu opératoire ou d'accouchement, Temporel & Spatial)

Permission (Chu, Professeur, Transférer, Le compte rendu opératoire ou d'accouchement, urgence)

Permission (Chu, Médecin Chef, Transférer, Le compte rendu opératoire ou d'accouchement, urgence)

Permission (Chu, spécialiste, Transférer, Le compte rendu opératoire ou d'accouchement, urgence)

Permission (Chu, généraliste, Transférer, Le compte rendu opératoire ou d'accouchement, urgence)

Permission (Chu, Sage-Femme, Transférer, Le compte rendu opératoire ou d'accouchement, Temporel & Spatial)

Permission (Chu, Sage-Femme, Transférer, Le compte rendu opératoire ou d'accouchement, urgence)

Permission (Chu, Professeur, Transférer, Résultats d'examens biologiques, Temporel & Spatial)

Permission (Chu, M.C.A, Transférer, Résultats d'examens biologiques, Temporel & Spatial)

Permission (Chu, M.C.B, Transférer, Résultats d'examens biologiques, Temporel & Spatial)

Permission (Chu, Professeur, Transférer, Résultats d'examens biologiques, urgence)

Permission (Chu, Médecin Chef, Transférer, Résultats d'examens biologiques, urgence)

Permission (Chu, spécialiste, Transférer, Résultats d'examens biologiques, urgence)

Permission (Chu, résidents, Transférer, Résultats d'examens biologiques, urgence)

Permission (Chu, généraliste, Transférer, Résultats d'examens biologiques, urgence)

Permission (Chu, Laborantin, Transférer, Résultats d'examens biologiques, urgence)

Permission (Chu, Professeur, Transférer, Personnes de confiance, Temporel & Spatial)

Permission (Chu, Médecin Chef, Transférer, Personnes de confiance, Temporel & Spatial)

Permission (Chu, spécialiste, Transférer, Personnes de confiance, Temporel & Spatial)

Annexe (B) : Les interfaces principales de l'application DMP-Doc

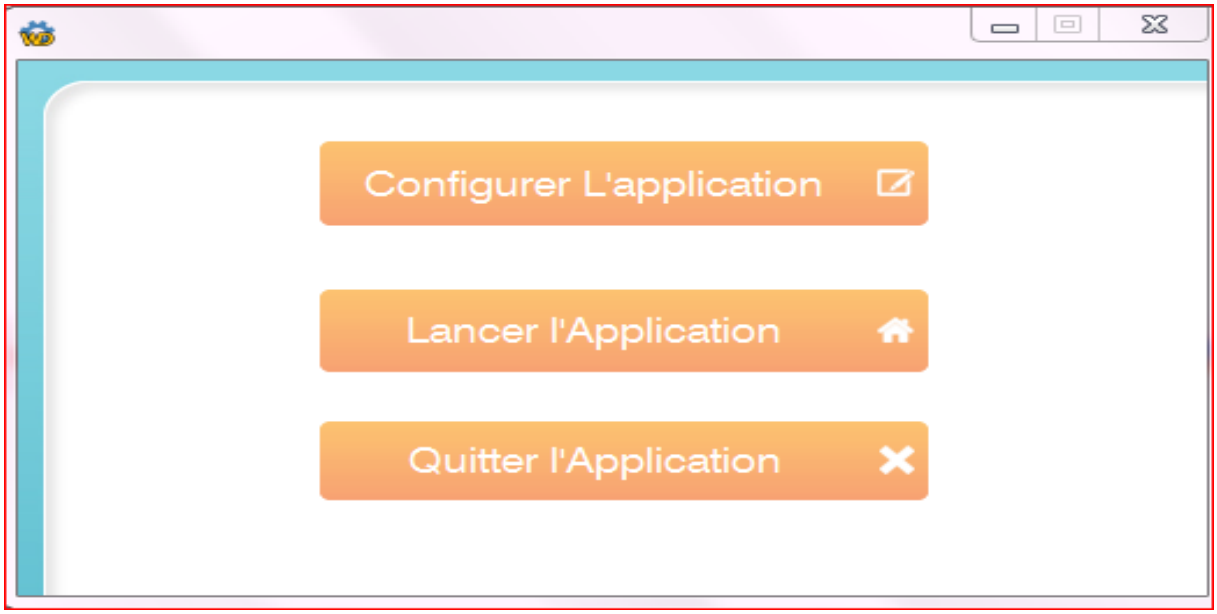

Figure : Interface Principale de DMP-Doc.

- L'interface principale ou bien l'interface d'accès : avec trois champs d'accès :
  - Le premier champ c'est pour l'administrateur général qu'il a le droit pour configurer l'application.
  - Le deuxième champ pour les personnels médicaux.
  - Et le dernier champ pour quitter l'application.
- Quand l'administrateur général accède à son espace, il doit saisir son Login et Mot de passe pour confirmer son identité :

Figure : Authentification de l'Admin.

- Une fois l'identité est confirmée, l'administrateur accède à la page d'administrateur.

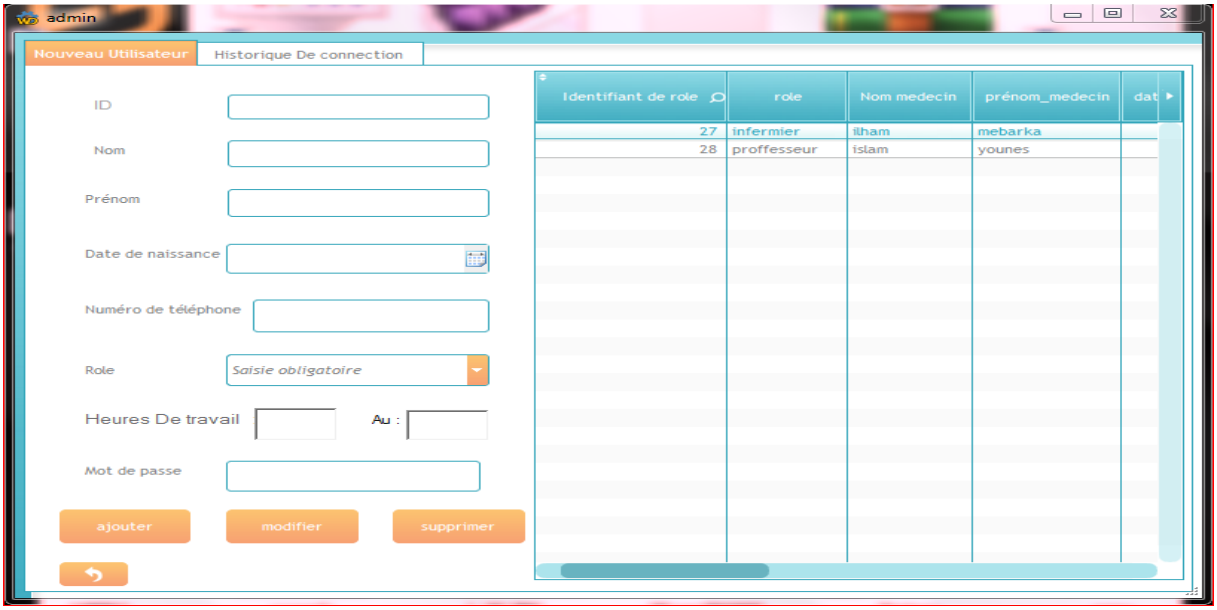

Figure : La page d'administrateur.

- Le rôle principal de l'administrateur général est la gestion des utilisateurs (médecin, professeur, infirmière, etc.), c'est à dire il a le droit d'ajouter un nouveau-utilisateur et de lui fournir un mot de passe pour qu'il puisse accéder à l'application. Ainsi l'administrateur général a le droit de modifier ou supprimer un utilisateur déjà créé.

- Le champ d'administrateur contient deux parties : une pour la gestion des utilisateurs, et l'autre pour consulter l'historique d'activités des utilisateurs en cas d'urgence.

- Lorsqu'un utilisateur lance l'application il doit saisir son login et mot de passe pour confirmer l'identité.

- Hors les horaires de travail, s'il accède à son espace, un message d'erreur va apparaitre, il signale que le contexte temporel est invalide, l'utilisateur doit citer le cas d'urgence qui va être enregistré chez l'administrateur général, sinon le system refus l'accès de l'utilisateur à l'application.

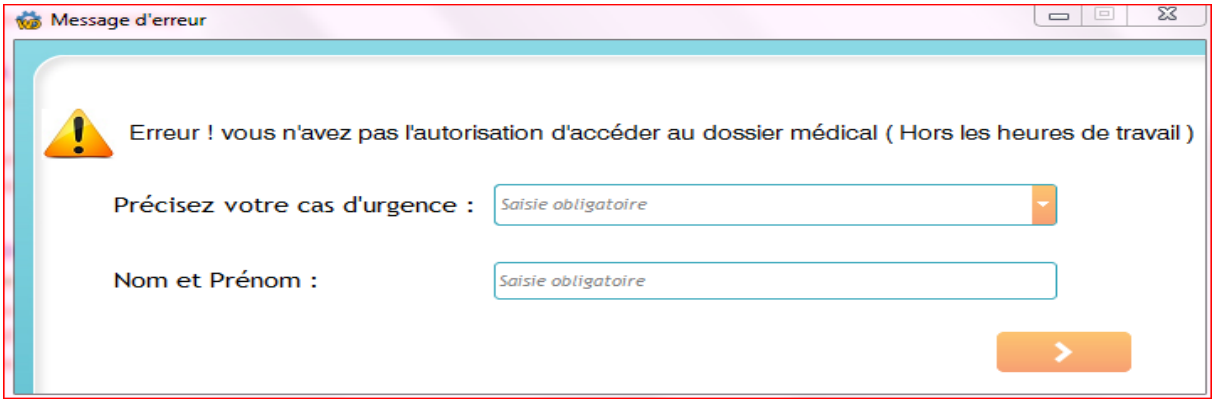

Figure : Message d'erreur.

- Dans **DMP-Doc** ; Le dossier médical est un ensemble des vues. Chaque vue contient des différent fonctionnalités.

- Selon le contexte (temporel ou urgence) et le rôle de chaque utilisateur, **DMP-Doc** donne l'accès ou le refus aux données des patients.

- Dans ce qui suit, nous allons présenter les IHM des fonctionnalités que le **DMP-Doc** offre.

Figure : Vue -Liste des patients-

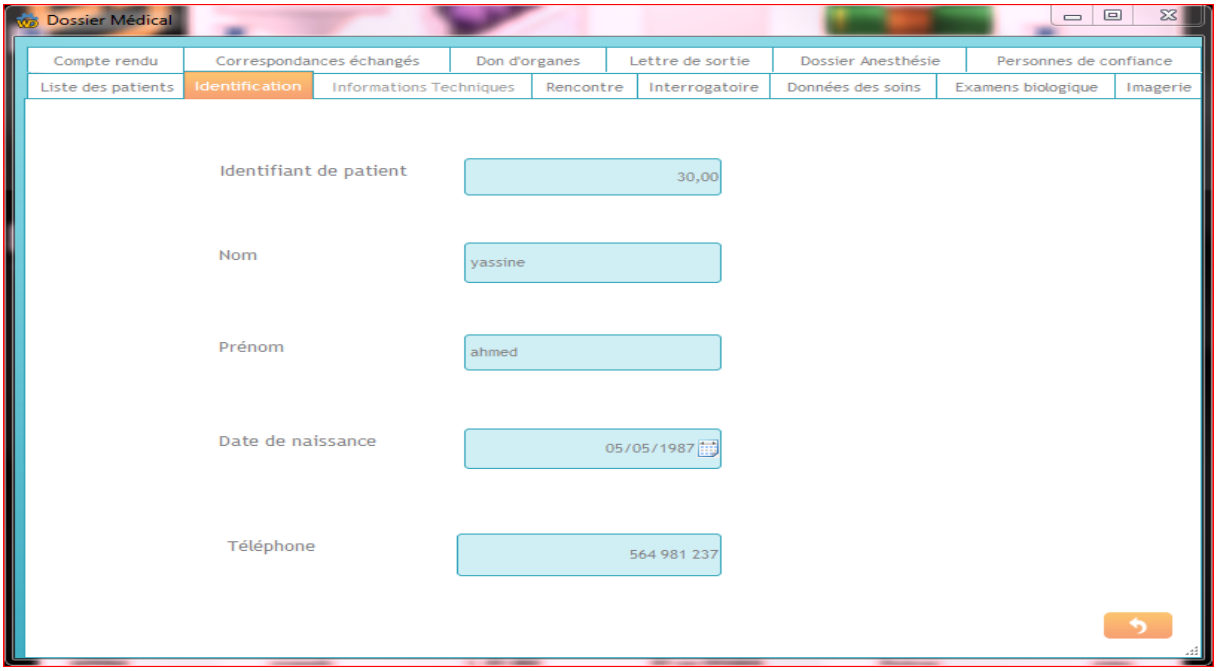

Figure : Vue –Identification-

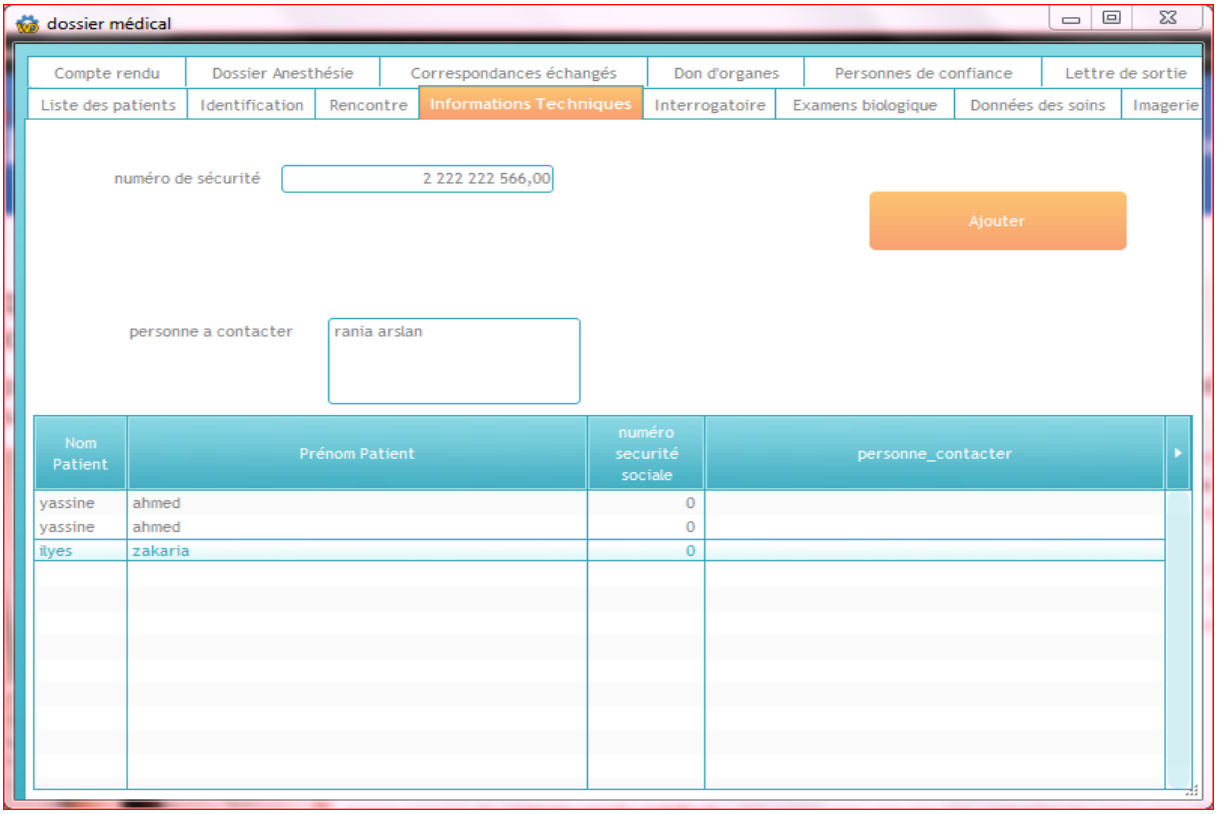

Figure : Vue -Informations techniques-

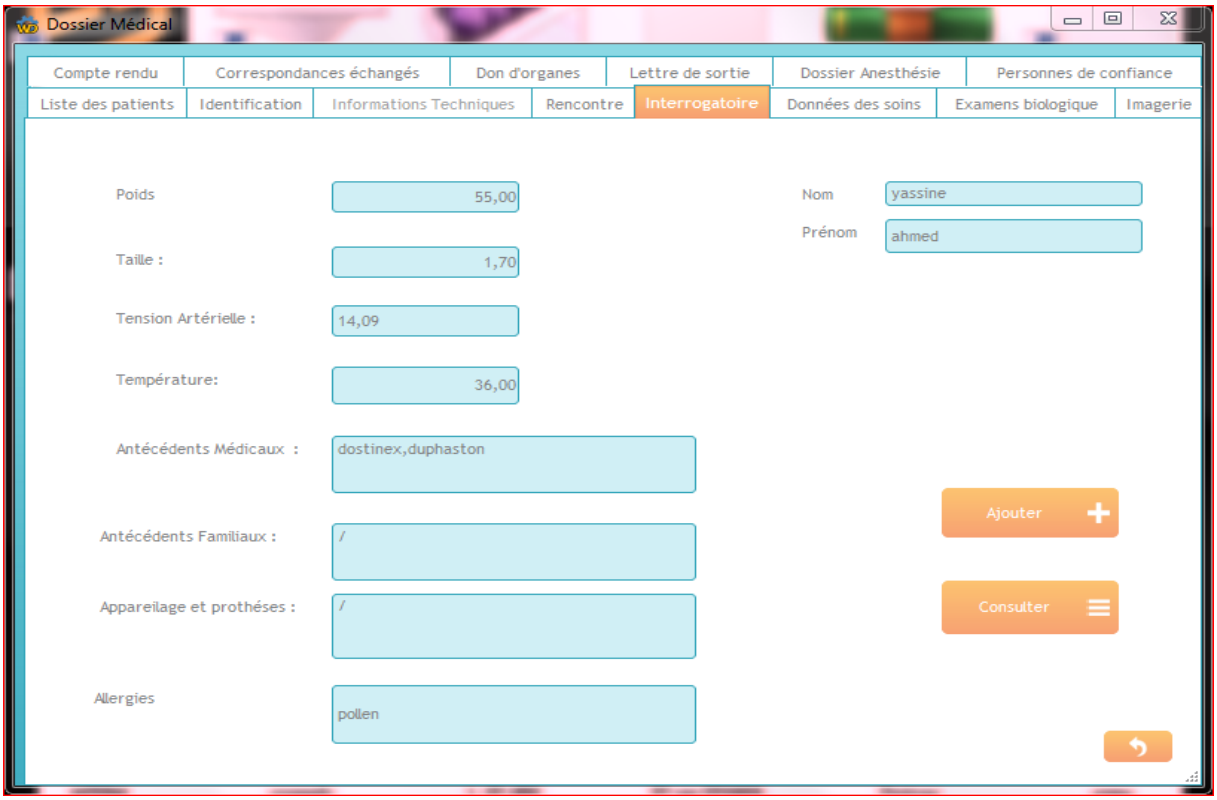

Figure : Vue -interrogatoire-

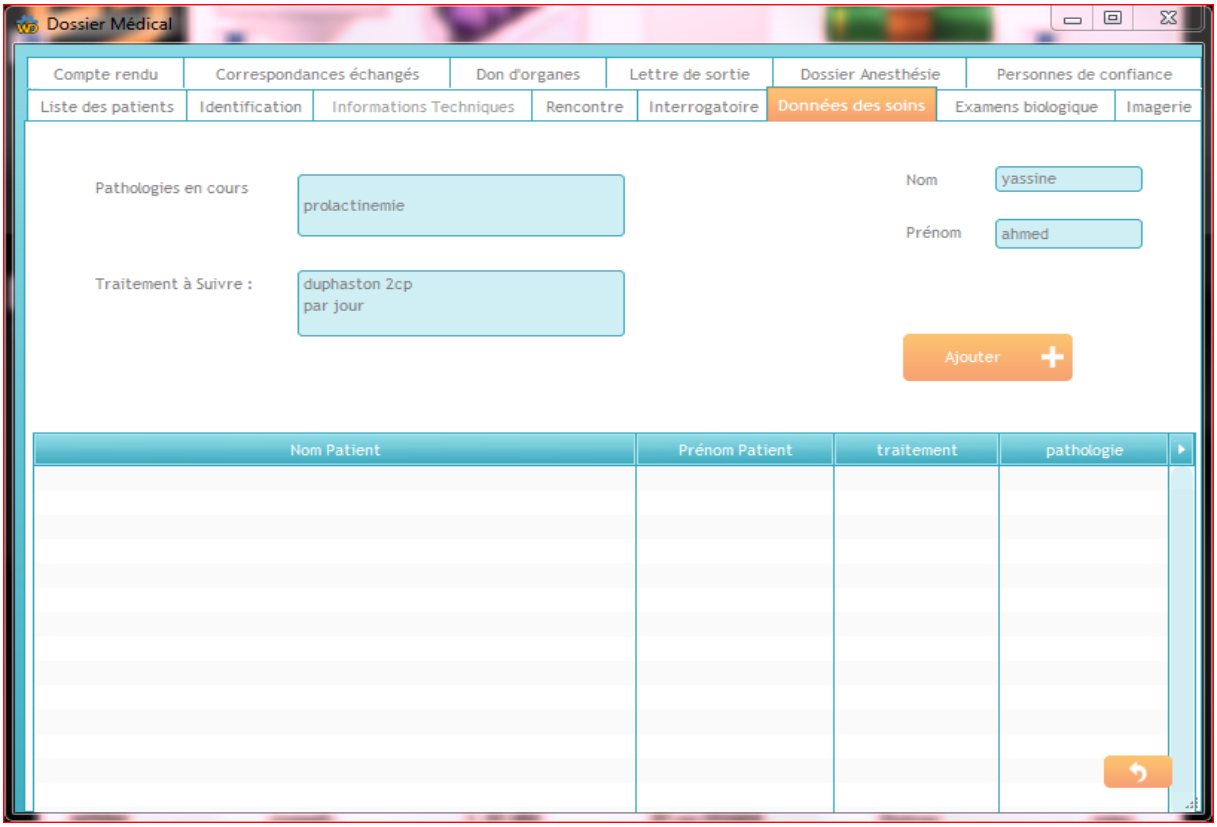

Figure : Vue - Données des soins-

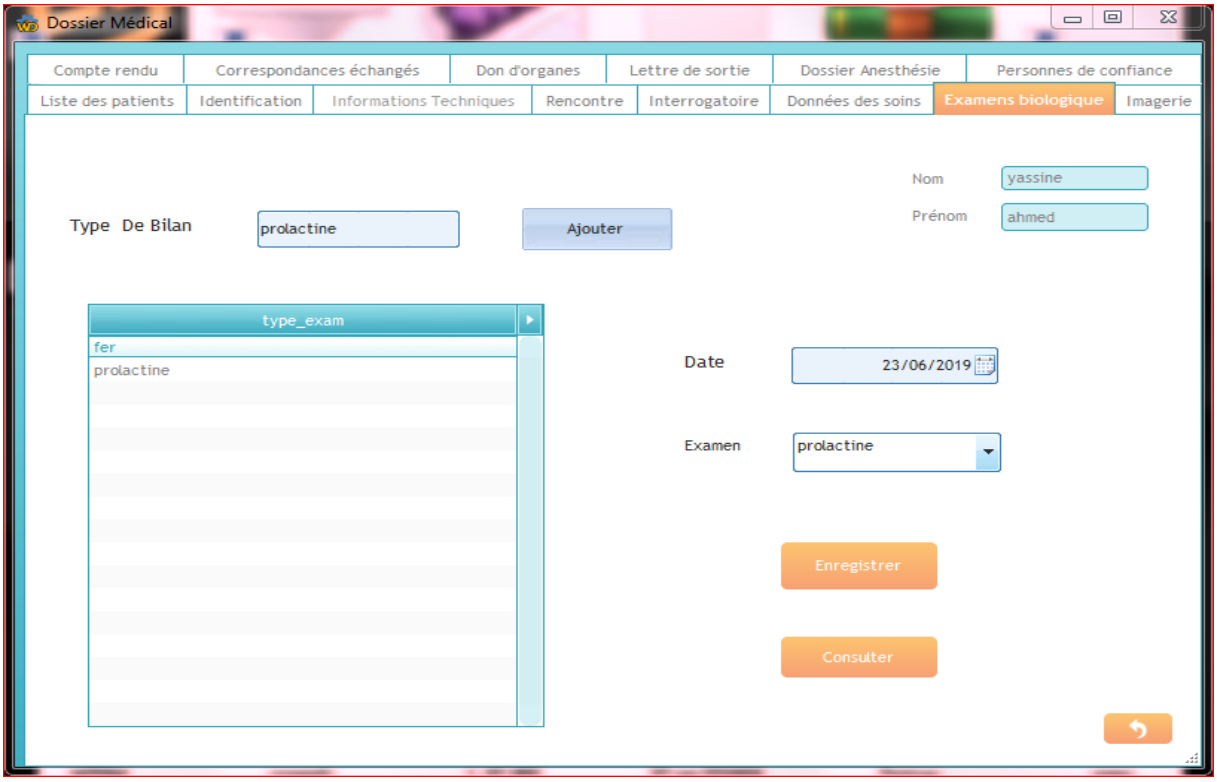

Figure : Vue -examens biologique-

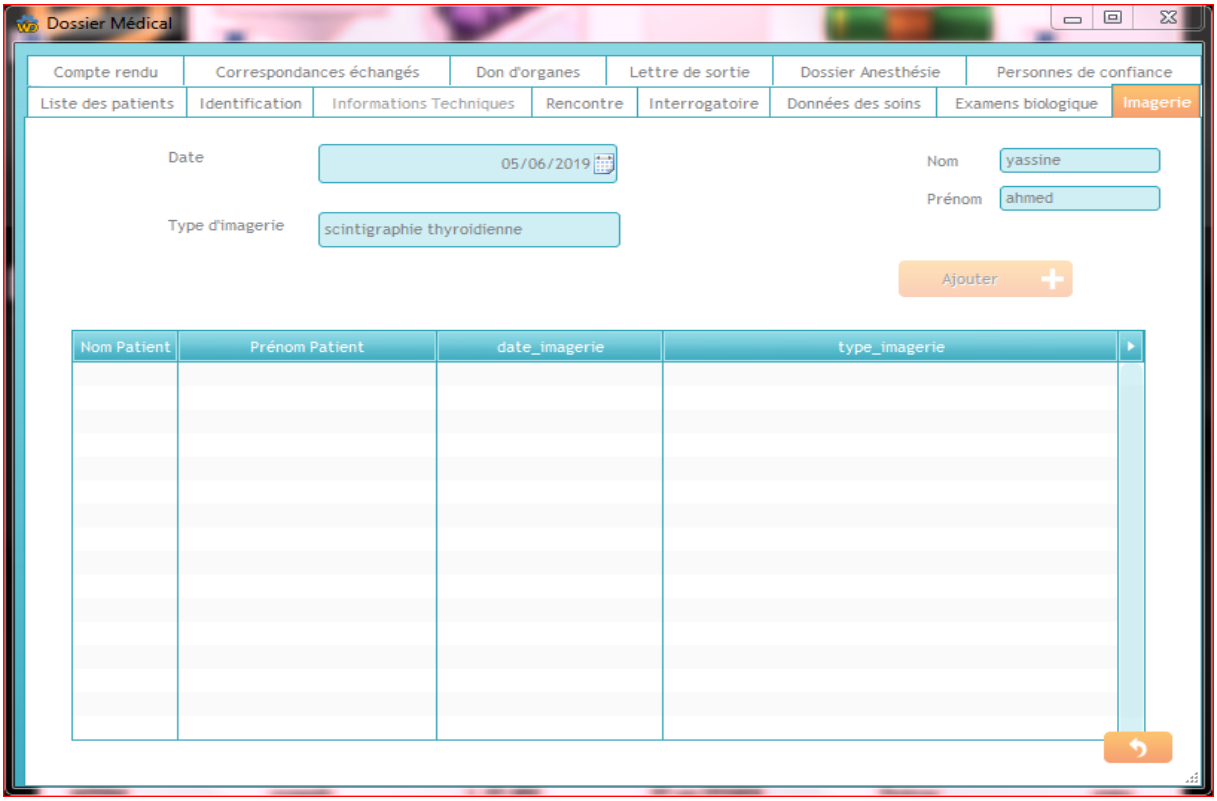

Figure : Vue -imagerie –

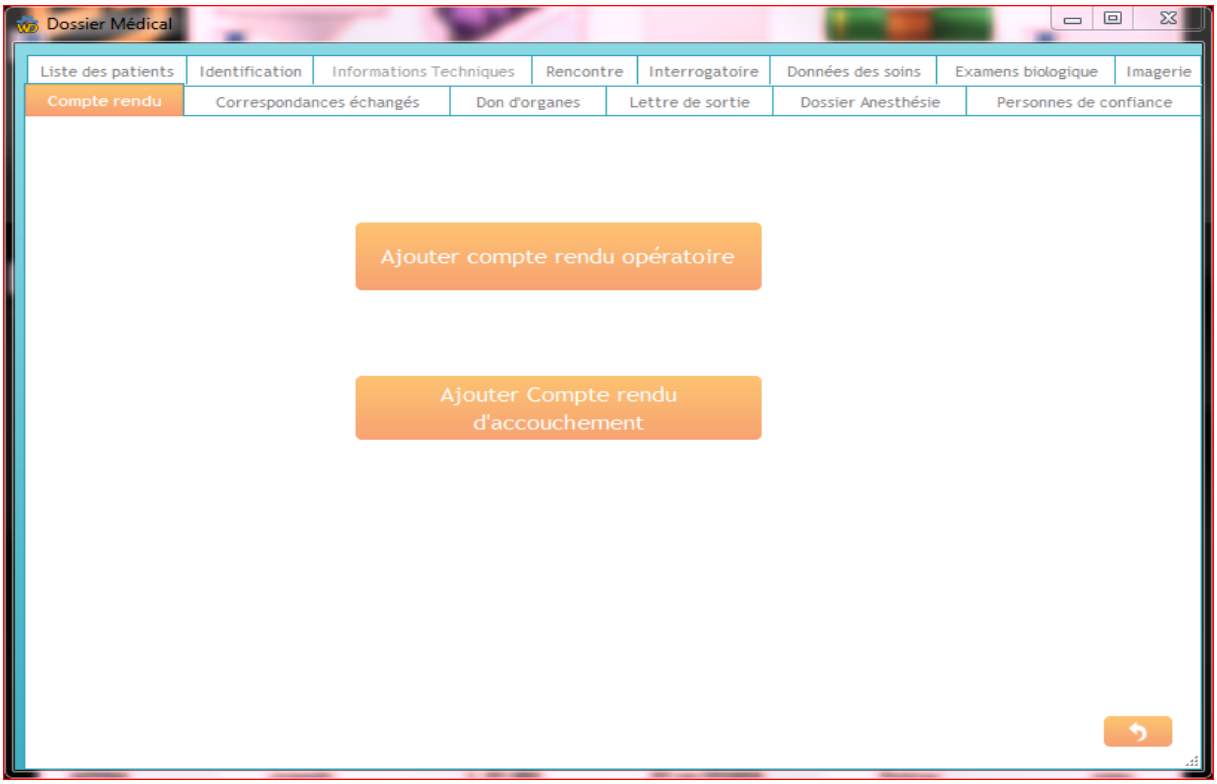

Figure : Vue -Compte rendu-

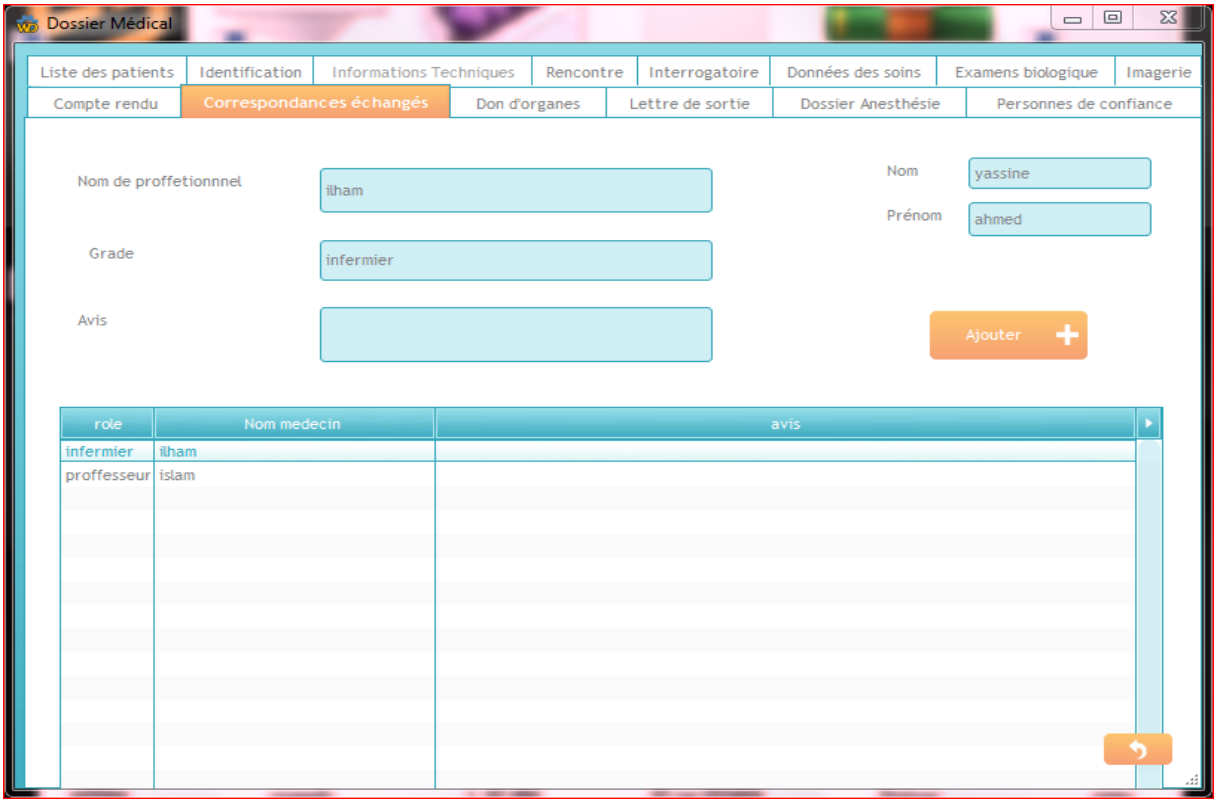

Figure : Vue -correspondances échangés-

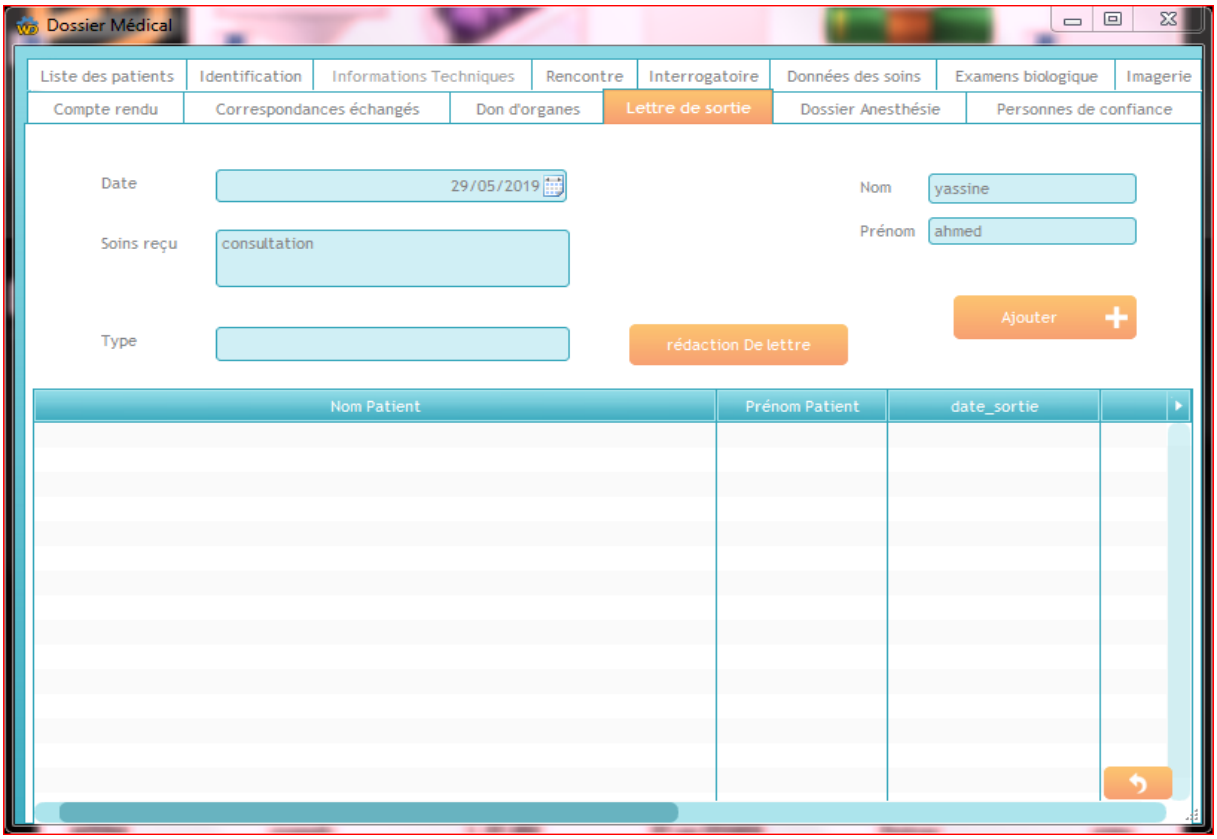

Figure : Vue -Lettre de sortie-

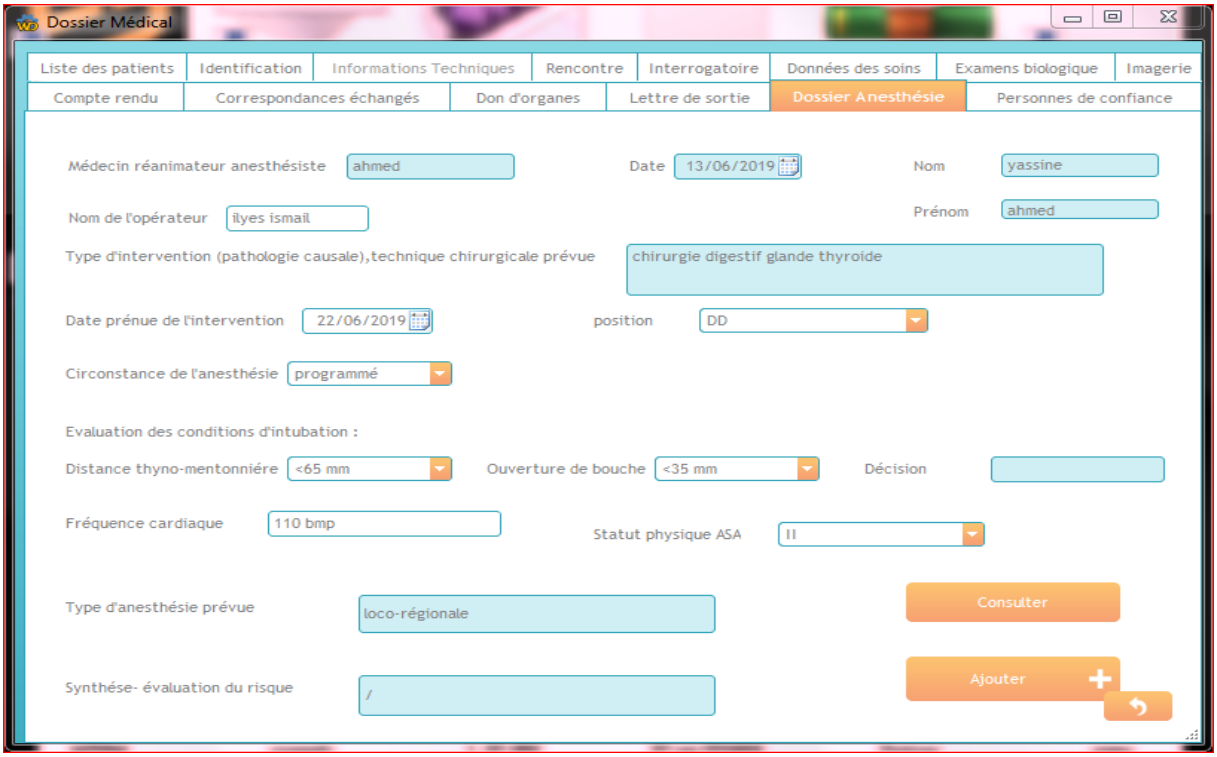

Figure : Vue-Dossier anesthésie-

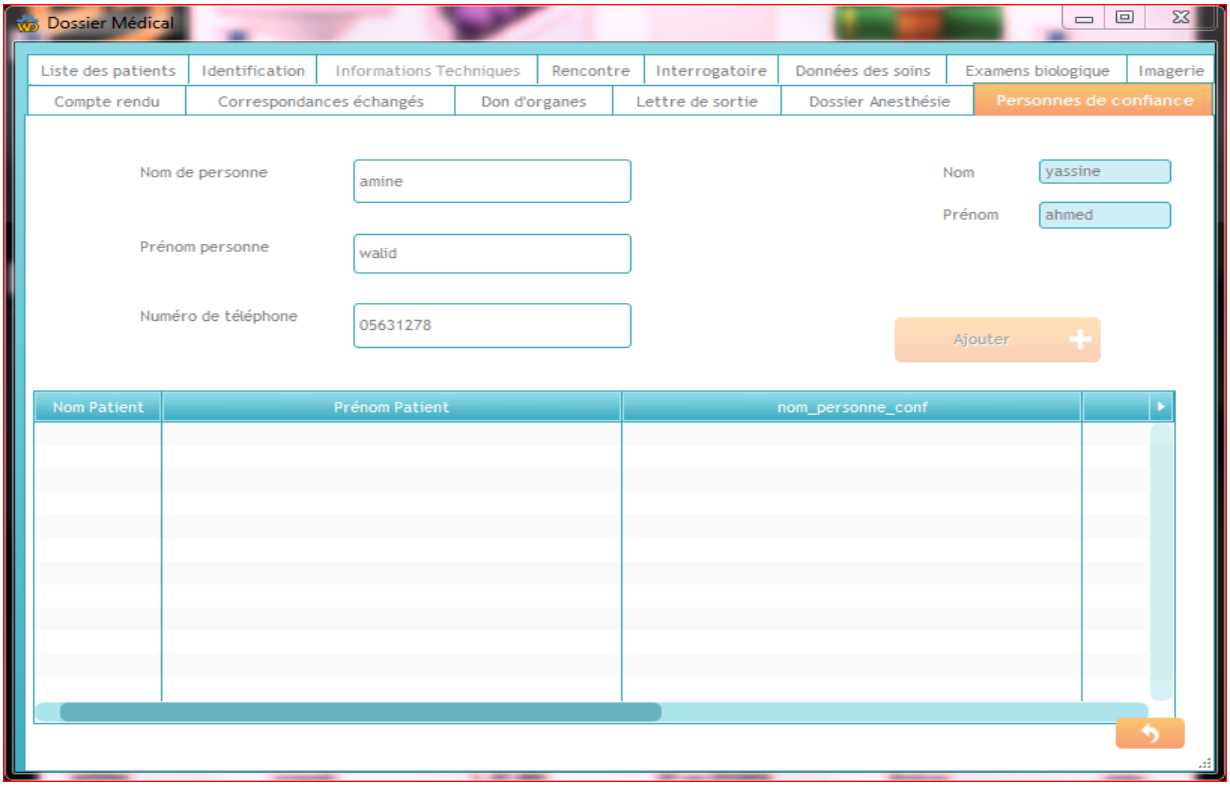

Figure : Vue -personnes de confiance-

BIBLIOGRAPHIE

- **[01] JF Pillou ;** Tout sur les systèmes d'information, Paris Dunod 2006, Collect° Commentcamarche.net
- **[02]** SecuriteInfo.com : https://www.securiteinfo.com/conseils/introsecu.shtml Consulter le Janvier 2019
- **[03]** Alban Gabillon « Contrôle d'accès – Contrôle de flux – Contrôle d'usage – Le projet ANR FLUOR ». Université de la Polynésie Française
- **[04]** LOUNIS Nawal. « Conception d'une architecture distribuée de contrôle d'accès avec la détection et la prévention de Clients intrus dans le Cloud. » ; Mémoire POUR l'OBTENTION DU DIPLOME DE MAGISTÈRE ; 2014.
- **[05]** Intrapole.com http://www.intrapole.com/spip.php?article16 Consulter le Janvier 2019
- **[06]** Marwan CHEAITO. « Un cadre de spécification et de déploiement de politiques d'autorisation » ; THÈSE En vue de l'obtention du DOCTORAT. Université Toulouse III - Paul Sabatier ; 2012.
- **[07] N**ational **C**omputer **S**ecurity **C**enter (**NCSC**), « A Guide to Understanding discretionary Access Control in Trusted systems », 1987
- **[08]** DEBIANE noureddine et ZEGMALI fatima zohra. « Développement d'un modèle pour le contrôle d'accès au dossier médical personnel (Etude de cas : CHU Algérien) » ; MEMOIRE DE PFE pour l'obtention du Diplôme de MASTER en GENIE BIOMEDICAL ; Université Abou Bakr Belkaïd de Tlemcen ; 2017
- **[09]** Pardonne KALIBA MULANGA ; « La gestion décentralisée d'un hôpital public en RD Congo » ; CIDEP/Université Ouverte, Licence en santé publique, Mémoire Online ,2008
- **[10]** Sofiene Boulare « Validation des politiques de sécurité par rapport aux modèles de contrôle d'accès » ; Université du Québec en Outaouais, Aout 2010
- **[11]** Amal HADDAD « modélisation et vérification de politiques de sécurité », Université Joseph Fourier, Genève
- **[12]** Anas ABOU EL KALAM Docteur de l'Institut National Polytechnique de Toulouse Thèse « MODÈLES ET POLITIQUES DE SECURITE POUR LES DOMAINES DE LA SANTE ET DES AFFAIRES SOCIALES » Année 2003, Roche 31077 Toulouse Cedex 4
- **[13]** HAOUCHE Djahida. « Sécurisation des Données de santé informatisées » ; MEMOIRE DE PROJET DE FIN D'ETUDES pour l'obtention du Diplôme de MASTER en GENIE BIOMEDICAL ; Université Abou Bakr Belkaïd de Tlemcen ; 2015
- **[14]** E. Bertino, P. A. Bonatti, ET E. Ferrari, « TRBAC: A temporal role-based access control model », ACM Trans. Inf. Syst. Secur. 4(3): 191-233, 2001.
- **[15]** R. Thion, « Structuration Relationnelle des politiques de contôrle d'accès Resprésentation, Raisonnement et Vérification, » Thèse sotenu en 2008.
- **[16]** R. K. Thomas et R. S. Sandhu. Task-Based Authorization Controls (TBAC): A Family of Models for Active and Enterprise-Oriented Authorization Management. In Tsau Young Lin & Shelly Qian, editeurs, IFIP'98: 11th International Conference on Database Security, Lake Tahoe,

California, volume 113 of IFIP Conference Proceedings, pages 166–181. Chapman & Hall, 1997. 27, 32, 34.

- **[17]** 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. » ; Université Jean Monnet de Saint-Étienne 2012.
- **[18]** Anas Abou El Kalam, Rania El Baida, Philippe Balbiani, Salem Benferhat, Frédéric Cuppens, Yves Deswarte, Alexandre Miège, Claire Saure, Gilles Trouessin. **«** ORBAC : un modèle de contrôle d'accès basé sur les organisations »
- **[19]** Aristote et al, Organon. Havard University Press, 1960.
- **[20]** T.Monnin, « *L'ingénierie philosophique du rodulf carnap* », Cahier philosophiques, no. 2, pp. 27-53, 2015
- **[21]** Raskin, C. F. Hcmpelman, K. ETriczenberg, et S.Nirenburg, « Ontology in information security: a useful theoretical foundation and methodological tool », dans *Procceding of the 2001 Workshop on New security paradigms*. ACM, 2001, pp.5-59.
- **[22]** Riad LEKHCHINE « Construction d'une ontologie pour le domaine de la sécurité : Application aux agents mobiles » Université Mentouri – Constantine ; 2009.
- **[23]** Natalya F. Noy and Deborah L. McGuinness, *"Ontology Development 101: A Guide to Creating Your First Ontology"*. Stanford Knowledge Systems Laboratory Technical Report KSL-01-05 and Stanford Medical Informatics Technical Report SMI-2001-0880, March 2001.
- **[24]** alsa-créations ; https://www.alsacreations.com/astuce/lire/40-quest-ce-que-le-w3c-a-quoi-sert-il.html consulter le 24/02/2019.
- **[25]** Garf ; Qualité en formation, analyses de pratiques d'entreprises (La) : journée technique du GARF 27 JUIN 1996.
- **[26]** Étienne Théodore SADIO « Contrôle d'accès par les ontologies Outil de validation automatique des droits d'accès » UNIVERSITE LAVAL ; 2015.
- **[27]** Gomez Pérez A., Benjamins V.R. *"Overview of Knowledge Sharing and Reuse Components: Ontologies and problem-Solving Methods"*. Proceeding of the IJCAI-99 workshop on Ontologies and problem-Solving Methods (KRR5), Stockholm (Suède), pp. 1.1-1.15, 1999.
- **[28]** Étienne Théodore SADIO ; « Contrôle d'accès par les ontologies Outil de validation automatique des droits d'accès » ; Université LAVAL Québec, Canada ; 2015
- **[29]** Lezghed Amir ; « La Génération Automatique des Ontologies à partir des Diagrammes de classes UML » ; Mémoire de Fin d'études Master ; Université de 8 Mai 1945 – Guelma - ; Juin 2017
- **[30]** Institut Numérique https://www.institut-numerique.org/21-les-ontologies-51f7a7f9e921c Consulter le Fev 2019
- **[31]** M. Buffa, C. Faron-Zucker, and A. Kolomoyskaya, "Gestion sémantique des droits d'accès au contenu : l'ontologie amo," in *EGC'10*, 2010, pp. 471–482.
- **[32]** Wei-Tek Tsai ; ET Qihong Shao « CA basé sur les rôles à l'aide d'une ontologie de référence dans les nuages ». IEEE
- **[33]** Chang Choi ; « Modèle de CA basé sur ontologie pour le raisonnement du politique de sécurité dans le cloud computing » ; Le journal de la superInformatique ; pp711-722. Mars 2014.
- **[34]** A. Mohammad , G. Kanaan , T. Khdour , S. Bani-Ahmad ; " *Ontology based access control model for semantic web services*"; The Arab academy for Banking and financial sciences, Damascus, Syria. The Arab academy for Banking and financial sciences, Amman, Jordan Al-Balqa Applied University, Salt, Jordan (Received March 7, 2011, accepted March 20, 2011).
- **[35]** Philippe MASSARI ; Médecin des Hôpitaux – Responsable de l'Unité d'Informatique Médicale - CHU de ROUEN ; « Informatisation du Dossier Médical »

- **[36]** DMP « Le Dossier Médical Partagé » https://www.dmp.fr/patient/faq Consulter le Janvier 2019
- **[37]** BENOUADAH Ali et GUENDOUSSI Nourelhouda ; « Conception et réalisation d'une application pour la gestion du dossier médical personnel (Etude de cas : CHU Algérien) » ; MEMOIRE DE PFE Pour l'obtention du Diplôme de MASTER en GENIE BIOMEDICAL. Université Abou Bakr Belkaïd de Tlemcen
- **[38]** CREGG https://www.cregg.org/commissions/informatique/le-dmp/objectif-du-dmp/ Consulter le Janvier 2019
- **[39]** Wikipedia, https://fr.wikipedia.org/wiki/Dossier_médical_personnel Dossier médical personnel. Consulter le Janvier 2019
- **[40]** ASIP SANTÉ, Site Web : http://esante.gouv.fr Consulter le Janvier 2019
- **[41]** HAOUCHE Djahida. « Sécurisation des Données de santé informatisées » ; MEMOIRE DE PFE pour l'obtention du Diplôme de MASTER en GENIE BIOMEDICAL ; Université Abou Bakr Belkaïd de Tlemcen ; 2015
- **[42]** code de la santé public. Article L1110-4. / Modifié par Ordonnance n°2018-20 du 17 janvier 2018 - art. 2
- **[43]** Code de la santé publique - Article L1111-7
- **[44]** TITRE : L'accès au dossier médical d'un patient décédé - Collège des Médecins du Québec. Une médecine de qualité au service du public. http://www.cmq.org/pdf/banque-info/binfo486.pdf?t=1536105600034 ; Consulter le Janvier 2019
- **[45]** Santé - CNIL - Commission nationale de l'informatique et des libertés Fiche pratique Sous-traitance : Modèles de clauses de confidentialité « Protéger les données personnelles, accompagner l'innovation, préserver les libertés individuelles », 02 mai 2011
- **[46]** ASIPSanté « Agence Des Systèmes D'Information Partagés De Santé ». [Le Dossier Médical Personnel et la sécurité]. FICHE PRATIQUE – JUIN 2011.
- **[47]** ZERKOUK Meriem ; « Modèles de contrôle d'accès dynamiques » ; THESE de Doctorat ; Université des Sciences et de la Technologie d'Oran Mohamed Boudiaf ; 2016
- **[48]** Sourour JEMILI « ANALYSE DE RISQUE DANS LES SYSTEMES DE CONTRÔLE D'ACCES » ; MÉMOIRE PRÉSENTÉ EN VUE DE L'OBTENTION DU DIPLÔME DE MAITRISE EN INFORMATIQUE ; UNIVERSITÉ DU QUÉBEC EN OUTAOUAIS 2013.
- **[49]** SYNBIOZ « Le Role Based Access Control » https://www.synbioz.com/blog/role_based_access_control Consulter le Fevrier 2019
- **[50]** SUPINFO International University: https://www.supinfo.com/articles/single/5548-securite-informatique-quoi-qui Consulter le Fevrier 2019
- **[51]** AFRI Faiza ; « Raisonnement sur une ontologie hybride pour la recherche d'informations Médicales » ; THESE de Magister ; Université Abderrahmane Mira de Bejaia ; 2009
- **[52]** Uschold, M.& Gruninger, M: "Ontologies: principals, methods and applications" Knowledge Engineering Review, Vol. 11, No. 2, 1996